Advances in Intelligent Systems and Computing 1132

Pradeep Kumar Singh ·
Bharat K. Bhargava · Marcin Paprzycki ·
Narottam Chand Kaushal ·
Wei-Chiang Hong *Editors*

Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's

Springer

Advances in Intelligent Systems and Computing

Volume 1132

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing such as: computational intelligence, soft computing including neural networks, fuzzy systems, evolutionary computing and the fusion of these paradigms, social intelligence, ambient intelligence, computational neuroscience, artificial life, virtual worlds and society, cognitive science and systems, Perception and Vision, DNA and immune based systems, self-organizing and adaptive systems, e-Learning and teaching, human-centered and human-centric computing, recommender systems, intelligent control, robotics and mechatronics including human-machine teaming, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, knowledge management, intelligent agents, intelligent decision making and support, intelligent network security, trust management, interactive entertainment, Web intelligence and multimedia.

The publications within "Advances in Intelligent Systems and Computing" are primarily proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

**** Indexing: The books of this series are submitted to ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springerlink ****

More information about this series at http://www.springer.com/series/11156

Pradeep Kumar Singh · Bharat K. Bhargava ·
Marcin Paprzycki · Narottam Chand Kaushal ·
Wei-Chiang Hong
Editors

Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's

Springer

Editors
Pradeep Kumar Singh
Department of Computer Science and Engineering
Jaypee University of Information Technology
Kandaghat, India

Marcin Paprzycki
Polish Academy of Sciences
Systems Research Institute
Warszawa, Poland

Wei-Chiang Hong
School of Education Intelligent Technology
Jiangsu Normal University
Xuzhou, Jiangsu, China

Bharat K. Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN, USA

Narottam Chand Kaushal
Department of Computer Science and Engineering
National Institute of Technology
Delhi, India

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-030-40304-1 ISBN 978-3-030-40305-8 (eBook)
https://doi.org/10.1007/978-3-030-40305-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Wireless sensor networks are being used in several kinds of applications varying from the health care, military, home, monitoring and industry. The prime objective of this book is to explore the current areas of research and challenges to be faced by different researchers. So, it can help the increasing number of scientists who depend upon sensor networks in some way. The book is organized into five parts, each part including chapters exploring a specific group of topics. The first part of the books covers the topics related to algorithms, protocols, communication strategies and data aggregation in wireless sensor networks (WSNs). The second part of the book is composed of topics related to energy conservation and management in WSNs. The third section of the book includes the chapters related to security and QoS in WSNs. Some of the useful applications of WSNs are covered in section four. Finally, the advancements on wireless sensor networks are included in section five. Book contains total 33 chapters.

The main readers of this book are expected to include the scientists, scholars and researchers in the field of computer science engineering and communication engineering; along with this, it is going to be very useful for the UG and PG students who are studying the wireless sensor networks as an elective or core course. Specialists, as well as student readers will find all the articles encouraging and helpful for their projects.

The main objective of this edited book is to concentrate on all aspects of current and future research directions related to the wireless sensor networks. Number of novel techniques that lead to future improvements in the area of wireless sensor networks are also included.

We would like to extend our sincere thanks to all the reviewers for providing the constructive feedback for the improvement of the quality of chapters. We also acknowledge the several authors who have contributed their chapter in this edited book. We are thankful to Dr. Thomas Ditzinger, Editorial Director, Interdisciplinary and Applied Sciences, Engineering, Springer, for his constructive comments for the

improvement of this book project. Finally, we would like to express our special thanks to Prof. Janusz Kacprzyk, Editor, and AISC Springer Series for believing in us and providing us constructive feedback during the approval of the book proposal.

Pradeep Kumar Singh
Marcin Paprzycki
Bharat K. Bhargava
Narottam Chand Kaushal
Wei-Chiang Hong

List of Reviewers

Abdul Zainul-Abedin	University of Ontario Institute of Technology (UOIT), Canada
Abhijit Sen	Kwantlen Polytechnic University, Canada
Ahmed Aliyu	Universiti Teknology, Malaysia
Amit Prakash Singh	GGSIPU, Delhi, India
Anton Pljonkin	Sothern Federal University, Russia
Arti Noor (Senior Director)	CDAC, Noida, India
Arvind Selwal	Central University of Jammu, J&K, India
Baijnath Kaushik	SMVDU, Jammu, India
Bharat K. Bhargava	Department of Computer Sciences, Purdue University, USA
C. K. Jha	Banasthali University, India
Chuan-Ming Liu	National Taipei University of Technology, Taiwan
Divya Chaudhary	Netaji Subhas Institute of Technology, University of Delhi, India
Gayatri Sakya	JSSATE, NOIDA, India
Hardeo Kumar Thakur	NSIT, Delhi, India
Inga Rüb	Warsaw University, Poland
Jitender Kumar Chhabra	Department of Comp. Engg., NIT Kurukshetra, India
Maheshkumar H. Kolekar	Dept. of Electrical Engineering, IIT, Patna, India
Malay Kumar	IIIT Dharwad, India
Maninder Jeet Kaur	Amity University, Dubai
Manju Chaudhary	NSIT, Delhi, India
Manu Singh	HRIT, Ghaziabad, India
Maria Ganzha	University of Technology, Warsaw, Poland
Maria Simona Raboaca	Romania
Marius M. Balas	Faculty of Engineering, University "Aurel Vlaicu" Arad, Romania
Mariusz Nycz	Rzeszow University of Technology, Poland

Mayank Aggarwal	Gurukul Kangari University, Haridwar, India
Miklós Molnár	Informatics Department, France
Mohd Helmy Abd Wahab	Universiti Tun Hussein Onn Malaysia, Malaysia
Nagesh Kumar	Shoolini University, Solan, HP, India
Narottam Chand	Department of CSE, NIT Hamirpur, India
Neeta Singh	Gautam Buddha University, India
Panagiotis Karkazis	University of West Attica, Greece
Pao-Ann Hsiung	National Chung Cheng University, Taiwan
Parulpreet Singh	Lovely Professional University, India
Pelin Angin	Purdue University, USA
Pooja Kapoor	Amity University Lucknow, India
Puneet Azad	Maharaja Surajmal Institute of Technology, Delhi, India
Rabindra Bista	Kathmandu University, Nepal
Rajeev Kumar	National Institute of Technology, Hamirpur
Ramiro Liscano	University of Ontario Institute of Technology (UOIT), Canada
Ritika Mehra	DIT University, Dehradun, India
Sabrina Tiun	UKM, Malaysia
Samayveer Singh	NIT Jalandhar, India
Sanjay Sood (Associate Director)	CDAC, Mohali, India
Satish Jondhale	Amrutvahini College of Engineering, Sangamner, India
Subhash Sharma	IIT Roorkee, India
Sudeep Tanwar	Nirma University, India
Sudhanshu Tyagi	Thapar Institute of Engineering & Technology, Patiala, India
Sultan Ahmad	Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia
Sumita Mishra	ASET, Amity University, India
Sushila Madan	LSR, University of Delhi, India
Tomasz Bartczak	Faculty of Engineering, Vistula University, Poland
Tuan Anh Nguyen	Vietnam Academy of Science and Technology, Vietnam
Virender Ranga	National Institute of Technology, Kurukshetra, India
Vivek Kumar Sehgal	JUIT, Waknaghat, India
Yashwant Singh	Central University of Jammu, J&K, India
Yu Miao	Baylor University, Texas
Yugal Kumar	JUIT, Waknaghat, India
Wei-Chiang Hong	School of Computer Science and Technology, Jiangsu Normal University, China

Agnieszka Kubacka	State Higher Vocational School in Krosno, Poland
Anshu Oberoi	IKG Punjab Technical University, India
Gonçalo Miguel Santos Marques	Telecommunications Institute, Portugal
Meera Indracanti	University of Gondar, Gondar, Amhara, Ethiopia
Mircea Raceanu	ICIT, Romania
Reinaldo Padilha France	State University of Campinas – UNICAMP, Brazil
Salome Oniani	Faculty of Informatics and Control Systems, Georgian Technical University Tbilisi, Georgia

Contents

An Introduction on WSN Algorithms, Protocols, Communication Strategies and Data Aggregation

Introduction on Wireless Sensor Networks Issues and Challenges in Current Era

Pradeep Kumar Singh[1(✉)] and Marcin Paprzycki[2]

[1] Department of Computer Science and Engineering,
Jaypee University of Information Technology, Waknaghat, Solan, HP, India
pradeep_84cs@yahoo.com
[2] Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland
paprzyck@ibspan.waw.pl

1 Introduction

Wireless Sensor Networks (WSNs) issues and challenges in current scenarios, covers the latest principles of WSNs, algorithms, protocols, architectures and technological advancements across all aspects of sensor systems, including the security and synchronizations related considerations. Here, an attempt has been made to identify the latest developments in the area of wireless sensor networks. Chapters of this book cover the recent advancements from architecture to protocols design, algorithm development, security issues, QoS parameters, to advance topics, including Internet of things, fusion and use of artificial intelligence for WSNs, one by one, in separate chapters. At the end of each chapter, future challenges are summarized, to help the researchers along with some challenging topics that can be taken as topics of their future research. This book is organised into five parts. Part 1 covers the latest developments in term of features, platforms, standards, algorithms, protocols, communication strategies and data aggregation issues in WSNs. Part 2 presents topics related to energy conservation and management in WSNs. Part 3 describes security & quality of service (QoS) requirements in WSNs. Several applications of WSNs are discussed in Part 4. Finally, Part 5 concludes discussion of advanced topics on WSNs, including use of IoT, data mining and fusion approached along with application of artificial intelligence in smart cities.

The scope of our book is to cover the recent issues and challenges specific to WSNs only. Prime objective of the book is to cover the recent developments. Numerous protocols and modification in architectures came into existence for WSNs due to change in day to day technological requirements along with the support of better communication channel bandwidth (4G&5G). This book covers the most recent technological advancements in the area of WSNs and also identifies the major issues and challenges for WSNs. It will help scholars, academicians, students, working in the area of WSN, to further lead their work and may serve as an essential reference material.

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario*, AISC 1132, pp. 3–12, 2020
https://doi.org/10.1007/978-3-030-40305-8_1

2 Summary of Book of Chapters

Let us now summarize content of all 33 book chapters, including this, introductory, chapter. There are eight chapters in the first Part of this book. Current chapter provides an overview of all chapters in the book, and an overview of wireless sensor networks and summary of current issues and challenges. Second chapter delivers a detailed overview of WSNs and their applications in smart grid, transportations, smart homes and smart agriculture along with the integration of internet of things (IoT). These two chapters can be seen as an overview and foundation for the remaining material.

Third chapter of Part 1, is focused on Medium Access Control (MAC) Protocols for Wireless Sensor Networks (WSNs). MAC is responsible for controlling access to the common wireless medium. Depending upon the type and level of information processed by MAC, coordination among the nodes is another big challenge, in terms of local and global aspects. Energy efficiency is still the open challenges, while designing the MAC protocol, due to limited energy capacity of sensor nodes. MAC protocol should also support the variations, in terms of network size, network topology and node density during scalability. In addition to this, fairness, bandwidth utilization of network, minimized latency and gain in throughput are also the significant features in the design of medium access control protocols for WSNs. Author has also considered the latest progress in cognitive radio research and developments, in the context of the design of MAC protocol for WSNs. This chapter reports two methods that are being used during MAC implementation; (i) first is based on the use of microcontrollers and RF communication modules, while (ii) the second method is based on implementation of full system on a single chip. As far as the first method for MAC is concerned, the microcontroller runs a RTOS or devoted software and usages the communication protocols to manage RF peripherals, on the other side all characteristics and functionalities of the WSN may be implemented on a single chip.

Fourth chapter is entitled “Performance of energy and distance based modified threshold for LEACH”. Author focuses on saving the energy to improve the network lifetime in WSNs. Emphasize is given on cluster head selection scheme, which is important to save the transmission energy. This chapter discusses the threshold conditions for selection of cluster head to save energy using improved LEACH. Simulation results deliver clear evidence of satisfactory lifetime extension with change in the density of nodes.

Fifth chapter considered the MAC Protocols for Mission Critical Applications using WSNs. Initially the review on existing MAC protocols and their mechanism is carried out. Thereafter, authors have identified the need for mission critical MAC protocol requirements. Next section of the chapter, covers use of matrices for performance analysis including a case study. Finally author has discussed the integration of machine learning algorithm for MAC protocol followed by recent issues and challenges for the MAC protocol.

Sixth chapter is entitled "QoS Routing for Data Gathering with RPL in WSNs". This chapter reports on two key issues; "(i) tools using traffic engineering (TE) to manage the packet forwarding, and (ii) QoS aware routing to compute routes offering the asked guaranties". Initially the issues related to QoS constrained routing are taken into account, followed by routing in WSNs. Routing Protocol for Low-Power and Lossy Networks (RPL) is reported as a better solution and QoS aware routing using RPL. It is identified that, in future simple multi-parent solutions using RPL, handling uncertainties by multi-path and opportunistic routing should be explored. Coupling of routing with traffic engineering is still an open research issue.

Seventh chapter covers a comparison of Neural Network Training Functions for RSSI based Indoor localization Problem in WSNs. Performance of eleven types of training function is analysed, for feed forward neural network, for the RSSI-based indoor target localization in WSNs, in terms of Average Localization Error. Based on performed analysis, it is found that Levenberg-Marquardt (LM) based FFNT implementation gives better results and is more consistent in providing quality location estimates.

Eighth chapter is entitled "Performance Assessment of the Fixed Node Assisted Col-lection Tree Protocol (FNA-CTP) in a Mobile Environment". In an indoor sport field, using tinyOS, FNA-CTP algorithm is applied on a set of senor nodes. Exciting part of the analysis done in the chapter is that CTP outperformed FNA-CTP in the field experiments, on the contrary to the simulation results that showed exactly the opposite. Authors have also included the experimental challenges during data pre-processing and capturing packets by a sniffer in the field and at the sink as well.

Part 2 is composed of six chapters and covers issues related to energy conservation and management in WSNs. Ninth chapter of the book and first chapter under this Part is entitled "An Effective Analysis and Performance Investigation of Energy Heterogeneity in Wireless Sensor Networks". Three level of heterogeneity are investigated for LEACH, SEP, DEEC, HEED, and PEGASIS. This chapter also highlights the benefits of the heterogeneous models, over the homogeneous ones, in term of WSNs.

In chapter ten, efforts have been put on "A Firefly Optimization Algorithm for Maximizing the Connectivity in Mobile Wireless Sensor Network". Initial issues, related to the mobile WSNs, are discussed followed by related work on mobile WSNs. Experimental results have been shown for the FACM algorithm, using a MATLAB tool box. Proposed FACM algorithm has shown better and promising results as compared to the existing Firefly Algorithm (FA) algorithms.

Eleventh chapter is entitled "Energy conscious packet transmission in wireless networks using trust based mechanism: A Cognitive Approach". This chapter discusses effectiveness of trust-based mechanisms for early detection of malicious nodes in WSNs. Authors have reported the summary of trust-based mechanisms, followed by contributions and gaps in trust-based mechanisms for WSNs. Finally a trust-based framework has been designed to identify the malicious nodes.

Twelfth Chapter is titled "Energy Distance Neighbourhood Based Weighted Hierarchical Clustering Algorithm". This chapter reports a new algorithm "EDN", which is based on a weighted scoring model, using the residual energy concept, and distance from the BS to neighbourhood stations, to further improve network lifetime. Proposed algorithm is found to be better in terms of network stability and longevity for WSNs.

Thirteenth has title “Recent Advances in Wireless Sensor Network for Secure and Energy Efficient Routing Protocol”. It summarizes state-of-the-art of secure and energy efficient routing protocols in WSNs. It discusses security requirements in WSNs and how different protocols are meeting these requirements.

In the similar direction of the previous chapter, the next chapter (number fourteen; entitled “Energy Efficient Routing Protocols for Wireless Sensor Network”) delivers a comprehensive coverage of parameter comparison of homogeneous and heterogeneous routing protocols in WSNs.

Part 3 of this book combines and covers topics related to security and QoS in WSNs. This Part contains total of seven chapters (numbered 15–21).

Chapter 15 is entitled “Low-cost architecture of the universal security threat detection system for Industrial IoT”. Here, the wired communication environment is reported for WSNs, from the algorithmic view point. Focal angels of results contained in this chapter are: intelligent data analysis and biologically inspired methods. Initially the industrial information systems architectural and security issues are discussed, followed by properties of the threat detection system and hardware architecture. Finally, reference vectors, k-nearest neighbours, neural networks and decision trees algorithms are analyzed in term of correctness, completeness and precision.

Chapter 16 is devoted to “SYLOC: hybrid key generation in sensor network”. It covers hybrid key generation approach to provide security in WSNs. The proposed approach is claimed to secure the network against the wormhole, sinkhole and sybil attacks.

Chapter 17 is written on the topic “Diffie-Hellman Algorithm Pedestal to authenticate nodes in WSNs”. Author focuses on use of authentication key, to bring security in the network. Diffie-Hellman Algorithm is used for generating the keys. Proposed technique has minimized the forge and replay attack and it also conserves the energy with improvement in reliability of the network.

“Privacy Aware prevention of Sybil Attack in Vehicular Ad Hoc Networks” is discussed in Chapter 18. This chapter applied the public key and symmetric key encryption for securing the communication path in VANET. Token based scheme is used in clusters to detect the attackers, whenever two identical token are spotted the algorithm revokes access to other vehicles in the cluster.

In order to gain insight to security in the area of the Internet of Things (IoT), Chapter 19 is devoted to “Key Management Schemes in Internet of Things: A Matrix Approach”. This chapter gives overview of matrix based key management schemes in IoT, followed by security mechanisms to secure the communication channel. BLOM’s, CARPY, Kronecker Product and pair wise key management schemes are covered and compared.

Chapter 20 concerns “Black Hole Attack and Its Security Measure in Wireless Sensors Networks”. This chapter mainly focuses on black hole attack, along with security measures that can be applied in this case. Author discusses various attacks in WSNs, followed by analysis on common attacks at various layers in WSNs. Finally, power variation with attack and with security is analyzed in the network.

The last chapter of Part 3, Chapter 21, is entitled on “Detection and Tracking of Mobile Intruder in Harsh Geographical Terrains using Surveillance Wireless Sensor

Networks". This chapter summarizes issues related to several real-time challenges for WSNs in intruder detection and tracking.

Part 4 is devoted to applications of Wireless Sensor Networks (WSNs) and it is composed of five chapters (22 to 26). First chapter of this Part covers the opportunities and challenges with Wireless Sensor Networks (WSNs) in smart/precision agriculture. Specifically, it is focused on three main issues; (i) what are the possibilities of use of WSN and IoT in agriculture? (ii) what are the newly developed sensors, to be used for making smart agriculture a revolution? and (iii) what are various issues and challenges researchers may face, when they are working with WSN in agriculture? Discussion covers data analytics in decision making for prediction of agriculture related attributes. In addition, hardware deployment and resistance of hardware to environmental factors as well as data storage, data security and deep analytics, device management from the remote sensing techniques, sensors deployed in field and for images received from drones are discussed.

Chapter 23 is on "Detection and Monitoring of Forest Fire using Serial Communication and Wi-Fi Wireless Sensor Network". NodeMCU an open IoT based platform is used for forest fire detection. A domain specific case study shows how the data is collected. Thereafter, implementation challenges for the forest fire system are reported.

Next, Chapter 24, is entitled "Application of Supervised Learning Approach for Target Localization in Wireless Sensor Network". It compares localization performance in terms of supervised algorithms, using Generalized Regression Neural Network (GRNN), Multilayer Perceptron (MLP), Radial Basis Function Network (RBFN), and Feed Forward Neural Network (FFNT), for the WSNs indoor localization. Overall, the proposed GRNN-based localization algorithm is found to perform better than the other algorithms.

In next two chapters, efforts have been put to discuss interesting applications of WSN and IoT. Chapter 25 is devoted to "Implementation of Automated Aroma Therapy Candle Process Planting Using IoT and WSN" while Chapter 26 concerns "Implementation of Automated Retractable Roof for Home Line-Dry Suspension Area Using IoT and WSN". In both chapters, specific applications are discussed, with attention paid to WSN aspects of developed solutions.

Last Part of this book is focused on recent advancements of wireless sensor networks. This Part contains total of seven chapters (27 to 33). Chapter 27 deals with "IoT enabled Air Pollution Monitoring in Smart Cities". The proposed solution may be useful for the current time for smart cities as it delivers real-time pollution matrices for better control. In the next Chapter (28), author discusses use of data mining and fusion techniques, applied to WSN data, for better event prediction. Specifically, data analytics are used to predict the forest fire with better accuracy.

Chapter 29 deals with "Internet of Things for Enhanced Living Environments, Health and Well-being: Technologies, Architectures and Systems". Here, the focus of presented work is on human-centred use of IoT in different areas of day-to-day life. Moreover, detailed summary of technologies, architectures, and systems utilizing IoT in Ambient Assisted Living (AAL), for enhanced living environments, is presented. Future challenges, in terms of implementation of such systems, are also added.

Chapter 30 concerns "Energy Efficient Data Collection in Smart Cities Using IoT". As data size is rapidly increasing, in almost every application area, and in smart cities

in particular, energy efficient data collection is one the key requirements. This chapter reports on one of efforts focused on exploring challenges during data collection, for various applications in an energy efficient way, using WSN within IoT as applied to smart city scenarios.

Chapter 31 is entitled "A Review on Hybrid WSN-NGPON2 Network for Smart World". There, it is claimed that several shortcomings of WSN may be overcome using the passive optimal network (PON). Next generation passive optical network stage 2 (NG-PON2) is considered as an improvement over the WSN, in terms of higher data rate and better Quality of Service (QoS) at low cost.

Chapter 32 shows one of the new directions of research concerning "Internet of Things in Forensics Investigation in Comparison to Digital Forensics". A detailed comparison, in term of set of steps involved in the investigation process in digital versus IoT forensics is presented.

As artificial intelligence is one of the popular area of research and is used in various application focused on betterment of life, combining use of AI and WSN, is the topic of the last Chapter (33) of this book ("A Review on The Artificial Intelligence Algorithms for The Recognition of Activities of Daily Living Using Sensors in Mobile Devices"). Specifically, recognition of Activities of Daily Living, on the basis of data available in mobile devices is analysed and associated challenges identified.

3 Open Research Challenges for Wireless Sensor Networks

Wireless Sensor Networks (WSN) consists of self-organized network of large number of distributed sensor nodes. The sensor nodes are resource constrained, application oriented, and comprise a dynamic topology. The major research in the field of sensor networks concerns: architecture, operating system(s), deployment, localization, data aggregation, Quality of Service, and security [1]. In addition to the unreliable communication within the sensor network, there exist also other challenges, such as nodes in the WSN that have to work with the limited energy, memory, computation, and limited processing capacity [3]. This section highlights some of the key current research challenges in the area of WSNs.

3.1 Challenges of WSNs in Terms of Design

WSNs are more challenging, due to the lack of resources such as limited battery, bandwidth and processing power [2, 4]. The following design requirements should be considered by the designers of WSN-based ecosystems.

a. **Energy Efficiency**
   Shortage of energy is major issue in sensor networks, as most of the WSNs are powered through batteries. The performance of the network is badly affected when the battery of a sensor device is depleted. The WSNs consist of thousands of energy constrained sensors that are deployed for an application; thereby designing an energy efficient routing protocol it is the foremost requirement. Here, energy conservation has to include all aspects of the system, each one of them separately, and their interactions.

b. **Complexity**
The second design issue is the complexity of routing protocols. Too complex routing protocols may affect adversely the performance of the sensor network. However, protocols that are too simplistic may not be able to effectively deal with complexity of ecosystems. Here, note that, heterogeneous capabilities of existing hardware, and pronounced energy constraints are the reasons for the complexity of deployed WSNs. Therefore the right balance needs to be found to effectively deal with complexity, while not degrading WSN performance.

c. **Scalability**
The routing protocol must support scalable network deployments, because sensors are getting cheaper. As a result very large numbers of sensors can be easily deployed in WSNs-based ecosystems. Moreover, when ecosystems are to be merged, to deliver novel services, sizes of resulting WSNs may even double at a moments notice. The addition of any number of sensor nodes into a network, at any time, should be supported by the WSN protocol.

d. **Real Time Challenges**
Sensor nodes collect sensed information of the environment and have to deal with practical environments. The sensed information must be delivered within a certain (restricted) time so that the necessary action can be undertaken. Here, some applications may even require an instant response, without any delay. Examples of such situations are fire detection, weather monitoring, etc. Therefore, a routing protocol in WSNs should offer minimal delay in terms of sensor stream processing. The time required to transmit sensed information should be as minimal as possible and this remains a considerable challenge for WSNs applications.

e. **Robustness**
The real time applications of WSNs may require deployment of sensor nodes in harsh and non-typical environments. There is also a possibility that sensor node(s) may expire, or leave the network, during ecosystem lifetime. Therefore, a node must be adaptable to such conditions including severe and harsh environments. So, the adaptability and dynamic routing are two big challenges. Note that this means also that more research on autonomy and self-* WSN ecosystems is needed.

3.2 Challenges of WSNs in Terms of Architecture

The architecture of the WSNs is one of major reasons, which limits the progress of sensor networks. The architecture of network may be referred to as basic building blocks for the implementation of functionalities, along with the set of interfacing devices, routing protocols, functionalities and basic hardware. The software architecture addresses a bridge among the raw hardware and the other system. The continuous monitoring, data encoding and its transmission required to be calculated in parallel. Additionally, the sensor events, and calculation of data, should be processed continuously along with the progress of communication. The topological changes for the durable and scalable architecture must require only a minimum transmission of updating messages across the network. The system should be flexible enough to serve wide range of applications, as the WSNs can be realized using different communication protocols. The architecture must also facilitate accurate control over the transmission timing of a

channel. This condition is motivated by the requirement of ultra low communication power for the collection of data. An efficient WSN architecture must increase the speed of data path and rate of radio transmission because the energy performance of a network depends on the processing speed and the communication rate [3].

3.3 Challenges of WSNs in Terms of Network Layer

In the past decade, sensor nodes have been built to serve specific applications. Network layer is responsible for routing the sensed data from the sensor node to the base station [5, 15]. The current issues related to network layer for WSNs are as follows:

1. The power efficiency is the major issue for the transmission of collected information. It is a challenge in network layer to discover the efficient route for the transmission of data, such that the lifetime of the ecosystem (consisting of a large number of battery operated devices) can be optimized.
2. The routing protocol should consider multiple path design procedure. In case of primary route failure, the data can be transmitted to the base station through the alternative path.
3. The maintenance of route is also of major concern as, in case of node breakdown, the routing algorithm must be capable of finding new possible path for data transmission.
4. In order to minimize the power consumption, a sensor network must provide flexible and adaptable platform for performing the path discovery and its management.
5. The design must overcome redundancy which is significant among each node in order to make good use of bandwidth and improving power efficiency.

3.4 Challenges of WSNs in Terms of Transport Layer

The transport layer is responsible for providing end-to-end reliable communication. The transport layer fragments the data into packets at the transmitter and defragments them at the receiver. It is the foremost requirement for a transport protocol to guarantee the ordered transmission of segments for reliability. This layer should be reliable enough for delivering packet to several sensors, at any condition. The low bandwidth availability may results in congestion, which further results in loss of packet. The communication among nodes, and with base station, may get affected because of two reasons: (1) the predetermined placement of sensor nodes and (2) external factors, which result in poor communication [6].

3.5 Challenges of WSNs in Terms of Data Aggregation and Data Dissemination

Data aggregation is the process of collecting data from several sensors and transmits it to the base station for processing in an aggregated form. The sensor node senses environmental parameters and transmits information to the sink or to the base station periodically. The regularity of reporting data to the base station is application specific. The

information, collected from the sensors, may be redundant and too large for the base station to process it. Therefore, aggregation of data is a method to process such huge amount of data into smaller and need-specific information by converting sensed data to high quality information using queries. Data aggregation is the procedure for combining sensed information and facilitating analysis of the sensed environment [7, 17].

The major challenge for data aggregation is the unreliable nature of sensor networks. The unavailability of required data, obtained from the deployed sensor, or an incomplete information, which is obtained from the responding sensors are a norm, rather than an occurrence. The protocol must be designed to consider the redundant data, which needs to be eliminated for reducing power consumption. The improved clustering techniques must be utilized to conserve the sensor power. On the other hand, the process of inserting and routing data, and other queries, across the network is data dissemination. Data dissemination is carried out in two steps. Initially, if some data is inserted in a node, it broadcasts the updating message into the network. In next step, the node that requires data will send request back to the source node [8, 9].

3.6 Summary

The advancement in wireless sensor networks has created next generation of open challenges, which still need addressing. They need to be addressed not only as a result of curiosity, but also for the development of the next generation of WSNs-based applications. In this section we have discussed some of the current design issues and challenges associated with the WSNs. It should be noted that WSNs are an emerging field which acts as the key tool for making the life more comfortable and safe. This is clearly visible when one considers WSNs applications in smart cities [12, 13]. Moreover, design of wireless sensor networks for Internet of Things (IoT) applications becomes another challenging area. Here, merging of existing IoT deployments into next generation of IoT ecosystems will bring about all kinds of scalability challenges. This, in turn, will require integration of WSNs with 5G technologies (and, later 6G) within community/city/state/country-wide deployments; resulting in challenges that we only start to envision. In this context, it has been identified that cross layer architectures must be designed, to integrate the IoT and WSNs, and to support the 5G technologies [10]. Adoption of WSNs to edge-fog-cloud continuum-based infrastructures is another area where a number of open research questions will have to be addressed. Again, some of these questions will become known only when such infrastructures will start to be deployed on large scale. Finally, we can conclude that in order to achieve the information centric networking, design of new security solutions is one the main challenging area for wireless IoT networks [11, 14, 16]. Already today, with relatively restricted use of WSNs the scale of security threats that will have to be addressed becomes visible, with steady stream of news of successful hacking attacks.

In summary, WSNs are the area where the research challenges that are already known, and that have been addressed in this book, are only a tip of the iceberg. We sincerely hope that reading this book, will bring more needed research efforts to the area.

References

1. Kobo, H.I., Abu-Mahfouz, A.M., Hancke, G.P.: A survey on software-defined wireless sensor networks: challenges and design requirements. IEEE Access **5**, 1872–1899 (2017)
2. Rout, R.R., Ghosh, S.K.: Enhancement of lifetime using duty cycle and network coding in wireless sensor networks. IEEE Trans. Wirel. Commun. **12**(2), 656–667 (2012)
3. Islam, K., Shen, W., Wang, X.: Wireless sensor network reliability and security in factory automation: a survey. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) **42**(6), 1243–1256 (2012)
4. Hussein, W.A., Ali, B.M., Rasid, M.F.A., Hashim, F.: Design and performance analysis of high reliability-optimal routing protocol for mobile wireless multimedia sensor networks. In: 2017 IEEE 13th Malaysia International Conference on Communications (MICC), pp. 136–140. IEEE, November 2017
5. Tian, Y., Ekici, E.: Cross-layer collaborative in-network processing in multihop wireless sensor networks. IEEE Trans. Mob. Comput. **6**(3), 297–310 (2007)
6. Prayati, A.: Wireless technology applications in environment and health: network design challenges. IEEE Latin Am. Trans. **10**(3), 1853–1855 (2012)
7. Milojevic, M., Rakocevic, V.: Location aware data aggregation for efficient message dissemination in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **64**(12), 5575–5583 (2015)
8. Zonouz, A.E., Xing, L., Vokkarane, V.M., Sun, Y.L.: Reliability-oriented single-path routing protocols in wireless sensor networks. IEEE Sens. J. **14**(11), 4059–4068 (2014)
9. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
10. Babber, K., Randhawa, R.: Cross-layer designs in wireless sensor networks. In: Mishra, B.B., Dehuri, S., Panigrahi, B.K., Nayak, A.K., Mishra, B.S.P., Das, H. (eds.) Computational Intelligence in Sensor Networks. SCI, vol. 776, pp. 141–166. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-662-57277-1_7
11. Nour, B., Sharif, K., Li, F., Wang, Y.: Security and privacy challenges in information centric wireless IoT networks, pp. 1–8 (2019)
12. Thakur, D., Kumar, Y., Kumar, A., Singh, P.K.: Applicability of wireless sensor networks in precision agriculture: a review. Wirel. Pers. Commun. **107**(1), 471–512 (2019)
13. Sharma, A., Singh, P.K., Sharma, A., Kumar, R.: An efficient architecture for the accurate detection and monitoring of an event through the sky. Comput. Commun. **148**, 115–128 (2019)
14. Sharma, A., Kumar, R., Singh, P.K.: SLA Constraint Quickest Path Problem for Data Transmission Services in Capacitated Networks. Int. J. Performability Eng. **15**(4), 1061–1072 (2019)
15. Kumar, H., Singh, P.K.: Power transmission analysis in wireless sensor networks using data aggregation techniques. IJISMD **9**(4), 37–53 (2018)
16. Tanwar, S., Thakkar, K., Thakor, R., Singh, P.K.: M-Tesla-based security assessment in wireless sensor network. Proc. Comput. Sci. **132**, 1154–1162 (2018)
17. Kumar, H., Singh, P.K.: Comparison and analysis on artificial intelligence based data aggregation techniques in wireless sensor networks. Proc. Comput. Sci. **132**, 498–506 (2018). https://doi.org/10.1016/j.procs.2018.05.002

Intelligent Applications of WSN in the World: A Technological and Literary Background

Reinaldo Padilha França(✉), Yuzo Iano, Ana Carolina Borges Monteiro, and Rangel Arthur

School of Electrical and Computer Engineering (FEEC), University of Campinas – UNICAMP, Avenue Albert Einstein – 400, Barão Geraldo, Campinas, SP, Brazil
{padilha, monteiro, yuzo}@decom.fee.unicamp.com

Abstract. Where Wireless Sensor Networks (WSNs) have been widely considered to be an important technology in the 21st century, the group of specialized devices or sensors that are used to monitor different environmental conditions and collect and organize this data at some central location, detect and measure the number of physical conditions such as humidity, temperature, sound, pressure, speed and direction, chemical concentrations, vibrations, pollutant levels. As a tremendous application ranging from monitoring, surveillance, forest fire detection, and many other applications, it is, therefore, a promising technology for achieving energy-efficient, reliable and cost-effective flawless monitoring and control in smart grids. state-of-the-art infrastructure for greater efficiency, reliability, and security with harmonious integration of renewable energy and alternative energy sources through automation control and modern communication techniques. Advances in the field of communication networking are becoming a very interesting and challenging area of networking, with sensors deployed in everyday objects to capture everyday information such as humidity, temperature, heartbeat, motion, and others. With these sensors and microcomputers, the object for integrating the Internet set of things (IoT), becoming intelligent objects. Therefore, this chapter aims to provide an overview of the WSN application in the smart grid, in intelligent transportation, in smart homes, in the same way as Smart Agriculture, and the joint use with IoT and Smart Cities, showing and approaching its success relation, with a concise bibliographic background, categorizing and synthesizing the potential of both technologies.

Keywords: WSN · Smart homes · Smart Agriculture · Node · Sensor

1 Introduction

Due to technological innovations in the fields of wireless communication, digital electronics, and micro-electro-mechanical systems, the world has seen a revolution in remote, focused and concentrated sensing for the development of wireless sensor networks (WSN). Wireless sensor networks (WSN) are a powerful monitoring tool in today's world, where this technology has been contributing from monitoring difficult-to-access locations to industrial process automation and is employed whenever network

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 13–34, 2020.
https://doi.org/10.1007/978-3-030-40305-8_2

cabling is complicated or difficult. high cost. Which can be characterized by the use of a large number of sensor nodes with the ability to communicate, where such nodes can be placed within or near the phenomenon to be analyzed, unlike traditional sensor networks, where the positions The relative values of each node are not predetermined or pre-calculated, they are random, since the deployment of sensor networks in hard-to-reach locations, and the nodes over the region to be analyzed [1].

The sensor node are standalone devices equipped with sensing, processing and communication capabilities, which implements the physical monitoring of an environmental phenomenon, which varies greatly by application, which generates measurement reports via wireless communication; which produces a measurable response to changes in physical conditions such as brightness, temperature, motion, humidity, magnetic field, among others. They can be understood as small and extremely basic computers in terms of interface and components, consisting of a processing unit with limited capacity, reduced memory, one or more sensors that pick up and recognize certain signals, a communication device, generally radio and a source of energy. When these nodes are networked in an ad-hoc mode, they form sensor networks, collecting data via sensors, processing locally or coordinated between neighbors, and transmitting this information, with tasks such as environment sensing, information processing, and tasks associated with it. traffic, among others [2–4].

Ad hoc networks are wireless networks that do not require the use of a common access point to the device connected to it, so that all devices on the network function as if they were a router, routinely routing information that comes from neighboring devices, as shown in Fig. 1 [3, 4].

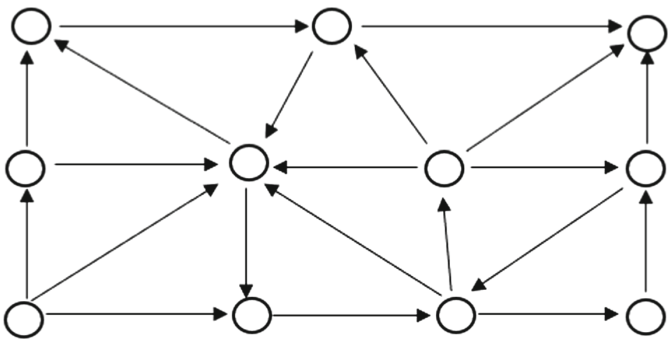


Fig. 1. Ad-hoc concept

Thus, each node consists of sensor devices that have some computational power - memory and processor, which will be responsible for the operation of applications and the retransmission of messages throughout the network. In addition, they communicate over a wireless interface and have a certain power range, usually powered by batteries [2–4].

Conceptually, a WSN is composed of three basic entities which are sensor, observer and phenomenon, where based on the monitoring problem can be solved

using sensors scattered in an area await the occurrence of a phenomenon whose alert will be sent to an observer (be Police, Firefighters, Hospital, among others.) [3, 5, 6].

The technology behind WSN nodes is basically ultra-low-power embedded systems with sensing and communication capabilities (RF, IR, Ultrasound, etc.), which form a communication network, usually independent of a usual infrastructure; with their elements scattered/thrown at the place of interest; where the number of elements can be tens, hundreds or thousands of sensors. Therefore, these positions in these particular places of interest should be addressed by the communication and network management protocols, making these protocols a vast field for research, and communication between these nodes is done through an ad-hoc wireless network, where one node is transmitting the sensing values to another node nearby. This next node should be in charge of passing the data to the next node, and so on. The idea is to take advantage of devices so small and relatively inexpensive that they can be used on a large scale [7, 8].

In addition to sensing, sensors perform data processing and communication between components. WSN features improvements over traditional sensors, which feature hardware with computational power, need and processing power; along with signal acquisition, digital-analog conversion; energy acquisition and management, still counting on low consumption; its sensors have communication and efficiency, spectrum use and low consumption; synchronous medium access; routing techniques; data collection and sending [3, 8, 9].

Sensors can be positioned away from the event to be monitored, leading to large and complex sensors. Where many sensors are placed close to the event to be monitored, only sending the values to a processing center, which requires a very careful study of the communication topology and proper methods for each application should be developed. In a common WSN architecture, measurement nodes are deployed to acquire measurements such as temperature, voltage, or even dissolved oxygen. Where nodes are part of a gateway-managed wireless network that governs aspects of the network such as client authentication and data security. This gateway collects the measured data on each node and sends it over a wired connection, typically Ethernet, to a host controller. The idea is to take advantage of devices that are so small and inexpensive that they can be used on such a large scale to enable many different types of applications [10–12].

A WSN is by nature data-centric, unlike traditional address-centric networks, but similar in this respect to faithful bus-type wired networks, such as a CAN, where a node broadcasts/requests attribute-based information (either temperature range, vibration levels, spatial location, speed limit, among others). Also having a feature that sensor nodes are expected to meet specific application requirements, it is common to meet a single attribute or, at most, a few combined attributes (detection of a vehicle on the street, or at an intersection, being attributes speed and direction), which will imply processing capacity within the network. Another feature, also derived from the low price per sensor and, consequently, its high availability, will certainly be the formation of dense and very large-scale networks, with little care and installation costs, generating a saturated distribution of nodes present in a given environment. monitor/analyze a particular aspect, taking advantage of a high degree of redundancy and availability [3, 13, 14].

Whereby linking high availability and data orientation it is possible to generate data aggregation on sensor nodes determined by interactions located between nodes sharing the same neighborhood and programmed to reduce traffic, resulting in energy savings, being possible to coordinate sensing and direct interests; data propagation by interest, restricting or directing data transmission according to rules and based on previously cached data; path reinforcement mechanisms, with rules for deciding when and how to enforce propagation messages [14, 15].

WSN has been attracting a lot of attention because of the challenges and the wide variety of possible applications, research and investments in the area are constantly growing, allowing the evolution of the technologies involved. Where the pursuit of ever smaller and lighter sensors draws studies to the search for technologies and protocols that allow sensors to communicate more and more efficiently, use less and less power and require less and less processing power [3, 14, 15].

Therefore, this chapter aims to provide an updated review of Wireless Sensor Network, showing and approaching its success relation, with a concise bibliographic background, categorizing and synthesizing the potential of both technologies.

2 Methodology

This study was based on the research of **66** scientific articles and books that address the theme of the present work, exploring mainly a historical review and applicability of techniques related to Wireless Sensor Network (WSN). These papers were analyzed based on the publication date of fewer than 5 years, with emphasis on publications with date greater than 2014 as well as publications and indexing in renowned databases, such as IEEE and Scholar Google.

3 Results

A Wireless Sensor Network is a wireless network consisting of spatially distributed standalone devices that use sensors to monitor physical or environmental conditions. These standalone devices, or nodes, are used with routers and a gateway to creating a typical WSN system where these distributed metering nodes communicate (wirelessly) with a central gateway which provides a wired world connection where you can measure, process, analyze and present your collected data. To increase the distance and reliability of a wireless sensor network, it is possible to use routers for an additional communication link between the end nodes and the gateway [3, 16].

WSN can be defined as a communication network formed by autonomous, spatially distributed sensing devices, cooperating in the monitoring of physical or environmental variables. Being the devices in this network presenting great memory, processing capacity and communication bandwidth constraint. The expansion of this technology was catalyzed by the cost reduction of microcontrollers, the miniaturization of RF transceivers, and the development of miniaturized sensors by MEMS (Micro Electro-Mechanical Systems) technology. Related to the battery life of network devices, being essential in home and building automation applications, having less importance in

industrial automation, and with features that the nodes are powered by the power grid. It has the benefit of cable elimination, which contributes to reduced installation cost while still considering fault tolerance characteristics and increased coverage when new nodes are inserted [17, 18].

The **communication** between two nodes is performed using radiofrequency, where a node sends a message in the middle and all nodes within range can receive it, we call this technique Broadcast. This type of communication is very influenced by the geography of the place, and messages may be lost. Sensor nodes can be configured to transmit information periodically or by exception and routers must always be active to forward messages. While sensor nodes must meet application-specific requirements, very often nodes focus on just one attribute, or a small set of attributes, and thus require processing within the network. The restrictions imposed on the wireless sensor network imply a series of requirements for communication protocols never before encountered at such a scale, and as a consequence of their characteristics, network management and communication protocols must have self-organizing capabilities promptly [15].

Sensor nodes must be inexpensive and small in size, which makes them unreliable, so the network must be fault-tolerant. Failures can occur for a variety of reasons: power outages, lack of visibility to another network node, or physical damage, and the network must be able to perform its tasks even with the loss of some nodes. Fault tolerance levels will determine different network control algorithms. Where your level of **fault tolerance** will depend on the environment and application, the network control algorithm also depends on these same factors [15, 19].

The fact that nodes have low cost and minimized size as their basic attributes contribute to the formation of dense networks and results in **scalability**, requiring little care and installation costs. With dense networks, a high degree of data redundancy and availability is achieved, which can be seen as a problem, but one that we should take advantage of. Thus, data aggregation on sensor nodes is of great importance for energy savings, through reduction of traffic, for example, coordination of sensing and targeting of interests, being determined by interactions located between nodes that share the same neighborhood. Some typical functions of sensor nodes are determining the value of a parameter at a given location; event detection and estimation parameter values as a function of the detected event; classification of a detected object; trace of an object. Thus, WSNs have obvious advantages over wired networks because they eliminate high cabling costs and can be deployed in hard-to-reach locations over the area to be analyzed [19–21].

WSN has a large number of nodes due to its related production cost to make installing such a network feasible and preferable over a traditional sensor network. **Energy** is seen as the crucial factor in a WSN, as power sources are limited, since sensors are microelectronic devices, sensor nodes must cooperate with each other in order to transport data efficiently in terms of spending power. Communication is the main energy consumer, with data transmission consuming even more than reception. Thus, one should also explore local adaptive algorithms that are not based on interaction or global information, avoiding energy expenditure by handling a very large information load [22].

Nodes should automatically adapt to the environment and can be dormant when not needed to save energy, as well as become operational and may need to automatically

rearrange themselves in case of loss or even destruction. any of them or in case new sensors are added to the network. Some techniques used to reduce node energy consumption are sensor cluster formation, sensor computational load reduction, efficient protocols, low-power circuits, dormant node sleep, and local energy production (with piezoelectric transducers, solar cells, magnetic fields), as shown in Fig. 2 [3, 15, 23].

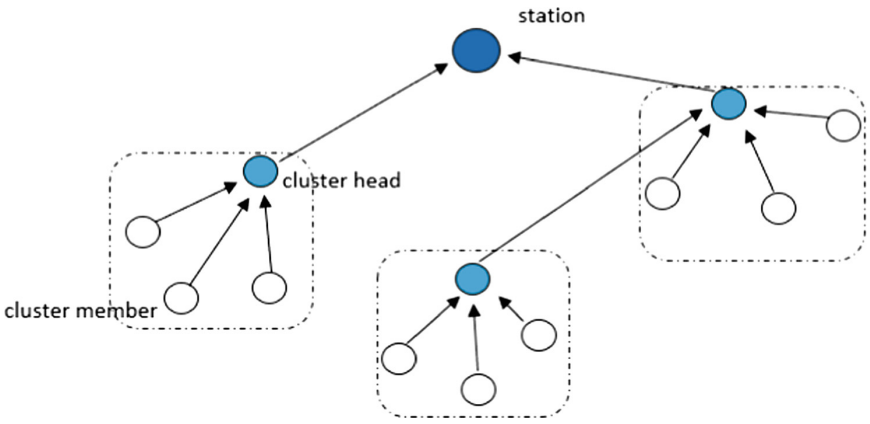


Fig. 2. Cluster formation

Since in the formation of these clusters, the nodes are distributed in clusters or node trees, which are formed according to some clustering algorithm. In each cluster there is a cluster head, being a head node to which the other nodes send their data, so the head nodes are the ones that send the data to the final destination, which is called the base station. This technique allows the reduction of energy use because nodes that transmit data to the cluster head spend very little energy due to the short distance between these nodes. However, cluster heads use a lot of energy, where the practice is to do a cluster heads rotation, so that nodes spend on average the same amount of energy [15, 24].

4 Network Topologies

In a common WSN architecture, measurement nodes are deployed to acquire measurements such as temperature, voltage, etc. Thus, a network topology is the channel in which the network medium is connected to nodes and other components of a network [25].

The first and most basic topology is the **star**, where each node maintains a single path of direct communication with the gateway, which is a simple topology, but restricts the total distance the network can reach, as shown in Fig. 3 [3, 25].

Where to increase the distance a network can reach, it is possible to implement a **cluster** or **tree** topology, as shown in Fig. 4. In this more complex architecture, each node maintains a unique path to the gateway, but can use other nodes to route data along that path. However, this topology has a disadvantage where if a router node loses

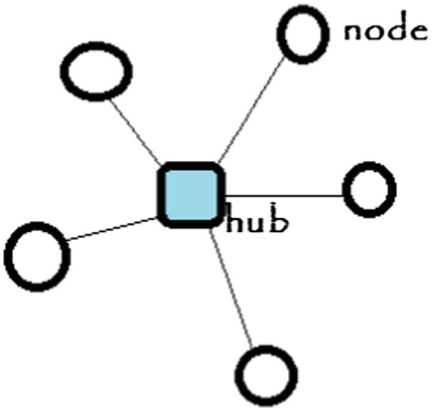


Fig. 3. Topology star

communication, all nodes that depend on that router node will lose their communication path with the gateway [3, 26].

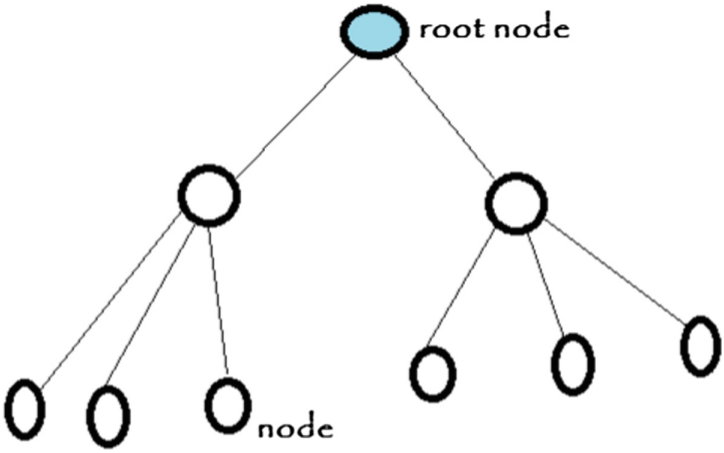


Fig. 4. Topology tree

The **mesh** topology remedies this problem by using redundant communication paths to increase system reliability, where nodes maintain multiple communication paths with the gateway, so that if a router node loses communication, the network automatically redirects the data in a different way, as shown in Fig. 5. In a mesh topology, while very reliable, it suffers from increased network latency, as data must make multiple hops before reaching the gateway [3, 27].

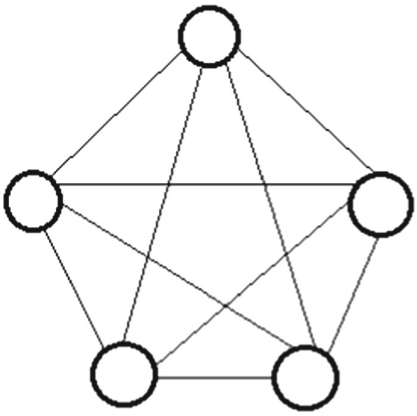


Fig. 5. Topology mesh

5 Wireless Sensor Network Applications

Wireless sensor networks have numerous possible applications, which is a great incentive for research in this area to continue. Nowadays, every day, the tendency is for the WSN to be used in the most varied places, more and more applications for its use appearing, being present many of the present-day applications of these networks. WSN has very flexible coverage, new sensor nodes can be added to the network already in operation to compensate for defective nodes or even to extend the network coverage area, without the need for a pre-existing infrastructure. Component mobility is an important feature, of great influence on issues such as energy consumption and data transmission, where it can be classified as **mobile** having wildlife monitoring applications, sea level measurements or even applications. in biomedicine; as well as **static**, with applications such as forest climate analysis, motion sensors forming a security perimeter, among others [29, 30].

The advent of WSN has enabled applications previously considered unfeasible or even impossible, a clear example is in the application as monitoring in remote or high-risk areas of industries, or the case of collecting physiological data from the ox for a better quality of meat produced. It's component mobility, autonomy, and self-organization, flexibility, fault tolerance, ability to add more sensors to the network, are positive points along with the characteristics that lead us to believe that the concept has revolutionized monitoring, tracking, coordination and control. processing in different contexts. The most common application of sensors is to measure environmental conditions such as temperature, pressure, humidity, and weather or ground conditions, but they are also widely used to monitor movement, control speeds and detect hazardous materials [31–33].

Wireless Sensor Networks can be used, for monitoring various characteristics of **natural environments**, such as those described in the example of a forest reserve, where for this type of monitoring, it usually deals with very large places or difficult access, the installation costs. and maintenance of a conventional network will be much

higher than those of a WSN. In addition, the use of a wired network, which is much more "sensitive" to these environments, can be considered, as they can be easily damaged by agents such as tree roots in the case of forests; irregular relief conditions and dense vegetation are unfavorable for the installation of monitoring structures of these environments [29, 34].

Assisting in biodiversity mapping where a WSN spreads in a given environment makes it possible to detect animals and plants located in the region. Assisting in the combat and monitoring of animals, used in fighting hunting assisting in the control of these animals near extinction. Also assisting in fire detection where this sensor distribution allows fires to be detected in a short time and to be located immediately and accurately, allowing control of fires quickly before spreading over a very large area. By also detecting floods by using the same principle as described for fire detection, flooding can be controlled even in hard to reach places. As well as controlling environmental conditions by monitoring environmental factors such as the level of air or water pollution, the concentration of pesticides in the water and the temperature and humidity conditions [29, 34, 35].

Sensors of microscopic dimensions can be introduced into a patient's body, used in conjunction with **medicine**, and through them, it is possible to monitor vital functions such as heartbeat, blood pressure, or even detect the presence of certain substances in the bloodstream. In the near future, with these sensors constantly broadcasting their readings, all patients could be monitored through a central computer, making it unnecessary for a nurse or other person to frequently attend each patient's room [30, 36, 37].

Sensors installed on vehicles and on-road infrastructure are able to communicate, providing important data to **traffic** control agencies and even preventing accidents. And all the information sent from the cars and the track infrastructure can be used by the traffic control agencies to detect accidents and traffic jams and thereby control access to such roads to mitigate such situations [38].

Wireless Sensor Networks could secure and monitor shopping centers, homes and apartments to detect potential **safety** hazards for people in such locations, used to detect a high concentration of flammable gas in a particular room of the house, that would pose a risk of explosion, for example. WSN can also be used as a **control** function in industries by inserting sensors into parts for the purpose of error detection and **quality control**, or even by using sensors inside machines such as automobiles, monitoring their operation in a timely manner. practice, and trying to detect defects or malfunctions [39].

WSN is increasingly being used in homes, with **household applications** with diverse functions such as housekeeping automation by installing sensors in everyday equipment, automating common tasks such as lighting where light intensity sensors can turn off. The lights during the day and turn them on at night, the control of equipment such as refrigerators, microwave ovens, and air conditioners. As well as safety in the distribution of temperature and motion sensors throughout the house allows the detection of fires and invasions, as well as the control of movements of children and elderly through the house. Currently increasingly in the development of intelligent environments, where WSN allows the integration of various equipment in which sensors are installed, and can even control them by voice or telephone, the

communication between these devices, the integration of cameras This network allows residents to view what is happening in a particular location of the house as soon as any sensor detects any irregularities, even the integration of the telephone line allowing police, fire brigade or a hospital to be automatically notified in case of intrusions or accidents [40, 41].

Military sensor applications are quite common today, mainly because it is not possible to define a communication infrastructure during a war operation. In addition to the time requirement, installing a switch would make the network vulnerable, whereby destroying this switch would end the network. Thus, WSNs are used in C4ISRT systems that are synonymous with Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance, and Targeting. It can be focused on the location of soldiers, where sensors installed on soldiers' uniforms allow the center to monitor the position and movements of each soldier, and this monitoring can even be viewed by a battlefield commander through a viewfinder. Controlling equipment and ammunition by installing sensors on the equipment and weapons that soldiers carry makes it possible to control ammunition or other available equipment. Even in the recognition of enemies by spreading sensors on a battlefield, it is possible to monitor and map the movements of enemy troops. Together with the detection of nuclear, biological or chemical attacks due to ground sensing allow the detection of these types of attacks or mines installed in the region [42, 43].

Similarly, in **engineering**, WSN can be applied in construction, structural monitoring, and modeling, material control, product quality control. The retail **industry** has made use of this technology with the "Radio Frequency Identification tag" or smart tag (RFID), which would be a possible replacement for bar code technology where each RFID merchandise identifies itself, forming an updated directory of the establishment, which must have a reader radio [31, 32, 44].

In **agriculture** and livestock, WSN can be used in crop management, where levels of fertilizer or any other substance concentration, livestock control and water quality analysis can be done. In WSN **radiation monitoring** it is possible to establish monitoring and control over areas near nuclear plants, if there is a significant change in radiation level, it is possible to evacuate the area in advance, saving lives. As well as **aviation** assisting in air traffic control, aircraft monitoring such as fuel and altitude control, route tracking. And also, in **entertainment** in the development of toys and other equipment that interact with the environment [45–47].

6 Wireless Sensor Network Applications Architecture

A wireless sensor network can be classified according to two criteria basically as proactive or reactive. In proactive networks, sensors exchange information periodically. In reactive networks, information exchange occurs only when certain events are sensed. As for architecture, a network can be classified as flat or hierarchical. In flat networks, all sensors are similar, and in hierarchical networks, sensors have different characteristics, such as processing capacity, which makes the network architecture take these differences into account. Thus, a sensor with higher computational power can be used more than sensing and routing [25, 48].

A wireless sensor network does not require the definition of an infrastructure. Thus, the placement of nodes in the network can be random, as the nodes themselves are able to communicate and organize. The sensors can monitor a particular type of data and sending the information monitored by it or received from another node to one of the neighboring nodes. This communication between nodes is performed until the node called sink, which receives the information, being able to communicate with the task manager via the Internet or a satellite connection [49].

This multi-hop-based architecture is called a multi-hop, which allows for reduced power consumption in transmission, as it prevents all nodes on the network from having to transmit information directly to the sink node. Instead, nodes only need to broadcast to their neighbors. as shown in Fig. 6 [49, 50].

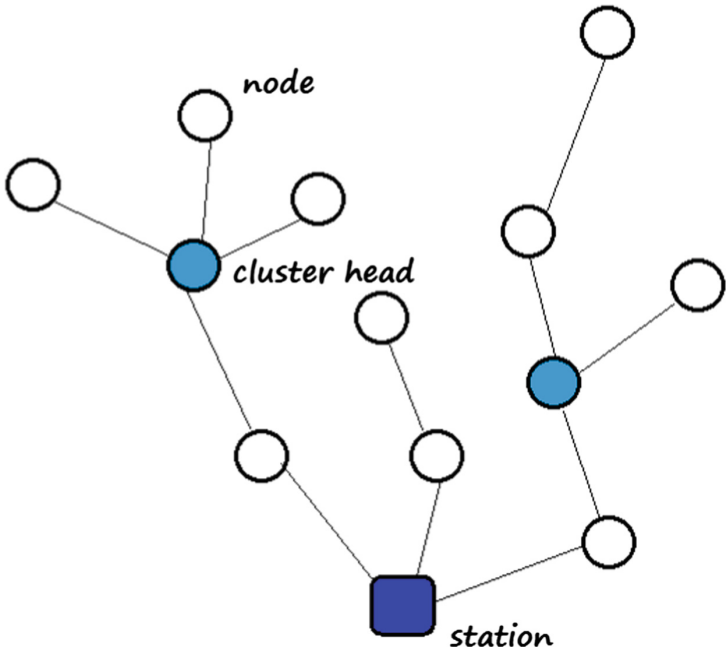


Fig. 6. Multi-hop

WSN has the feature that each node helps forward messages, where a node sends a message on the network, its neighboring nodes receive and, if necessary, resend to new neighbors, this approach is called multi-hop. This message exchange strategy has some problems, and if all nodes are subject to forwarding a message, this message can be repeated indefinitely in the network, thus flooding the network; otherwise, a node wants to send a message, but due to physical conditions or if the neighbors are not subject to forwarding it, the message will be lost [49–51].

Network nodes, sensors as well as the sink, use a series of protocols, which can be described in layers, similar to the OSI and TCP/IP reference models; physical, data

link, network, transport, and application layer. In addition to the layers, three power management, mobility management, and task management plans are defined, which are layer independent, as shown in Fig. 7 [3, 52].

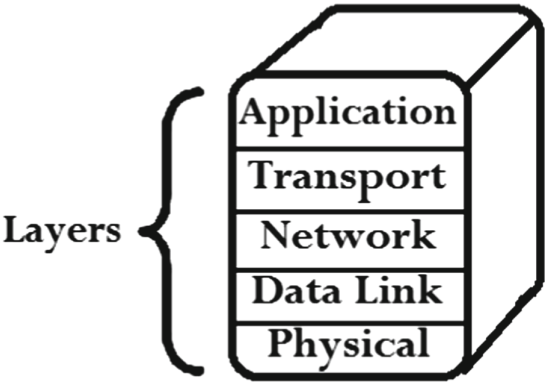


Fig. 7. Layers

Management plans are designed to enable sensors to work more efficiently, consume as little power as possible, manage the movement of sensors across the network as efficiently as possible, and share resources across the network, allowing sensors to actually work as one. network. Otherwise, there would simply be a set of sensors working individually, as shown in Fig. 8 [3, 52].

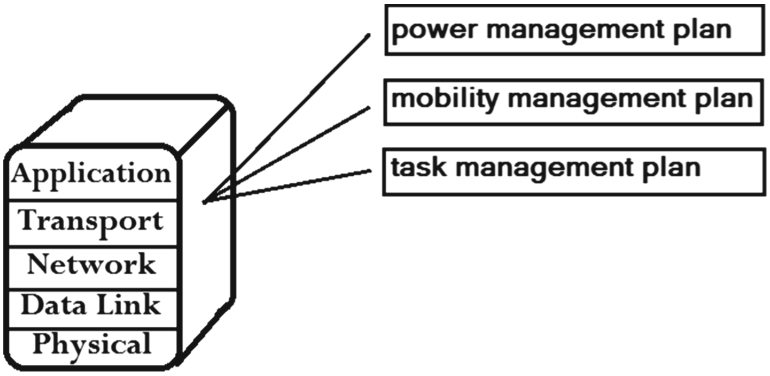


Fig. 8. Management plans

The **power management** plan is responsible for controlling the energy use of each sensor, acting when the power level is low, a sensor can send a broadcast message to inform the other sensors, because due to the multi-hop architecture. Some other sensor could use it to forward information to the sink node. Thus, when receiving this

message, the other sensors will look for an alternative path to the sink node, without passing through the low energy sensor, possibly generating a bottleneck. Another method for power saving would be to turn off the receiver after receiving a message, avoiding receiving the same message by another sensor and reducing power consumption [3, 15, 52].

The **Mobility Management Plan** is related to the need for sensors to know who their neighbors are, and to know a route to reach the sink node, because they are mobile, each sensor should always keep a list of neighboring sensors updated. Thus, it is possible to balance the energy consumption and the tasks performed. Because not all sensors need to perform sensing simultaneously, the **task management** plan works by staggering these tasks in specific regions, commonly the sensors with the most energy are chosen to perform these tasks more often than those with the highest energy level low [3, 15, 52].

The layers were defined with the purpose of allowing the isolation of tasks, thus determined application of a sensor can be defined independently of the transmission medium used. The task of the **physical layer** is the transmission of messages between sensors, being responsible for selecting the frequencies that will be used, generate the carrier, detect, modulate and encode the signal. Because minimizing power consumption is a major concern in a wireless sensor network, the physical layer must address issues that are common to any wireless transmission, such as signal reflection [3, 15, 52].

Important in a physical layer design in WSN is the choice of modulation type, binary or M-ary. In binary modulation, each symbol is represented by only one bit, representing only two levels, being more efficient because it consumes less energy. In M-ary modulation, M bits are used to represent 2M levels, respecting the relationship that the higher the value of M, the more complex and precise the circuits for modulation and detection, and the higher the power consumption. Communication between network sensors can use optical signals, infrared signals or radio frequency (RF) signals. Optical communication has the main advantage of lower power consumption than other technologies, just as RF requires a line of sight of the signal, in which the transmitter and receiver must be aligned, being sensitive to weather conditions [3, 15, 52].

Communication through RF signals is the most common. The main advantage is that, unlike optical and infrared communications, in this type of network the transmitter and receiver need not be aligned. The receiver only needs to be close enough to the transmitter that the power level is sufficient to decode the correctly transmitted signals. The only disadvantage is that radio communication is extremely sensitive to noise caused by handsets operating in the same frequency range, and many frequency ranges are already used by various services [53].

The task performed by the **data link layer**, in addition to media access control (MAC), is under error control, frame detection and data flow multiplexing. Because WSNs do not require the prior definition of an infrastructure, the sensors must have some mechanism that allows the identification of other sensors in the network. Since sensors are free to move around the network, the MAC is responsible for establishing multi-hop communication as a way of organizing the network and establishing routes,

as is the distribution of transmission media among sensors that are part of the network [53, 54].

Protocols are the ones that control the operation and the main characteristics of the network, being responsible for the formation and control of network applications; where they must also take into account the characteristics imposed by wireless communication: such as great attenuation, and the characteristics of the channel vary with time, high error rate and the various signal reflections that arrive at the receiver in different phases. With the emergence and increase of wireless sensor networks, it has become increasingly important to choose protocols that aim to reduce energy consumption and network security. Thus, there is no rule regarding the use of protocols, usually, these are chosen according to the needs of the project involved [13].

Through various protocols such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), EAR (Eavesdrop-And-Register), SMACS (Self-Organizing Medium Access Control for Sensor Networks) and a TDMA(Time Division Multiple Access)/FDMA (Frequency Division Multiple Access) hybrid, the most common is CSMA, also used in the Ethernet standard, with a collision avoidance mechanism, more precisely CSMA/CA [13, 16, 55].

CDMA is a system that allows the separation of signals that coincide in time and frequency, where all signals share the same frequency spectrum, each signal being encoded by a user-specific code and spread over the entire width. Bandwidth as noise to all users. Signal identification and demodulation occur at the receiver when a replica of the code used for spreading each signal in the transmission is applied, thus returning with the signal of interest, while discarding all other signals as interference [56–58].

CSMA/CA consists of listening to the medium before sending a packet, a way to avoid collisions and consequently the retransmission of packets, which has the characteristic of avoiding collisions by using a random waiting time for access to the medium, called back-off time. Still considering the existence of two types of spaces between frames, SIFS (Short Inter-Frame Space) and DIFS (Distributed Inter-Frame Space), the first being the time between sending a packet and receiving the ACK of this packet from the source having a longer duration than SIFS; and the second is related to the time at the end of transmission, which is divided into small slots, where devices interested in sending files access the medium, both of which are multiples of the time of each slot [56, 57, 59].

TDMA is the media occupancy time being divided between media-using devices, where each device has a time x to transmit a frame, after which time transmission ceases and the next device has its turn to access the medium. Thus, this cycle time is the number of devices present in the middle times the size of the time window (x), at the end of transmission the same device can only access the medium in a new cycle [56, 57, 60].

FDMA is characterized by the allocation of different spectrum bands to channels, it is the most common method of access, especially among analog systems. Where the spectrum is divided into channels where each subscriber tunes to their bearer, thus the information of a propagating channel does not interfere with that propagated in another parallel, where the number of channels in the system will be a function of the width of each channel [56, 57, 61].

SMACS is used to initiate and organize the network link layer, where the nodes can randomly choose any frequency to operate, forming communication between the nodes without the need for the main node, where they will communicate intermittently and can automatically shut down. save energy when there is no data to transmit, and thus build a flat topology, which does not require clusters or major nodes [13, 16, 25, 56, 57].

EAR enables communication between mobile and static nodes, using broadcast to recognize their neighboring nodes, by fixed leasing of dual time slots at a fixed frequency, taking advantage of the fact that the available bandwidth is much larger than the sensory data bandwidth, and still considering the random wake up time plus turning off the radio when idle. Error control is also a very important data link layer task, allowing the retransmission of data that was not received correctly, usually due to transmission errors, which is more common in wireless networks [13, 16, 25, 56, 57].

The main protocols used in WSN are Automatic Repeat Request (ARQ) and Forward Error Correction (FEC); being the first, the receiver sends acknowledgment messages of type ACK when it receives a packet correctly and NAK when it detects the loss of a packet, thus the transmitter is informed of the errors that occur in the transmission, resending the packets in which there were errors; and the second use error-correcting codes and transmits redundant data, reducing the likelihood of errors occurring, and when they do occur, they can be corrected. However, packet size is greatly increased due to the corrector codes entered in the header and the redundant data transmitted [13, 16, 25].

The **network layer** is responsible for data routing between sensors, and the routing protocols used must support multi-hop communication, always seeking the most efficient use of sensor energy. Where the choice of the most efficient route between a sensor that wishes to transmit a message and the sink node can take into account several criteria, for example, if sensor A has detected a bottleneck event and wants to send this information to the sink node, this sensor can use multiple routes [56, 57].

The applications of a WSN in the **application layer** vary for each case, and several applications can be defined in this layer, from those exemplified in this chapter as those aiming at the application of new services. Sensor Management Protocol (SMP) is designed to manage WSN applications by isolating them from the lower layers. The main tasks are sensor clustering; sensor management by moving, turning on or off; network reconfiguration after changes in sensor status; performing safety-related tasks [13, 16, 25, 56, 57].

The task of the Task Assignment and Data Advertisement Protocol (TADAP) is to distribute user interests among sensors, where users may wish to be informed of the occurrence of certain events, or the state of the sensors at a certain time interval, or only of a specific set of sensors; also informing the user of the availability of new data on any network sensor. Sensor Query and Data Dissemination Protocol (SQDDP) focuses on the user interface for querying network sensors. These queries are not limited to a specific sensor, but to a set of sensors in a region that you want to monitor and may also refer to a specific event. One application using this protocol is Sensor Query and Task Language (SQTL), which defines three events for the application: receive, every, and expire [25, 56, 57].

Thus, in a sensor network, the protocol is responsible for managing communication in general, both between the sensor nodes, and between the network and the outside world. The protocol is critical, as simply adding nodes to the network can be disruptive to the entire system, requiring the protocol to intelligently manage communication to prevent and correct congestion and to balance a load of information generated. And the efficiency of this communication protocol varies according to the network topology and its application. There are several types of protocols, the most common being the IEEE 802.11 (WiFi), IEEE 802.15.1 (BlueTooth), and IEEE 802.15.4 (ZigBee) standards. Because it has a good range with low implementation complexity and low power consumption, the ZigBee standard is the most economical and is, therefore, most commonly used in sensor nodes today [13, 56, 57].

Routing protocols for flat networks are Directed Diffusion; SPIN (Sensor Protocol for Information via Negotiation); Sequential Assignment Routing (SAR); Adaptive Local Routing Cooperative Signal Processing: Noncoherent; Processing and Coherent Processing and similarly there are routing protocols for hierarchical networks which are LEACH (Low Energy Adaptive Clustering Hierarchy); CBRP (Cluster Based Routing Protocol); TEEN (Threshold-sensitive Energy Efficient Network); APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient Network); PEGASIS (Power Efficient Gathering in Sensor Information System) [13, 25, 56, 57].

Among the most commonly used routing protocols for WSN is **Directed Diffusion**, where the node to transmit names the data using attributes, a pair of them, that describe the task to be performed. The base station (sink) propagates your interests, which attributes you want to receive. Neighboring nodes propagate this information, which, when passing through the nodes, fills a gradient field, i.e., the distance traveled, and when it arrives at a node containing the attribute of interest, it sends it through the gradient path to base station, with no prior identification of nodes in the network [13, 56, 57].

The **SAR** performs multi-hop routing using tables by which it selects multiple paths, avoiding overhead in case of failure. It creates several trees, the root of which is next to the base station. It bases the choice of the path to use according to available power resources, QoS and the priority of the packet to be sent, through a weighted metric between these factors. Trees, which form the multiple paths, avoid problem nodes and can send their messages through one of several available trees [13].

SPIN is a family of adaptive protocols for sensor networks, so nodes use descriptors, called metadata, to name their data. Rather than spreading data across the network, they spread metadata, which is smaller in size than the data itself, addressing the problem of power shortages. It also has resource management, allowing you to make decisions so as not to waste an amount of energy that can lead to the node shutdown. SPIN work with three types of ADV (Advertisement) messages being the message that the sensor spreads containing the metadata; REQ, being the message that a neighboring node sends to the sensor that spread the ADV message, when the metadata contained in that ADV interests him and DATA, being the message itself, that the node, which sent the ADV, sends to the node that returned the message REQ [13].

LEACH is an energy-efficient protocol for non-mobile networks, using a cluster-based architecture where nodes that are part of a cluster send their data only to that cluster's root node, cluster-head. This cluster-head aggregates the data from each

sensor in the cluster, treating redundant information, and sending this data to the base station. To solve the problem of power failure, there is a rotation of cluster heads, considering the time allocation of different nodes as cluster heads of a given cluster, having a more uniform energy expenditure between the nodes and also preventing the loss of a cluster-head leads to network disruption, this communication being done through TDMA [13].

It is also possible to classify by cooperative and multi-hop network routing, where multi-hop protocols used in ad-hoc networks are not good for sensor networks, although they can be used for some reasons such as low battery charge and memory availability, and so Routing table size becomes large, and does not support cooperative dissemination as well as merging or aggregating data [55, 56].

As discussed above, an old routing technique is broadcast-based flooding, with the idea that sensor nodes propagate their information to all their broadcast neighbors, and these neighbors do the same thing with the information until it reaches the sink Being immune to changes in network topology, but can cause high overhead, still considering two very common flooding problems, such as implosion and overlap. In the first one node receives the same message, by two different neighbors; and in the second, two nodes, acting in the same field of observation, eventually detect the same situation and generate the same message and both propagate to a common neighbor. Still analyzing that in flooding the sensors can, instead of using broadcast, communicate directly with the sink, through multi-hop routing or with a cluster-head, using unicast message, in an attempt to reduce overhead, and may also use data aggregation [55, 56].

There is gossiping, which is a derivation of flooding, where instead of broadcasting the message, the node transmits it to a randomly chosen neighbor node, and so on, until it reaches the sink, thus avoiding implosion, but it takes a long time for information to travel the network [55, 56].

7 Wireless Sensor Network Limitations

Each WSN node consists of an electronic device with relative processing power, a sensor, and a battery, the latter having to guarantee a viable life, being considered one of the limitations in WSN. One of the biggest problems in power management in WSN, in the case of a cooperative model, is its asymmetry in the data flow, where the nodes closest to the sink tend to spend more energy because in addition to fulfilling the sensing functions are responsible for relay a larger flow of information [3, 62].

Due to the dynamic nature of WSN, its power limitations and transmission range, related to its energy autonomy, and because they are generally in harsh environments, it is necessary to look for the best communication infrastructure to ensure the best combination of performance, robustness, efficiency and lowest cost possible. An alternative considered for optimizing communication in a WSN is the fusion or aggregation of data from different sensor nodes, since one effect resulting from a large number of sensors is redundant data transmission and collisions. In this way, the benefits from fusion would be greater read accuracy, making the network less vulnerable to single sensor failures and inaccuracies; coupled with energy savings as the number of messages that need to be transmitted is reduced [3, 63].

In an attempt to assign greater reliability WSN is about using redundancies, where nodes that perform the same function and then cross over the obtained data, having a way to decrease the delay is overusing error-correcting codes avoiding retransmission. However, there is the disadvantage of the possibility of reducing the precision and robustness of the WSN application. Since WSNs implemented in critical locations that require a high degree of accuracy should be sufficiently reliable to avoid failures and/or delays, resulting in the safety of the application [3, 64].

The processing power and therefore the size of the WSN node can be affected by increasing the processing capacity of each node where more data will pass through and be transmitted by WSN making it able to perform even more costly processing tasks. Thus, in order to reduce the processing capacity of each node, it is necessary for each device to process the information collected by the node itself, as well as the information that comes to it from other nodes, thus the processors used, by their low. Computational power has its own operating systems, but it is possible that there are some nodes within a network that have a slightly higher processing power than the others, which are then scaled to head nodes [3, 65].

Security in WSN that has very limited resources and the most varied security needs, where it varies according to applications from those with little need (for remote environment monitoring, there are no network confidentiality requirements) to those most in need (industrial application where sensor data can be used by competitors). Common requirements are data integrity, confidentiality, node and data authenticity, network availability, and ensuring that data is recent, since simple data encryption and possible signature addition to packages can either increase or ruin the performance of a WSN [3, 66].

8 Conclusions

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed standalone devices that use sensors to monitor physical or environmental conditions. These standalone devices, or nodes, are used with routers and a gateway to creating a typical WSN system. Distributed measurement nodes communicate (wirelessly) with a central gateway which provides a wired world connection where it is possible to measure, process, analyze and present the collected data.

To increase the distance and reliability of a wireless sensor network, routers can be employed for an additional communication link between the end nodes and the gateway. The wireless protocol selected for one is dependent on the requirements of your application. A WSN system is ideal for an environmental monitoring application whose requirements require long-term data acquisition to measure water, soil or climate characteristics. For utilities such as utility power, street lighting, and water distribution, wireless sensors offer a cost-effective method for collecting system health data, reducing power consumption and improving resource management. In the health monitoring of structures, it is possible to use wireless sensors to effectively monitor highways, bridges, and tunnels. These systems can be deployed to continuously monitor commercial buildings, hospitals, airports, factories, power plants, and production facilities.

Managing the sensor environment with large deployment of intelligent and autonomous sensor numbers is a complex task where cognitive sensor networks are used to obtain localized information. Like holes, considered a communication gap between sensor nodes, deploying WSNs over a large area is one of the increasingly present challenges. Still, when it comes to WSN time synchronization gathering the clocks of the clock sensor nodes, the challenge will be to design a lightweight, fault-tolerant, energy-efficient protocol to minimize power consumption [67].

As a trend there will be the application of low power wireless protocols is increasing where a future is expected in which wireless devices such as health monitoring sensors will be ubiquitous. Just as it will lead to increased interference and congestion within and between sensor networks due to overlapping physical frequencies, approaches to cognitive radios and multi-frequency MACs should be developed using various communication frequencies. Just as underwater sensors will also be further used in the exploration of underwater natural resources such as oceanographic data collection, pollution monitoring, exploration and disaster prevention applications and scientific data collection. As well as new generations of distributed embedded systems represented by WSNs will be developed with a focus on a broad real-time application horizon, ranging from border surveillance, medical assistance, and highway traffic coordination to fire monitoring, overcoming the limitations of resources in highly dynamic environments [67].

Given the broad applicability and great potential of this technique, more academic and industry research must be undertaken to develop more cost-effective and inactive technologies. Only by reducing the cost of existing methodologies is it possible to bring quality of life to underprivileged populations, whether through medical devices related to the transmission of medical data or related to the monitoring of more violent areas.

References

1. Miettinen, M., Asokan, N.: Ad-hoc key agreement: a brief history and the challenges ahead. Comput. Commun. **131**, 32–34 (2018)
2. Shaikh, F.K., Zeadally, S.: Energy harvesting in wireless sensor networks: a comprehensive review. Renew. Sustain. Energy Rev. **55**, 1041–1054 (2016)
3. Pathan, A.K. (ed.): Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. CRC Press, New York (2016)
4. Papadopoulos, G.Z., et al.: Performance evaluation methods in ad hoc and wireless sensor networks: a literature study. IEEE Commun. Mag. **54**(1), 122–128 (2016)
5. Liang, S.H.L.: Sensor networks, the sensor web, and the Internet of Things. In: International Encyclopedia of Geography: People, the Earth, Environment and Technology: People, the Earth, Environment and Technology, pp. 1–17 (2016)
6. Khan, I., et al.: Wireless sensor network virtualization: a survey. IEEE Commun. Surv. Tutor. **18**(1), 553–576 (2015)
7. Al-Suhail, G.A., Mehdi, J., Nikolakopoulos, G.: A practical survey on wireless sensor network platforms. J. Commun. Technol. Electron. Comput. Sci. **13**, 23–30 (2017)

8. Kaur, H., Sharad, S.: UWDBCSN analysis during node replication attack in WSN. In: Handbook of Research on Information Security in Biomedical Signal Processing. IGI Global, pp. 210–227 (2018)
9. Singh, S., Sharma, S.R.: Localization system optimization in wireless sensor networks (LSO-WSN). In: Handbook of Research on Wireless Sensor Network Trends, Technologies, and Applications. IGI Global, pp. 1–34 (2017)
10. Mohamed, S.M., Haitham, S.H., Iman, A.S.: Coverage in mobile wireless sensor networks (M-WSN): a survey. Comput. Commun. **110**, 133–150 (2017)
11. Yang, L., et al.: Survey and study on intelligent monitoring and health management for large civil structure. Int. J. Intell. Robot. Appl. **3**, 239–254 (2019)
12. Oladimeji, M.O.: Computational intelligence algorithms for optimisation of wireless sensor networks. Dissertation London South Bank University (2017)
13. Ray, N.K., Ashok, K.T. (eds.): Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures. IGI Global, Hershey (2016)
14. Yang, X., Dengteng, D., Meifeng, L.: An overview of routing protocols on wireless sensor network. In: 4th International Conference on Computer Science and Network Technology (ICCSNT), vol. 1. IEEE (2015)
15. Kumar, A.: Energy efficient clustering algorithm for wireless sensor network. Doctoral Dissertation, Lovely Professional University (2017)
16. Ilyas, M., Imad, M.: Smart Dust: Sensor Network Applications. Architecture and Design. CRC Press, New York (2018)
17. Yetgin, H., et al.: A survey of network lifetime maximization techniques in wireless sensor networks. IEEE Commun. Surv. Tutor. **19**(2), 828–854 (2017)
18. Sabato, A., Niezrecki, C., Fortino, G.: Wireless MEMS-based accelerometer sensor boards for structural vibration monitoring: a review. IEEE Sens. J. **17**(2), 226–235 (2016)
19. Sarangapani, J.: Wireless Ad Hoc and Sensor Networks: Protocols, Performance, and Control. CRC Press, New York (2017)
20. Yang, C., et al.: Big-sensing-data curation for the cloud is coming: a promise of scalable cloud-data-center mitigation for next-generation IoT and wireless sensor networks. IEEE Consumer Electron. Mag. **6**(4), 48–56 (2017)
21. Vasuhi, S., Vaidehi, V.: Target tracking using interactive multiple model for wireless sensor network. Inf. Fusion **27**, 41–53 (2016)
22. Warrier, M.M., Kumar, A.: An energy efficient approach for routing in wireless sensor networks. Procedia Technol. **25**, 520–527 (2016)
23. Shu, T., et al.: An energy-efficient dual prediction scheme using LMS filter and LSTM in wireless sensor networks for environment monitoring. IEEE IoT J. (2019)
24. Xia, H., Zhang, R.H., Yu, J., Pan, Z.K.: Energy-efficient routing algorithm based on unequal clustering and connected graph in wireless sensor networks. Int. J. Wirel. Inf. Netw. **23**(2), 141–150 (2016)
25. Xu, Q., Zhao, J.: A WSN architecture based on SDN. In: 4th International Conference on Information Systems and Computing Technology, Atlantis Press (2016)
26. Acharyya, I.S., Al-Anbuky, A., Sivaramakrishnan, S.: Software-defined sensor networks: towards flexible architecture supported by virtualization. In: Global IoT Summit (GIoTS). IEEE (2019)
27. Iqbal, M., et al.: Hybrid tree-like mesh topology as new wireless sensor network platform. Telkomnika **14**(3) (2016)
28. Bera, S., et al.: Soft-WSN: software-defined WSN management system for IoT applications. IEEE Syst. J. **12**(3), 2074–2081 (2016)

29. Toldov, V., Laurent, C., Mitton, N.: Multi-channel distributed MAC protocol for WSN-based wildlife monitoring. In: 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE (2018)
30. David, D.S., Jeyachandran, A: A comprehensive survey of security mechanisms in healthcare applications. In: International Conference on Communication and Electronics Systems (ICCES). IEEE (2016)
31. Li, X., et al.: A review of industrial wireless networks in the context of industry 4.0. Wirel. Netw. **23**(1), 23–41 (2017)
32. Xu, L.D., Xu, E.L., Ling, L.: Industry 4.0: state of the art and future trends. Int. J. Prod. Res. **56**(8), 2941–2962 (2018)
33. Chaulya, S., Prasad, G.M.: Sensing and Monitoring Technologies for Mines and Hazardous Areas: Monitoring and Prediction Technologies. Elsevier, Amsterdam (2016)
34. Olasupo, T.O., et al.: Empirical path loss models for wireless sensor network deployments in short and tall natural grass environments. IEEE Trans. Antennas Propag. **64**(9), 4012–4021 (2016)
35. Borra, S., Rohit, T., Nilanjan, D.: Applied examples. In: Satellite Image Analysis: Clustering and Classification, pp. 83–97. Springer, Singapore (2019)
36. Chia-Hui, L., Yu-Fang, C.: Secure user authentication scheme for wireless healthcare sensor networks. Comput. Electr. Eng. **59**, 250–261 (2017)
37. Alvarez, F., et al.: Behavior analysis through multimodal sensing for care of Parkinson's and Alzheimer's patients. IEEE Multimed. **25**(1), 14–25 (2018)
38. Ghaffari, A.: Congestion control mechanisms in wireless sensor networks: a survey. J. Netw. Comput. Appl. **52**, 101–115 (2015)
39. Hammoudeh, M.: Applying wireless sensor networks to solve real-world problems. In: Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication. ACM (2015)
40. Pirbhulal, S., et al.: A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors **17**(1), 69 (2017)
41. Nisar, K., et al.: Smart home for elderly living using wireless sensor networks and an android application. In: IEEE 10th International Conference on Application of Information and Communication Technologies (AICT). IEEE (2016)
42. Ahmad, I., Khalil, S., Saif, U.: Military applications using wireless sensor networks: a survey. Int. J. Eng. Sci. **6**(6), 7039 (2016)
43. Ismail, M.N., et al.: Establishing a soldier wireless sensor network (WSN) communication for military operation monitoring. Int. J. Inf. Commun. Technol. **7**, 89–95 (2018)
44. Asici, T.Z., et al.: Applying model driven engineering techniques to the development of contiki-based IoT systems. In: Proceedings of the 1st International Workshop on Software Engineering Research & Practices for the Internet of Things. IEEE Press (2019)
45. Banđur, Đ., et al.: An analysis of energy efficiency in wireless sensor networks (WSNs) applied in smart agriculture. Comput. Electron. Agric. **156**, 500–507 (2019)
46. Venkatesh, G., Chandramouli, P.: An IOT based environmental radiation monitoring through wireless sensors network. HELIX **8**(1), 2753–2756 (2018)
47. Olson, J.S., Redkar, S.: A survey of wearable sensor networks in health and entertainment. MOJ App. Bio. Biomech. **2**(5), 280–287 (2018)
48. Kumar, A.: Energy efficient clustering algorithm for wireless sensor network. Dissertation, Lovely Professional University (2017)
49. Silberschatz, A., Gagne, G., Galvin, P.B.: Operating System Concepts. Wiley, Hoboken (2018)
50. Arioua, M., et al.: Multi-hop cluster based routing approach for wireless sensor networks. Procedia Comput. Sci. **83**, 584–591 (2016)

51. Ramezan, G., Cyril, L., Zhen, J.W.: A survey of secure routing protocols in multi-hop cellular networks. IEEE Commun. Surv. Tutor. **20**(4), 3510–3541 (2018)
52. Fahmy, H.M.A.: Wireless Sensor Networks. Concepts, Applications, Experimentation and Analysis, vol. 52. Springer, Berlin (2016)
53. Le-Giang, T., Hyouk-Kyu, C., Woo-Tae, P.: RF power harvesting: a review on designing methodologies and applications. Micro Nano Syst. Lett. **5**(1), 14 (2017)
54. Navaz, A.S.S., Kadhar, G.M.N.: Layer orient time domain density estimation technique based channel assignment in tree structure wireless sensor networks for fast data collection. Int. J. Eng. Technol. **8**(3), 1506–1512 (2016)
55. Wang, J., et al.: On MAC optimization for large-scale wireless sensor network. Wirel. Netw. **22**(6), 1877–1889 (2016)
56. Selmic, R.R., Phoha, V.V., Serwadda, A.: WSN architecture. In: Wireless Sensor Networks, pp. 37–81. Springer, Cham (2016)
57. Selmic, R.R., Phoha, V.V., Serwadda, A.: Wireless Sensor Networks. Springer, Berlin (2016)
58. Okawa, T., Hiromasa, H.: Rigorous communication success probability of MC-CDMA with MPOMS codes for radio-on-demand WSN. In: IEEE 6th Global Conference on Consumer Electronics (GCCE). IEEE (2017)
59. De Guglielmo, D., et al.: Accurate and Efficient Modelling of IEEE 802.15. 4 unslotted CSMA/CA through event chains computation, pp. 2954–2968 (2016)
60. Alvi, A.N., et al.: BEST-MAC: bitmap-assisted efficient and scalable TDMA-based WSN MAC protocol for smart cities. IEEE Access **4**, 312–322 (2016)
61. Abd El-Rahman, A.F., et al.: Companding techniques for SC-FDMA and sensor network applications. Int. J. Electron. Lett., 1–15 (2019)
62. Rashid, B., Rehmani, M.H.: Applications of wireless sensor networks for urban areas: a survey. J. Netw. Comput. Appl. **60**, 192–219 (2016)
63. Kumar, M.S., et al.: Quality improvement techniques in WSN: a review (2016)
64. Chiumento, A., Marchetti, N., Macaluso, I.: Energy efficient WSN: a cross-layer graph signal processing solution to information redundancy. arXiv preprint arXiv:1906.10453 (2019)
65. Al-Turjman, F.: Cognitive-node architecture and a deployment strategy for the future WSNs. Mobile Netw. Appl. 1–19 (2017)
66. Pandey, S.V., Raju, K.S.: Secure and efficient DiDrip protocol for improving performance of WSNs. Int. J. Adv. Eng. Manag. Sci. **2**(5) (2016)
67. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2019)

Medium Access Control Protocols for Wireless Sensor Networks

Prashant R. Rothe[1] and Jyoti P. Rothe[2(✉)]

[1] Priyadarshini College of Engineering, Nagpur, India
p_rrothe@rediffmail.com
[2] St.Vincent Palloti College of Engineering, Nagpur, India
j_p_rothe@yahoo.co.in

Abstract. In wireless networks communication between sensor nodes is performed using a sole channel i.e. air. This channel has the characteristic that only one node is able to broadcast a message at any instant of time. Therefore this prevalent transmission medium should be allocated to each one of the nodes in an honest way. For accomplishing this purpose, a medium access control protocol is used. The goal of the medium access control protocol is to control access to the common wireless medium so that the concerned demands of the underlying operation are fulfilled.

In devising MAC protocols for common access medium the main complexity comes up due to spatial allotment of the nodes. To identify the node that is able to ingress the medium instantaneously, node has to transfer certain correlating details among them. However it requires employment of the transmission channel himself. This will increase the complexity of the protocol and as a result the overhead required to control access of the nodes to the medium.

Also immediate status of other nodes cannot be identified by the node under consideration because of the spatial distribution. The intellect of the verdict by the protocol along with the overhead employed, affect the overall performance of a distributed multiple access protocol.

Deciding the type and level of information utilized by a multiple access protocol is not easy assignment. The information is predetermined, dynamic global, or local. Predetermined and dynamic global information cause the wonderful coordination amongst the nodes. But, a high price is to be paid in the form of misused channel capability. Employment of local details will decrease the overhead needed to manage the nodes however the net performance of the protocol is reduced. The balancing among the overhead required and efficiency of medium access control protocol are the basis of the majority of the access techniques.

In Sect. 1 an introduction to MAC protocol is given and is followed by background for design of MAC protocol in Sect. 2. Section 3 gives fundamentals and performance requirements of MAC protocol. Section 4 illustrates some MAC protocols for the wireless networks. Section 5 depicts about IEEE 802.15.4WPAN standard.

Keywords: MAC protocol · Delay · Throughput · Energy efficiency · Schedule-based protocols · Contention based protocols

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 35–51, 2020.
https://doi.org/10.1007/978-3-030-40305-8_3

1 Introduction

In wireless networks communication is accomplished through the common transmission medium i.e. air. This general communication channel should be allocated to every one of the sensor nodes in an honest way. To realize this objective, a MAC protocol is used. The selection of MAC protocol is the key parameter for evaluating the wireless sensor network function. Many MAC protocols have been advised for WSNs.

2 Background

A unique channel that is used for communication among wireless sensor nodes has the characteristic that merely a particular node can send out a message at particular moment. Hence, for the collaborative access of transmission medium a MAC protocol must be set up between the nodes. The function of medium access control protocol is to control ingress of the sensor nodes for shared channel so that the functional needs of the concerned purpose are fulfilled [1, 2].

Against the viewpoint of the open systems interconnection model, medium access control protocol functions are offered by lower sub layer of the data link layer (DLL). The MAC sub layer exists over the physical layer and performs the functions mentioned below:

- It assembles data in the form of frame for communication by adding a header field which hold address details as well as trailer field used for detecting the error.
- It disassembles a obtained frame to take out address and error control instructions to carry out address identification and error detection.
- To control access for common communication channel to support the performance of the application (Fig. 1).

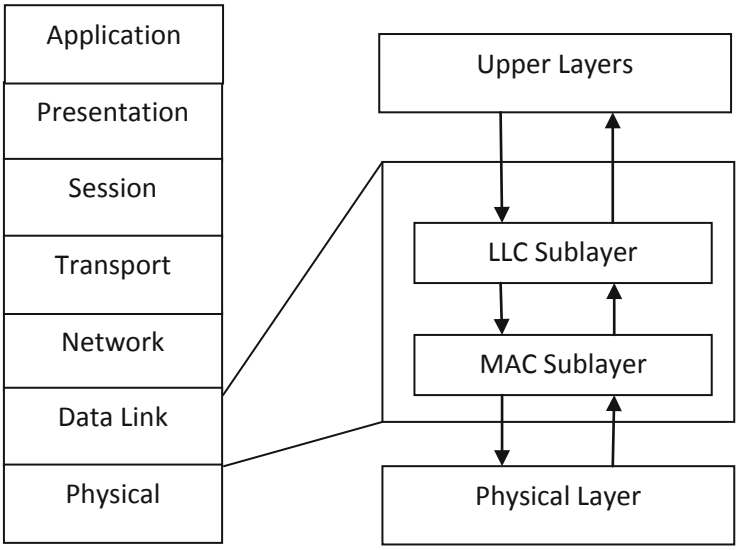


Fig. 1. OSI model with composition of DLL composition

3 Fundamentals of Mac Protocols

The spatial distribution of the nodes creates significant problem in proposing medium access control protocol. Part of coordinating data must be shared to decide a particular node that is able to access transmission medium at a particular instant of time. However this necessitates use of the communication channel itself which will increase the complication of the protocol and consequently, the overhead needed to control access between the nodes.

In the network a particular sensor node doesn't perceive instant status of another node due to spatial distribution. The working of a protocol is affected by the intellect of choice made by the protocol and the overhead incurred.

It is a difficult task to determine the nature of information utilized by MAC protocol. The information is of three types namely predetermined, dynamic global and local. Information of Predetermined type is familiar to every broadcasting node whereas dynamic global information is obtained by various sensor motes all through protocol working and local information is familiar to every node. Dynamic global and predetermined information is advantageous in excellent coordination between the nodes. But, a extra price is to be paid in form of misused channel capacity. The adoption of local information will decrease the overhead needed to manage the nodes, however will cause reduced overall performance of protocol. The balancing among the efficiency of medium access protocol along with the overhead needed to attain it is the foundation of the majority of the access methods.

3.1 Performance Requirements

The design of MAC protocols involves the issues like delay, throughput, stability, robustness, fairness and scalability [3].

1. **Delay:** The time for which data packet remain in the MAC layer prior to its faithful transmission is called Delay. The amount of delay relies on traffic and structure of the medium access control protocol. In case of time-sensitive purposes, the MAC protocol provides two forms of delay-bound guarantees namely probabilistic and deterministic [4]. Probabilistic delay guarantees are described by three factors namely an expected value, confidence interval and variance. Deterministic delay guarantees provides a certain amount of state transitions amid arrival and transmission of message. Hence, deterministic MAC systems assure an upper bound in case of the access time. In case of real time situations the accuracy is dependent on completion of the primary tasks within the specified time. Therefore determinism is a critical requirement.
2. **Throughput:** The rate by what messages are transmitted by system is referred as throughput. It is evaluated in messages per second. In the case of wireless communication it indicates part of the channel capability utilized for transmission of data. There are two aim's of a medium access control protocol first is to increase the channel throughput while second is to reduce the message delay.
3. **Robustness:** The measure of inattentiveness of the protocol to errors and incorrect information is referred as robustness. It takes care of error confinement and error

detection, reconfiguration and restart. In wireless sensor network it is difficult to accomplish robustness as it is based on the collapse models of communicating nodes and communicating links.

4. **Scalability:** It is the capability of a network to handle a growing amount of work. Scalability can be achieved by avoiding the dependence on globally consistent network states. The highly scalable shared medium access protocols are designed by grouping sensor nodes into clusters. By collecting particulars out of various sensors traffic patterns are evolved that are employed to scale medium access control protocol.
5. **Stability:** It is the measure of the capacity of the communication network to tackle changes in traffic over a specific time period. If the protocol can handle the instantaneous load which is larger than the maximum sustained load then it is said to be a stable protocol. The stability of a MAC protocol is defined analogous to delay and throughput. In case of MAC protocol if message waiting period is bounded then it is believed to be stable with regard to delay. Similarly if throughput isn't crumble as the load presented is increased then MAC protocol is believed stable with regard to throughput.
6. **Fairness:** If a MAC protocol allocates the channel capacity equally between the competing nodes with no decrease in the network throughput then it is considered to be fair. Fairness of MAC protocol is necessary to attain equitable quality of service and avert conditions where few nodes perform superior than others. Therefore none of the application is starved unnecessarily.

Energy Efficiency

In wireless sensor networks the energy conservation is important to extend the lifetime of nodes. Therefore energy efficiency is a vital issue in designing the MAC protocol. Number of sources contributes to energy inefficiency in MAC-layer protocols.

(1) Collision: It occurs when two or more sensor nodes try to transmit the data simultaneously. In this case the data packet gets corrupted and the need to retransmit a packet increases energy consumption.
(2) Idle listening: This occurs when a sensor node is listening for a traffic that has been not sent. The energy wasted in monitoring a silent channel is high in many sensor network applications.
(3) Overhearing: It occurs when a sensor node receives packets that are destined to other nodes.
(4) Control packet overhead: Access to the transmission channel is regulated by the control packets. If large numbers of control packet are transmitted as compare to the data packets conveyed then less energy efficiency is indicated.
(5) Frequent switching: Repeated switching among different operating modes cause considerable energy consumption. For example by restricting the number of changeovers among the sleep and active modes, considerable energy saving can be achieved.

The heterogeneous stable election protocol (HetSEP) was used by for prolonging the network lifetime [5].

3.2 Common Protocols

Number of strategies has been recommended for answering a difficulty of allocating access to the common channel. These strategies are broadly divided into three classes namely fixed, demand plus random assignment protocols.

Fixed-Assignment Protocols: For these protocols every mote is assigned a predecided secured quantity of channel. Every mote utilizes its assigned channel resource devoid of comparing along with another node. Frequency-division multiple access (FDMA), time-division multiple access (TDMA), and code-division multiple access (CDMA) are some examples of this type [6].

CDMA: It is based on spread spectrum system which allows several communicating nodes to transmit at the same time. The systems which work on the principal of spread spectrum technique make use of frequency hopping (FH) or direct sequence (DS). The frequency-hopping spectrum systems uses narrowband carrier to modulate the data signal. Over the time this narrowband carrier hops from one frequency to another in a pseudorandom manner. The transmitting and receiving radios hopping patterns should be synchronized so that the signal is decoded correctly.

In DSSS systems the sequence of information being relayed is divided into minute parts. Then across the spectrum each part is allotted a unique frequency channel. At the transmitting node a data signal is combined with a chipping code. The chipping code is a higher-data-rate redundant bit pattern which boosts the opposition to obstruction of signal being transferred. It also raises chances of restoring initial data provided any of the bits are destructed all through communication process.

Demand Assignment Protocols: It was used for getting better utilization of the channel by assigning its capacity in a best possible way to contending nodes. These protocols overlook idle nodes and think about the nodes which are prepared to transmit. The channel is assigned to the selected node for a specific time.

These protocols needs command of network and logical control mechanisms. The network control mechanism is required to select a particular node from the competing nodes for access to the channel. The logical control is needed by the competing node for requesting access to the channel.

Demand assignment protocols are divided into two categories namely centralized (e.g. polling scheme) and distributed (e.g. reservation based scheme).

Polling Scheme: It is a commonly employed scheme in which a master node asks every slave that if it is having any data to transmit in a predetermined order. When the referred mote is having information to broadcast, it updates the controller about his intent to broadcast. The controller then assigns channel for prepared station that utilizes the entire data rate for transferring his data. When polled mote is not having any information for broadcast then it rejects controller's appeal following which controller continues probing the subsequent mote in network.

Advantage: All nodes have equal right to use the channel. High priority nodes were given preference by polling them frequently.

Drawback: The considerable amounts of overheads were occurred because of large number of queries from the controller to the nodes.

The reliability of controller determines the efficiency of the polling formats.

Reservation: In reservation based systems few slots are kept for transporting the reservation messages. These messages are called *minislots* since they are smaller than data packets. When the station has data to send then in this minislot it send a reservation message and thus requests for access to the channel.

In case of fixed-priority-oriented demand assignment, every node was allotted separate minislot. Whereas for packet demand assignment multiple access, nodes have to compete for ingress to a minislot with the help of distributed packet-based contention methods, like slotted ALOHA. On receiving the request the master prepares a transmission schedule and declares it to the slaves.

Random Assignment Protocols: These includes the protocols ALOHA, CSMA, CSMA/CD and CSMA/CA.

ALOHA

In ALOHA the channel access is asynchronous and it does not depend on the present action on channel. A mote transmits information when it is ready for transmission. Then the node waits for a time sufficient for the longest feasible return journey propagation period in network which equals to the duration taken by signal to move amid two farthest away network motes. In case communicating mote obtains the acknowledgement before this time period is pass then transmission is considered to be successful. The receiving node gives the acknowledgement after confirming the faithfulness of the data. If the acknowledgement is not received by the communicating node then data is believed to be lost. Usually the data is missing because of collisions or errors produced due to noise on the transmission medium. In this case the communicating node resends the data. When the total transmission bid surpasses a specific threshold value, the node stops retransmission of the data and declares a lethal error.

CSMA

There are two types of CSMA protocols namely nonpersistent CSMA and persistent CSMA. This classification is based on the method adopted to get hold of a free channel along with the approach adopted to delay in case of a active channel to turn into free. In case of the nonpersistent CSMA protocol, as a mote has packet for transfer, it initially check channel and decide if it is free or any other transmission is going on. If the channel is in unused state then the mote transfers its data instantly then stands by for receiving an acknowledgment.

If before cutoff time the acknowledgment is not received then the sending mote presumes loss of information. The loss of data packets occur because of collision as well as due to noise interference. The station once again plans for retransmission of lost information. In case channel is occupied, the transmitting mote "backs out" for an arbitrary time period following which it checks the channel once more. Based upon condition of channel, mote broadcasts its data packet when the transmission medium is free else goes into the back-out condition in case it is occupied. The procedure is continued till the information is transferred fruitfully.

Though nonpersistent CSMA protocol decreases conflict among packet transmissions but has the major drawback that a channel can turn to idle all through the back-

out time of a competing station. This will produce wastage of channel capacity and decrease throughput appreciably.

To beat limitations of nonpersistent CSMA, p-persistent CSMA protocol was developed. This protocol uses different method to get a free channel. In this arrangement when a node is all set to transfer a data packet it initially checks the channel and if it has not having any activity then mote broadcasts its data instantaneously. Else, when channel is occupied then the mote continuously carries on listening till it turns out to be free. Once the channel becomes free the transmission is performed instantly.

CSMA/CD

In CSMA/CD a communicating node can listen while transmitting. When the mote is having information to transmit then firstly it listens and check whether any transmission being continues on the channel. If the channel is idle then the transmitting node begins sending its data packets and starts monitoring the channel during transmission. If an obstructing signal is found over the channel, the node instantaneously abandons transmission. It will decrease the wastage of bandwidth because of collision. If a collision takes place then every competing node engaged in the collision hang around for arbitrary time duration before it try to resend the data packet. The probabilistic algorithm is used to determine the waiting time period of the colliding mote.

4 Medium Access Control Protocols for WSNs

The major purpose of MAC protocols is to reduce wastage of energy due to collisions, idle listening, overhearing, and excessive overhead. These protocols are divided into two groups: schedule based and contention based MAC-layer protocols.

In case of Schedule-based protocols access to the channel depends on a schedule. The sensor node can access the channel as per the schedule. Only one sensor node can access the channel at a particular moment. This is realized by pre allocation of assets to each sensor node. Contention-based MAC-layer protocols circumvent pre allocation of channel to each sensor. Instead, a particular radio channel is used by all nodes and allocated on demand. However collision results due to simultaneous attempts to access the channel. The major purpose of contention-based protocols is to reduce the incidence of collisions. To reduce energy consumption, it reduces the occurrence of a collision, minimize overhearing and control traffic overhead.

4.1 Schedule-Based Protocols

In these protocols a schedule regulates access to channel to avoid conflict among the motes. The main objective of schedule based protocols is to prolong the network lifetime by securing very high energy efficiency [7]. Scheduled-based protocols are analogous to a TDMA system in which the channel is partitioned into time slots, as shown in Fig. 2.

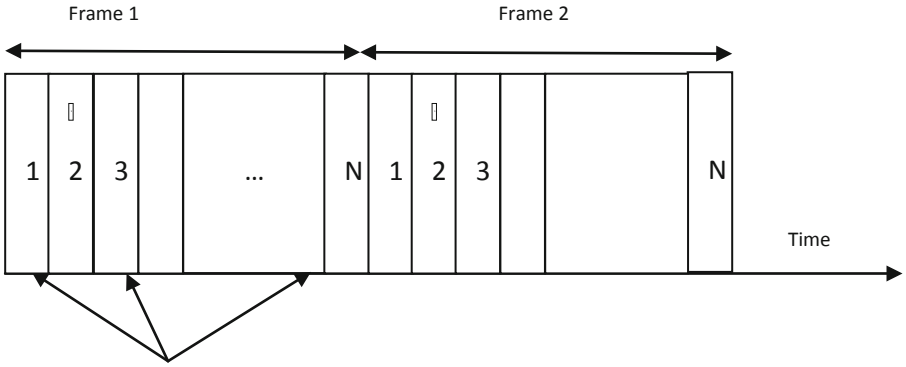


Fig. 2. Schedule-based MAC protocols

A group of N adjacent slots form logical frame which is repeated at regular intervals over time. Every node is allocated a group of specific time slots, in every logical frame. This set forms the schedule as per which the sensor node functions in every logical frame. Either the schedule is fixed or developed as per demand on a frame by frame ground by the base station, according to the present requisites of nodes and traffic pattern.

There are two modes of operation of a sensor node: active and sleep mode. In the event of active mode, the sensor node utilizes its allocated slots to transmit and receive data frames. Out of the allocated slots, sensor nodes go in sleep mode in which the node switch off its radio transceivers to save energy.

Self-Organizing Medium Access Control for Sensornets (SMACS)
It allows the formation of random network topologies without establishing global synchronization among the network nodes [8]. SMACS uses nonsynchronous scheduled communication that facilitates designing of links. For communication with known neighbors every node keeps a frame similar to time division multiple access, called a superframe. The length of a superframe is fixed but is further partitioned in shorter frames. The dimensions of every frame are not firm but can differ from one node to other. In SMACS every node routinely executes a neighborhood discovery process to identify nearby nodes. Every node set up a link to every identified neighbor by allocating a time slot in the link. The time slots are selected such that the node communicates to neighbor by node in every time slot.

It is required that a node and its neighbors should transmit in the same time slots therefore the link establishment procedure have to make sure that no intrusion takes place between the adjacent links. By means of the superframe structure, every node keeps its individual timeline with the neighboring nodes. To attain communication nodes must tune their radios to the appropriate frequency channel.

Bluetooth: It is developing technology in which access to the communication medium is managed by a federal TDMA dependent protocol [9]. It functions in the 2.45-GHz frequency band. It makes use of a pseudorandom frequency-hopping system having

1.6 kHz hopping frequency. It has 79 hop carriers having spacing of 1-MHz. Every hop sequence describes a Bluetooth channel that provides a throughput of 1 Mbps.

The cluster of devices that share a same channel is reffered as piconet. Each piconet consists of one master and utmost 7 slave devices. The master unit regulates access to the channel. Every channel is partitioned in slots of 625-ms. To every piconet an exclusive hopping frequency is allotted that was decided from address of master's Bluetooth device along with the clock. Every slave device follow its piconet allocated hopping sequence. Therefore the coexistence of various piconets is guaranteed since each piconets use different hopping sequences

A unique 3 bit internal address is given to each slave by the master device. Access to the channel is controlled with the help of slotted time-division duplex (TDD) protocol. To the slaves the timing slots are allotted by master device by using a polling protocol.

The Bluetooth frame which signifies a single polling epoch has 2 slots in which a packet is swap among the master and slave devices. For communication the master constantly polls the slaves. A slave device is able to communicate within a provided slot by the master if it has been addressed in a preceding time slot. In case of asynchronous communication a packet can be in excess of one slot long.

Bluetooth defines 4 operational modes to decrease consumption of energy. These modes are active, sniff, hold, and park mode. During active mode the master device deliver data packet to the slave. Then slave verifies the address and if packet hasn't its specific address, it sleeps in residual time period of packet transmission. But the planed slave stays active to take delivery of the packets in subsequent reserved slot. Sniff mode is utilized to decrease duty cycle of slaves listening. While operating in sniff mode, slave node hears master node transmission solely in particular slots. During sniff mode the slave node receive data packets from the master only in periodic slots that are defined in sniff time interval. Within the hold mode, a slave sleeps for a particular extent of time, called as hold time. After the completion of the hold time interval slave node come back to the active mode. Slave node sleeps for undefined time interval during park mode. Master node needs to wake up the slave node to fetch it in active mode for time to come.

Low-Energy Adaptive Clustering Hierarchy (LEACH)

LEACH uses a hierarchical methodology to group the nodes in the form of clusters. A cluster head exists in each cluster. The cluster head is responsible for forwarding the messages received from its cluster nodes to the base station.

LEACH employs TDMA scheme to have communication among the nodes and their cluster head [10, 11]. The cluster head constructs a TDMA plan and also transmits it to all the nodes within his cluster. This type of scheduling circumvents collisions between the data packets. The nodes make use of the schedule to decide the timing slots whereupon they have to be active. This permits every node in the group to shut down its radio components down to its allotted slots.

Direct-sequence spread spectrum (DSSS) is used for communications between a node and its cluster head. A peculiar spreading code is allotted to every cluster. This code is utilized by each node within a cluster to transmit its data to head of the cluster.

Once data packets are received by the cluster head from the nodes it will aggregate the received data prior to sending the data packets to base station. The head of the cluster then checks the channel to determine if any another head is presently transmitting the data. If the channel is full of activity then cluster head waits till the channel becomes idle. Finally the cluster head send the data by means of base station spreading code.

Following remarks are applicable to Schedule-based protocols.

(1) They are contention-free and avoid wastage of energy due to collisions.
(2) When data is to be transmitted or received then only the nodes will turn on its radio. For all other slots the nodes will turn off its radios which will avoid overhearing.
(3) This will cause low duty cycle operation of the nodes therefore the network lifetime is increased significantly.

Disadvantages of Schedule-based MAC protocols:

(1) The use of TDMA requires the grouping of nodes in the form of clusters. Such hierarchical arrangement limits peer-to-peer communication between the nodes.
(2) Schedule-based protocols depend on time synchronization to align slot boundaries which is difficult and costly to achieve among distributed sensor nodes.
(3) Schedule-based protocols needs added means like FDMA as well as CDMA to avoid inter cluster talk as well as impediment.
(4) A TDMA dependent MAC protocol has restricted scalability. They aren't freely compliant to mobility of nodes, network traffic changes and topology.

4.2 Random Access-Based Protocols

They are also called as contention-based protocols. In these protocols colliding nodes abandon for a random time period prior to trying to ingress the channel once again. However random based protocols are not fit for wireless sensor network. Performance of these protocols was improved by using the additional mechanisms such as collision avoidance, clear-to-send (CTS) and request-to-send (RTS). However collisions, overhearing, excessive control overhead and idle listening reduces the energy efficiency of contention-based MAC protocols.

PAMAS the power aware multi access protocol evades overhearing among neighboring nodes by using a separate signaling channel. STEM the sparse topology and energy management protocol trades latency for energy efficiency [12].

5 IEEE 802.15.4 LR-WPANs Standard

It was being used to provide the connectivity of many of wireless industrial and home usages. These usages need a extremely good technology that provides extended battery life.

This standard was accepted by the ZigBee Alliance for wireless personal area network technology [13]. Its reference model was presented in Fig. 3.

It indicates the different layers of architecture of ZigBee technology. These layers provide the features such as extremely low power consumption, low cost, consistent data transfer, and easy implementation that make ZigBee very attractive.

The physical layer (PHY) specifies the network interface components, their parameters and their operation. The PHY layer provide features like receiver energy detection (RED), link quality indicator (LQI), and clear channel assessment (CCA) to support the working of MAC layer.

In addition the PHY layer also furnishes the lower-power features comprising small-duty-cycle functions, stringent power management, and reduced transmission overhead.

The MAC layer uses two modes that is beaconing and nonbeaconing to control access to the medium. The beaconing mode is employed in the situations where consistently active devices perform data and control forwarding. The nonbeaconing mode utilizes unslotted nonpersistent CSMA MAC protocol.

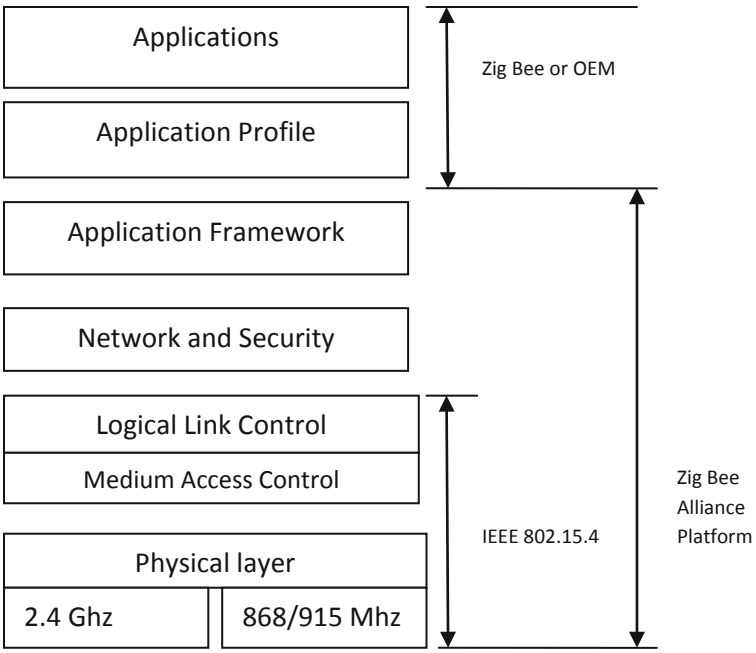


Fig. 3. The reference model of ZigBee architecture

Network layer offers utilities needed to sustain network configuration and device discovery, medium access control layer management, topology management, management of routing and security. It supports star, mesh, and cluster tree network topologies.

Basic security services specified by the IEEE 802.15.4 are furnished by the security layer. The first security service of the model gives backing for access control with the

help of which it stops entry of illegal individuals in network. The second security service is data message integrity protection, this stop the attacker from tampering a message during transit. In addition to these it offers data confidentiality that maintain the details transported by a message secret against the illegal persons with the help of advanced encryption standard (AES) algorithm. The fourth security facility provides sequential data freshness to prevent replay attacks. In this case an attacker secretly listening to the private conversation of others without their consent is prevented.

The application support sub layer maintains tables for combining devices collectively depending upon their services along with needs. ZDO perform overall device management, security keys as well as policies. It fixes the function of the devices within the network, initiating and responding to binding appeals and maintaining a secure relationship among devices in the network.

6 Current Endeavors

For hierarchical wireless sensor networks Ahmad Naseem Alvi and Safdar Hussain Bouk proposed an adaptive TDMA based medium access control (MAC) protocol, called bitmap-assisted shortest job first based MAC (BS-MAC) [14]. The BS-MAC provides several advantages: it employs minute time slots; the numeral of these time slots is larger than the numeral of member nodes, to schedule the time slots shortest job first algorithm is used, and member nodes are identified by short node address which is of 1 byte. The first two advantages manage the adaptive traffic loads of all members efficiently. The shortest job first algorithm decreases job completion time of the node and reduces the average packet delay. The tiny addresses of the nodes decreases the control overheads thereby making the system energy efficient.

In WSN for efficient routing between wireless nodes and sink discrete clustering techniques are proposed. These techniques partition the wireless sensor network in different groups referred as *clusters*. In every cluster one of the nodes is selected as a cluster head (CH) and remaining nodes acts as member nodes. The members have to communicate with the sink all the way through their concerned CH. The cluster setup phase takes place as follows. In the beginning of new round every node determines if to act as a cluster head for current round or not. This verdict is taken by stochastic algorithm. Probability that every node turns out to be a cluster head is 1/p, in which p indicates the desired % of CHs. If the node is selected as a cluster heads it will not become head till the remaining nodes become CH's. Then cluster head begins communication rounds. Every round consists of a *setup phase* (SP) and *steady state phase* (SSP).

A. Setup Phase (SP)
It consists of the steps mentioned below:

i. Cluster head relay CH Announcement (*CH_ANN*) message of 11 bytes consisting of 1 byte control portion, 8 byte CH's extended address along with 2 bytes frame check sequence.
ii. The CH_ANN message was listened by the nodes in the neighborhood of CH. These nodes then reply by sending join request signal of 19 bytes to CH. The

JOIN_REQ consists of a control byte, extended address of the node, extended address of the cluster head, and FCS.

iii. Cluster head waits for a particular period of time to obtain JOIN_REQs from every node in its communication range.
iv. Cluster head counts the received JOIN_REQs to determine the total number of member nodes and then allots a control slot to every node.
v. Cluster head uses 1 byte address to itself and to the connected members. Hence at the most 255 nodes can be connected with a single cluster head. After that cluster head allots individual control slot to every member and airs allotted control slot details to his members by way of CS_ALLOC message.

B. Steady State Phase (SSP)

In steady state phase source node cast *DATA_REQ* message during its assigned control slots. *DATA_REQ* contains the quantity of slots required by source node. However non-requesting nodes turn off their radios off to save energy. The cluster head stays in receiving mode throughout the whole control period for receiving DATA_*REQ* information from all source nodes.

At the end of control period, cluster head calculates the total of *DATA_REQ* messages. It has details of total quantity of data slots demanded by source nodes. Then cluster head apply shortest job first algorithm and updates every source node about its allotted data slots by transmitting allocated data slot announcement (*ADS_ANN*) signal.

Xin Yang and Ling Wang proposed a CSMA/CA- and time division multiple access dependent hybrid medium access control protocol (CTh-MAC) for 3-D mobile wireless sensor networks that increases energy efficiency [15]. Some of the characteristics of CTh-MAC are mentioned below.

(1) Based on the distance between sensor node and sink node all the nodes are allocated in several subsets using position prediction. (2) Then with the help of TDMA all subsets transmit data to sink node. In every subset, every sensor node contends for transmission using CSMA/CA scheme.

The CSMA/CA-TDMA protocol is having two methods. In one method the time slot is allocated to each subset by the sink node for communication purpose. In the second method depending upon the CSMA/CA scheme every node of the subset contending for transmission is allocated the channel.

The major function of TDMA scheme is to divide the subsets and allocate time slot to each subset for communication. Firstly the sink node transmits a wake up frame to every node. Then the sink transmits a preamble which consists of its coordinates along with the value of number of subsets m. After that each sensor node sends an information acknowledgement (IACK) signal to sink node. IACK signal consists of the information regarding whether the node has data to send, it's coordinate, and velocity vector. Each node sends IACK signal in the time division multiple access format subset-by-subset and by every mote. Then transmission of data starts in the time division multiple access formats. The outermost subset m initially communicates with the sink. During this time period all remaining subsets operates in relay mode whereby all nodes go into the sleep mode. After receiving data packets from the outer nodes a sensor node gets up to sends the data to inner nodes. This will improve the energy efficiency as well as convey transmission from external subsets to the sink node.

In every subset transmission slot is dependent on CSMA/CA; every node within subset competes for transmission to the sink node. In the beginning of slot, sink node transmits a wake up beacon to trigger every mote in the subset. The nodes which are having data for transmission will wake up and start contending. When the node wins it sends data to the sink node. Except for the node which was monitoring the channel all other nodes turn OFF to save energy. Once the node completes transmission with an acknowledge (ACK), another mote begins competing for the transmission. The major achievement of CTh-MAC is in the reduction of energy consumption in high-speed mobile transmission model.

In underwater sensor network (UWSN) sensors communicate with the help of acoustic signals. As compare to earthbound networks that uses radio and acoustic signals have long propagation delay, low available bandwidth, and high dynamic channels. These features present difficulties for protocol proposal in UWSNs. For UWSNs Faisal Abdulaziz Alfouzan and Alireza Shahrabi proposed a novel energy-conserving and collision-free depth-based layering MAC (DL-MAC) protocol [16].

DL-MAC addresses underwater medium access control problems like the near far effect, spatial temporal uncertainty as well as hidden terminal problems. The aquatic network region is separated in number of horizontal layers that are segregated in three kinds. Every type of layer is two layers apart from each other and each layer type is given separate frame. To evade chances of vertical collisions layers of same type are operated at the same time. Similarly to avoid horizontal conflict among the nodes in each layer-type, a distributed clustering methodology is used for one-hop neighboring nodes. With the help of these a Depth-based Layering MAC protocol is capable to resolve spatial-temporal uncertainty, hidden terminal problems and near-far effect.

DL-MAC consists of three phases namely updating, scheduling, and operational phase. The main objective of updating stage is to gather information about one-hop neighborhood nodes. This was executed by way of transferring g updating messages. Objective of scheduling stage was to allot a distinctive slot to each sensor. Each cluster head allot distinct time slots to his members which are one hop away from it. By the completion of scheduling phase each network sensor is allotted a different time slot; therefore no collision will occur. The operational phase consists of many cycles each of which consists of three frames. Every frame is made up of k sub frames. The frames along with sub-frames shun cluster interference. Every sub-frame consists of many time slots, equal to highest number of nodes in a one-hop neighborhood. Every sensor knows his reserved time slots and the time slots booked by his neighborhood sensors. Hence during the reserved time slots the sensor can be scheduled to wake-up either to transmit its own data or to receive a data from the neighborhood sensor. In the remaining time slots they are asleep.

DL-MAC addresses various problems of UWSNs and consequently conserves additional energy and improves the network lifetime.

Abdul Razaque and Khaled Elleithy proposed Scalable and efficient Medium Access Control (SEMAC) protocol for improving the functioning of (WSNs) [17]. The objective of proposed protocol was to lower the communication, channel and control delays produced due to acknowledgment packets. This is achieved by employing the adaptable application independent aggregation (AAIA) model. This protocol is having the handoff process feature to improve lifetime of the network.

The communication technique goes after the 1-hop destination. Within these technique preceding to sending the data every node transmits a short permeable that notify the 1-hop neighboring node to be prepared to receive the data. The communication lasts till receiver generates the handoff process. At the time a sender node desires to stop the communication or its energy is exhausting, then it includes flag in the last sent packets to update receiver regarding his present condition. On receiving the packet a receiver presumes that the communicating node is about to stop the communiqué else will suffer the loss of energy soon. It assists the receiver for selection of a different 1-hop neighboring node before this condition occurs. This process also helps to increase the network scalability.

The AAIA model exists between MAC sub-layer and network layer. It offers a cross-layered assistance for data aggregation. This model consists of Processing Unit, Aggregation Function Unit and Service Access Unit. Packet aggregation and de-aggregation was accomplished by the processing unit. The needed data aggregation is carried out by the service unit that manages timer setting. After the packets came out from network layer they are forwarded to processing unit that sends the packets to aggregation function unit. This unit applies the addressing methodologies to build the aggregate. Lastly the aggregated data is provided to medium access control sub-layer for transmission. The service access unit determines how many packets need to be aggregated (Fig. 4).

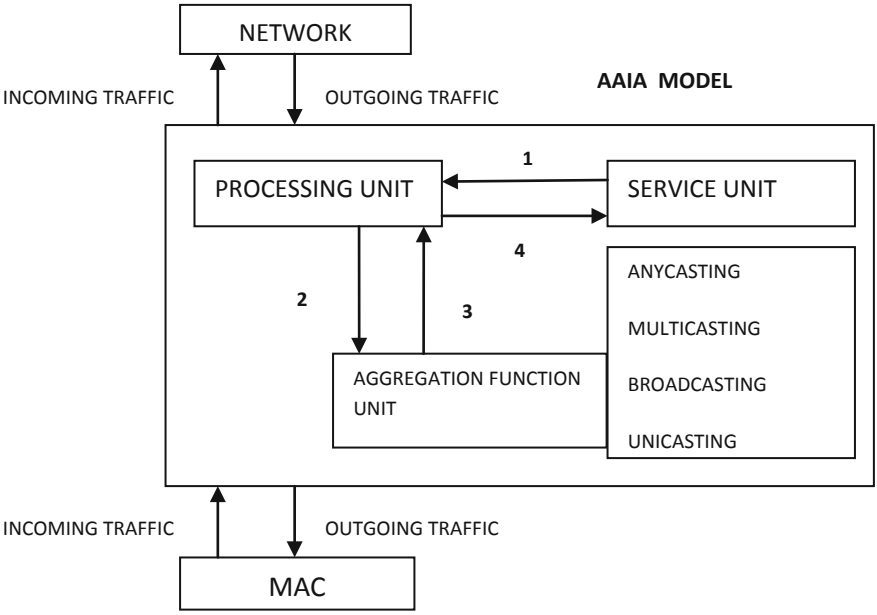


Fig. 4. Adaptive application independent aggregation model

The multiple network unit aggregation becomes a single aggregation to send the data that produces the decrease in channel, transmission and control overheads like RTS/CTS/ACK and acknowledgment. The compensation in contention time period on every transmission is provided by single aggregation.

7 Conclusion

Networking of sensor is forthcoming science having a broad variety of usages. The selection of the medium access control protocol is the key factor in deciding the performance of wireless sensor networks. Number of factors must be taken into consideration while designing an efficient MAC layer protocol. Usually sensor networks are powered by battery and it is not easy to alter or recharge these batteries on the nodes. Therefore a medium access control protocol for a wireless sensor network has to be energy efficient so as to increase the network lifetime. Further to harbour variations in the network size, network topology and node density the MAC protocol has to be scalable. Lastly the aspects such as fairness, bandwidth utilization, reduced latency and high throughput are as well significant features in the design of medium access control protocols for wireless sensor networks.

Several MAC layer protocols have been suggested for wireless sensor networks. In this chapter the design aspects of MAC protocol for wireless sensor network were discussed as well as the overview of these protocols was provided. The development of a MAC-layer protocol for WSN will continue to be an affair of concern. Also the latest progress in cognitive radio will bring an innovative context in the design of MAC protocol for wireless sensor networks.

Implementation platform also place limitations on the design of MAC protocols for WSN. These days, two prominent methods are being used for implementation. First is the use of microcontrollers and RF communication modules and second is implementation of entire system on a single chip. In the first method, the microcontroller runs a RTOS or a devoted software and communication protocols that manages the RF peripherals whereas in the another method all features and functionalities of WSN are implemented on a single chip.

References

1. Dam, T.V., Langendoen, K.: An adaptive energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems (SenSys 2003), Los Angeles, November 2003
2. Ding, J., Sivalingam, K., Kashyapa, R., Chuan, L.J.: A multi-layered architecture and protocols for large-scale wireless sensor networks. In: Proceedings of the IEEE 58th Vehicular Technology Conference (VTC 2003), October 2003, vol. 3, pp. 1443–1447 (2003)
3. Monks, J., Bharghavan, V., Hwu, W.-M.: A power controlled multiple access protocol for wireless packet networks. In: Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (InfoCom 2001), Anchorage, AK, April 2001

4. Bacco, G.D., et al.: A MAC protocol for delay-bounded applications in wireless sensor networks. In: Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop, June 2004
5. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
6. El-Hoiydi, A.: Spatial TDMA and CSMA with preamble sampling for low power adhoc wireless sensor networks. In: Proceedings of the 7th IEEE International Symposium on Computers and Communications (ISCC 2002), July 2002, pp. 685–692 (2002)
7. Lin, P., Qiao, C., Wang, X.: Medium access control with a dynamic duty cycle for sensor networks. In: IEEE Wireless Communications and Networking Conference (WCNC 2004), March 2004, vol. 3, pp. 1534–1539 (2004)
8. Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, G.J.: Protocols for self-organization of a wireless sensor network. IEEE Pers. Commun. **7**(5), 16–27 (2000)
9. Haartsen, J.C.: The Bluetooth radio system. IEEE Pers. Commun. **7**, 28–36 (2000)
10. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy efficient communication protocols for wireless microsensor networks. In: Proceedings of the 33rd Hawaii International Conference Systems Sciences (HICSS 2000), January 2000, Maui, HI, pp. 3005–3014 (2000)
11. Heinzelman, W., Sinha, A., Wang, A., Chandrakasan, A.: Energy-scalable algorithms and protocols for wireless microsensor networks. In: Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2000), June 2000
12. Schurgers, C., Tsiatsis, V., Ganeriwal, S., Srivastaval, M.: Optimizing sensor networks in the energy-latency-density design space. IEEE Trans. Mob. Comput. **1**(1), 70–80 (2002)
13. "ZigBee Specification," Document 053474r05, Version 1.0, ZigBee Alliance, Bishop Ranch, CA, 14 December 2004
14. Alvi, A.N., Bouk, S.H., Ahmed, S.H., Yaqub, M.A., Javaid, N., Kim, D.: Enhanced TDMA based MAC protocol for adaptive data control in wireless sensor networks. J. Commun. Netw. **17**(3), 247–255 (2015)
15. Yang, X., Wang, L., Su, J., Gong, Y.: Hybrid MAC protocol design for mobile wireless sensors networks. IEEE Sens. Lett. **2**(2), 1–4 (2018)
16. Razaque, A., Elleithy, K.: Scalable and energy efficient medium access control protocol for wireless sensor networks. In: IEEE Conference Long Island Systems, Applications and Technology (2015)
17. Alfouzan, F.A., Shahrabi, A., Ghoreyshi, S.M., Boutaleb, T.: An energy-conserving collision-free MAC protocol for underwater sensor networks. IEEE Access **7** (2019)

Performance of Energy and Distance Based Modified Threshold for LEACH

Remika Ngangbam[1(✉)], Ashraf Hossain[2], and Alok Shukla[3]

[1] Department of Electronics and Communication Engineering, National Institute of Technology, Mizoram, Aizawl 796012, India
ngangbamremika7@gmail.com
[2] Department of Electronics and Communication Engineering, National Institute of Technology, Silchar, Silchar 788010, India
ashrafiit@gmail.com
[3] Department of Physics, National Institute of Technology, Mizoram, Aizawl 796012, India
aloks.nitmz@gmail.com

Abstract. At present scenario wireless sensor network (WSN) occupies a major position in networking domain and it comprises of very tiny nodes in terms of thousands of numbers which are deployed in a specific region for determining the particular environmental condition. These sensor nodes have limited power and are irreplaceable once it has been deployed. Hence, saving power becomes an important factor to increase its lifetime. It has been observed that energy expenditure during transmission of data to base station or sink node directly is much larger than energy expenditure required for computations at senor nodes. Efficient energy consumption can be obtained by selecting proper cluster head since direct data transmission which is a heavy energy consumption process is performed by the cluster head. The authors propose the improvement of existing hierarchical, cluster based routing protocol LEACH. This chapter proposes a threshold condition for election of cluster head (CH) based on energy and distance and using this improved threshold LEACH provides better lifetime performance in comparison to existing LEACH and other LEACH associated protocols. The simulation result also shows that the modified threshold LEACH also exhibit satisfactory lifetime extension with change in density of nodes.

Keywords: Routing in WSN · LEACH · Lifetime of network · Cluster head election · Performance · Density

1 Introduction

Due to the fast development of microelectronics technology, advanced radio technology and sensors with great computational ability, wireless sensor network (WSN) makes a notable attention in networking domain. This sensor network basically comprises of specific number of nodes that can compute to high extent and can transmit and receive data among the nodes which are set out in the target region. These nodes perform the role of sensing the particular region, collecting the data, aggregating those data and transmitting it to destination like base station (BS) or sink node or to some

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 52–66, 2020.
https://doi.org/10.1007/978-3-030-40305-8_4

other nodes like cluster heads. The application of this type of network is increasing in many domains like agricultural application, medical systems, military purpose, industrial applications, etc. [1]. These nodes operate from the power source which is available in them or may be from some other renewable energy sources. Utilizing other power source rather than their own battery becomes a trade-off condition for cost and complexity factor in the system [2]. Hence, saving the limited power source of sensor nodes (battery) eventually comes out to be the most important matter to be considered.

WSNs face many challenges in the current scenario which include coverage problems, fault tolerance, quality of service (QoS), optimization of energy usage in the network, network lifetime, etc. Among these network problems and challenges data routing is one of the most serious issues that has to be considered since data transmission is directly related with lifetime of network [3]. Number of routing protocols have been developed to extend network lifetime [4] since replacing of battery is not feasible with lesser cost. Energy efficient routing protocol can also be obtained by using different types of data aggregation approaches [5]. Among all the routing protocols for extending network lifetime cluster based protocols are the leading protocols in the existing scenario [6, 8].

Cluster based routing protocol constitutes of two stages. In the first stage, dividing the whole network into clusters is performed by assembling the nodes into groups and electing leader (cluster head) for the particular cluster. This clustering process may be controlled by BS or some central node or it may be totally self organizing process [9]. After the cluster formation, data transmission will be carried out by nodes in the second stage participating in the clusters to the cluster heads and then passing the aggregated data to destination by head nodes of every cluster takes place. One of the most considerable routing protocol of hierarchical cluster based in wireless sensor network is LEACH (Low Energy Adaptive Clustering Hierarchy) [1, 10].

The rest of the chapter is compiled as follows. Section 2 presents the current wireless sensor network cluster based routing protocols. Section 3 outlines radio energy model of present LEACH and drawbacks of LEACH. Section 4 represents detail explanation of proposed protocol. Simulation results and performance comparison are shown in Sect. 5. Conclusion and future scopes are shown in Sect. 6. References are included in last section of this chapter.

2 Related Works

This section comprises of existing routing protocols which are cluster based and other associated protocols are also briefly described in this section. LEACH [3, 9] is one of the most prominent cluster based hierarchical protocol and election of leader nodes is completely random in nature provided if the random number produced by the nodes satisfies threshold condition as in Eq. (1). To solve the unevenness of cluster head selection in the whole network LEACH-C (centralized LEACH) was proposed where the cluster head selection is done in centralized manner [3]. In LEACH-C even though uniform cluster head distribution is obtained, the cost of communication becomes high if the BS is located at far distance from the region where nodes are deployed and cost of

installation also becomes high since it has to be associated with some location aware techniques.

In HEED [7] protocol the authors consider nodes' unconsumed energy as the primary parameter for choosing leader nodes assuming that the nodes are of different initial energy level. They also consider communication strength level of intra cluster nodes and cluster size as the secondary parameters for clustering process. The result shows that the proposed protocol (hybrid energy efficient distributed clustering) provides uniform clustering process and uniform cluster head distribution with less overhead. Also better residual energy can be obtained in the head node of every cluster for each clustering process.

In [11], the authors proposed PEGASIS protocol where the charge for transmitting and collecting the sensed data from the network to destination is done by a single node. The nodes in this protocol (power efficient gathering in sensor information systems) are linked only with neighbor nodes in chain fashion and can pass the data to their immediate neighbors only until it reaches the head node. Every node takes the turn of becoming head node periodically. The simulation shows that PEGASIS has better lifetime than LEACH for various network sizes. The authors in TEEN [12] presented a method unlike the LEACH protocol to preserve energy of nodes to some extent by passing the sensed data to the nearest leader node only when the amount of collected data exceeds some pre-defined threshold value (hard TEEN) or when there is slight change in the sensing aspect (soft TEEN). The data transmission is done only when it is needed and not for all the time so that considerable amount of energy can be saved in comparison with other dynamic clustering protocols. Both hard and soft TEEN (threshold sensitive energy efficient sensor network protocol) indicate improved lifetime than LEACH and LEACH-C and lesser energy dissipation is shown by the protocol.

Handy et al. [13] proposed a deterministic cluster head selection method in self organizing clustering based protocol by considering an additional factor to overcome the complete randomness in cluster head selection of LEACH. This determining factor helps to overcome the process of being stuck in the middle of network operation (rounds) in cluster head selection process due to the improper threshold condition caused by the inclusion of energy value of nodes in the threshold equation of LEACH related protocols. Improvement in lifetime is achieved by this proposed protocol. Haseeb et al. [14] proposed a protocol called adaptive energy aware cluster based routing (AECR) that employs the weighted factors of node degree, distance of nodes to BS and unconsumed nodes' energy in the current round for electing cluster head and also it engages centralized form of transmitting data from leader node to BS. The information from nodes is passed to BS through neighbours so that huge energy consumption is avoided by direct communication with BS. The authors simulated the proposed protocol for various densities of nodes and different data generation timings. The result shows that this protocol performs better lifetime and throughput than other protocol like LEACH-DT.

In [15] the author proposed new clustering protocols for heterogeneous wireless sensor networks (WSNs) called M-EECP and S-EECP. In S-EECP (single-hop energy efficient clustering protocol), ratio of nodes' remaining energy and overall average network energy is considered in the threshold condition for CH selection and in

M-EECP as well. In M-EECP (multi-hop energy efficient clustering protocol) the author uses relay nodes to decide the minimum length path from the leader node to BS which is located at far distance from network by using directed weighted graph to overcome the fast death of nodes due to transmission of data in longer distance. The proposed protocol shows improved lifetime and lesser energy dissipation by nodes than the existing protocols like EECT (energy efficient clustering technique). The authors in [16] proposed a new cluster head election algorithm which is an energy efficient distance based protocol to provide further enhancement in the existing LEACH. It developed a new threshold including the factors like nodes' energy, separation between nodes and destination (base station) and distance between cluster head and destination for balancing the energy expenditure of nodes and to have extended network lifetime.

Hong, et al. [17] proposed a new method in wireless sensor networks based on pre-defined threshold value for replacing leader role called T-LEACH. This protocol has taken into account the energy consumption in overhead transmission for every round (clustering process) by head node for head node (leader node) replacement. The leader node replacement is done only when energy of nodes drop down below some calculated threshold value to avoid wasting of energy in overhead transmission for every round. In [18] the authors proposed a protocol to overcome the drawbacks of T-LEACH called MT-CHR. This protocol (modified threshold-based cluster head replacement) provides the appropriate probability of cluster head election after every cluster head replacement process to prolong the network lifetime. In [19] the authors proposed an improvement approach for lowering the energy dissipation in WSNs based on LEACH and developed a modified threshold condition consisting of additional factors like ratio of average distance between nodes to BS and nodes' distance to BS, number of times a node being in the position of leader role and the number of neighbour nodes surrounding the leader node for selecting cluster head nodes for every round. Apart from this, the authors also introduced modified TDMA scheme to overcome the unbalanced energy dissipation in the network by the leader node of smaller cluster size. The proposed method shows improved lifetime, better data packet delivery to BS and longer stability than the present hierarchical protocol and other LEACH associated routing protocols.

Authors in [20] developed a protocol (LEACH-DT) with new probability of cluster head election based on nodes' distance to base station and also incorporates multi-hop techniques for those leader nodes which are lying at longer distance from the base station. The simulated output shows improved lifetime over LEACH for different base station location. In [21] the authors proposed EE-LEACH for WSN. In this protocol which is an energy efficient LEACH based protocol the author considers Gaussian distribution model of nodes instead of uniform distribution. This protocol employs conditional probability for aggregating nodes into a macro node and also for passing the accumulated message to the next node. The result of EE-LEACH provides better network lifetime, better packet transmission and lesser source to destination delay than LEACH and EBRP (energy balance routing protocol).

The authors in [22] developed a new threshold condition for LEACH (E-LEACH) where they included factors like current residual nodes' energy to bring balance in the

energy depletion of the network and proposed new probability for selecting cluster head node. This inclusion of present residual energy makes the round operation to choose higher remaining energy node as cluster head more often than the lower remaining energy nodes. Also the authors introduced variable round time based on the present cluster size in contrast to that of LEACH constant round time. This protocol shows improvement in lifetime of network as a whole and amount of packets delivered to the base station when compared to LEACH protocol. In [24] the authors proposed an improved LEACH by considering both the free space path and multipath model for optimum cluster head calculation. The result shows better network lifetime for different network sizes, base station locations and densities of nodes than the existing LEACH. In [25] the authors proposed a modified threshold condition which shows improved network lifetime than the conventional LEACH.

3 LEACH Protocol

One of the leading hierarchical based clustering protocol in wireless sensor networks is LEACH (low energy adaptive clustering hierarchy) because of its energy saving process in three stages. Firstly, transmitting of data is done by few cluster head nodes only. Secondly, the collected data is sent to the base station after the process of aggregation to remove all the repeated data to save energy and lastly, the nodes undergo sleep mode after sending their sensed data to the corresponding head nodes to save its energy. In this adaptive energy routing protocol, the data transmission takes place for every round and each round is composed of two stages (phases) - set up and steady state phases. The steady state phase is taken to be of longer duration than the set up stage in LEACH.

In every round, election of cluster head is done on the set up phase based on the number generated randomly by any nodes between [0, 1]. If the number generated randomly by the nodes is less than the threshold value (1) then the node is chosen as cluster head for that round. After this election process the leader nodes (cluster head) will make an advertisement to the remaining nodes as the leader of the current round for its particular cluster after election process. The cluster members will decide its cluster head depending on the strength of the signal received by the nodes and will send joining acknowledgement to the particular cluster head. After receiving joining acknowledgment, the leader node will broadcast time slots for its member nodes for sending their collected data to the head nodes. The threshold condition for LEACH [3] is given by:

$$T(n) = \begin{cases} \frac{p}{1-p*(rmod 1/p)}, & \text{n } \varepsilon \text{ G} \\ 0, & otherwise \end{cases} \tag{1}$$

where p denotes probability of CH that can become cluster head in the network, r is the current round, G are nodes that have not been CH in the recent clustering process. Steady state phase is followed by transmission of the sensed data to the cluster head by the cluster members in their assigned slots for the particular time frame and will remain

in sleep state until next round starts. Every round contains certain number of time frames. The cluster heads will assemble the received data and send the integrated data to the BS after removing all the redundancy. This aggregation process also makes LEACH protocol to occupy the available bandwidth for lesser time. For transmission of data to base station by cluster head it uses CSMA scheme (carrier sense multiple access) to check whether other cluster heads are transmitting data using the carrier in the moment or free to be used. The cluster head will remain in active state for whole round time operation until next cluster head election process starts. Although LEACH seems to be one of the leading energy efficient hierarchical cluster based routing protocol it suffers from drawbacks like repeated selection of same nodes to be cluster head for the consecutive rounds, faster death of far away nodes from the BS, unbalanced energy consumption by different clusters, improper cluster head distribution due to complete randomness in set up phase.

4 Proposed Approach

In LEACH protocol the main parameters that play an important role for electing cluster head are probability of nodes that can be elected as cluster head and the threshold condition as in (1). The proposed protocol (TH-LEACH) uses the radio energy dissipation model same as the traditional LEACH and has steady state phase operation similar to that of LEACH. This protocol is usually meant for extending network lifetime in application specific purpose. This chapter aims to improve the threshold condition for LEACH with the inclusion of additional parameter R_c for easy selection of cluster head till the lifetime of network ends, energy and distance factors to the present threshold condition of LEACH. By considering these additional factors, the election of cluster head takes into account the present energy of nodes, i.e., more energy level nodes will be elected as cluster head in every clustering process (rounds). The inclusion of distance factor provides preference to nearer nodes to be elected as cluster heads more often than the nodes located at far distance from base station. This improved threshold will allow the nodes which have not been elected as cluster heads in the recent rounds to become leader in the consecutive rounds. The modified threshold condition is given as:

$$T(n) = \begin{cases} \frac{p}{1-p*(Rmod1/p)} * \left(\frac{1}{logd(i)} + E_{CR} + Rc * (1 - E_{CR})\right), n \varepsilon C \\ 0, \qquad\qquad otherwise \end{cases} \tag{2}$$

where p is the probability of CH among the deployed nodes, R is the present round, C are nodes that have not been CH in the recent rounds, E_{CR} represents the ratio of remaining energy of node to its initial energy, R_c is the number of consecutive rounds that the nodes have not been selected as cluster head and *d(i)* represents the separation of a particular node from BS and the logarithm function is performed with base 10 and i ranges from 1, 2, 3, …, n.

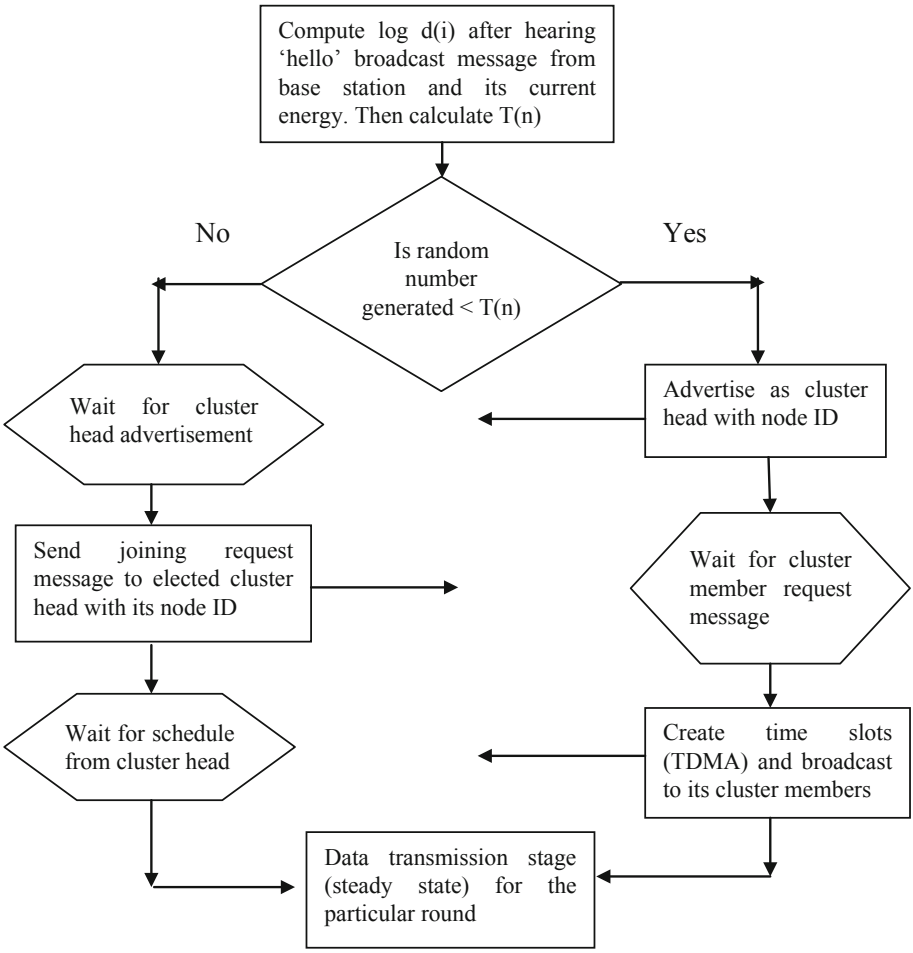


Fig. 1. Flowchart of proposed algorithm

Figure 1 represents the flowchart of the proposed algorithm. The main favorable matter of this protocol is that the nodes are not required to spend extra energy for obtaining information about energy of other nodes or total energy of the network or distance among the nodes. The nodes will perform few local computations which do not require passing data to other nodes and energy dissipated in local computation is very much less as compared to data transmission. When the destination node or Base Station announced 'hello message' in broadcast manner to the nodes in network at the initial stage of the network operation the nodes will compute its distance to BS with the help of signal strength received by them only for once in its lifetime. The logarithm

function is used so that the threshold should not drop to a very small value for far away nodes from BS. Similarly, R_c factor is included to avoid the network being stuck since the residual energy of nodes is also included in the improved threshold.

With this new threshold condition the proposed protocol is able to save energy to some extent and the problem of fast energy depletion of head nodes can be lessened in the network. The protocol which is being proposed considers some suppositions to set up the network:

- All nodes are initially homogeneous.
- All nodes have the ability for transmitting to the BS and are stationary with location aware.
- All nodes are identical, i.e. they have the ability for the same function to be operated.
- Communication between nodes is symmetric in nature.

5 Simulation Results

For simulation purpose, we use different system parameters as described in Table 1.

Table 1. Parameters used in simulation

Parameters	Values
Starting energy of nodes	0.5 (Joules)
Nodes used in network	100,50
P	0.1
E_{elec}	50 nJ/bit
E_{DA}	5 nJ/bit
ε_{fs}	10 pJ/bit/m^2
ε_{mp}	0.0013 pJ/bit/m^4
Information packets (bits)	4000
Overhead bits	200
BS location	(50,50) centre of the network
Network area	(100 × 100 & 200 × 200) m^2

MATLAB simulation is used for performance analysis of the proposed protocol. The comparison is performed for separate network sizes and different number of network nodes (density) to compare network lifetime, overall remaining energy of network and packets transmission to base station. The comparison is performed based on the threshold condition of LEACH and other LEACH related protocols.

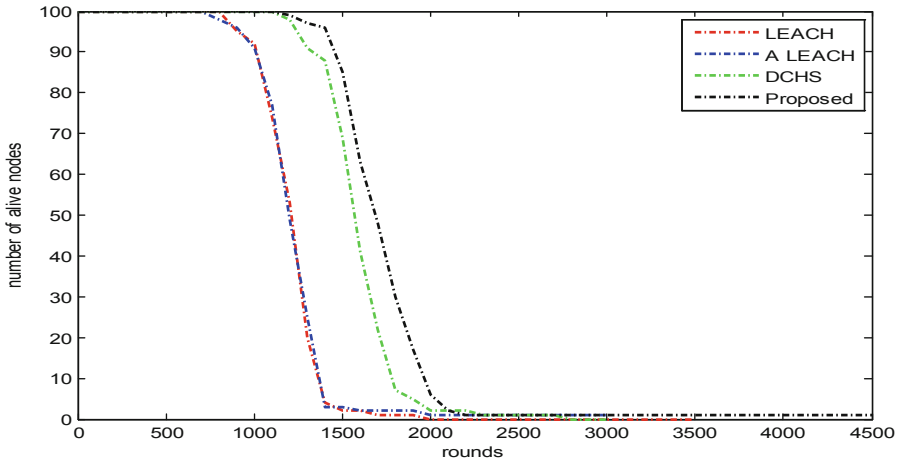


Fig. 2. Alive nodes vs rounds for 100 × 100 network size

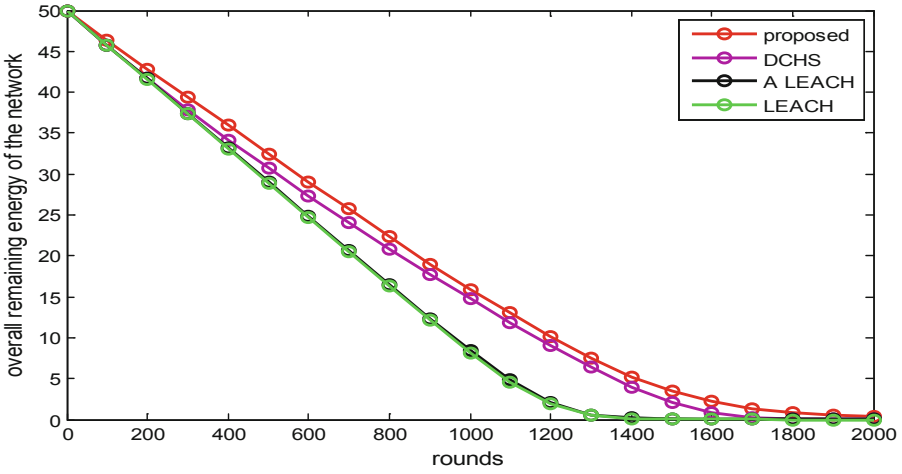


Fig. 3. Overall remaining energy of nodes per round vs rounds for 100 × 100 network size

In Fig. 2 it can be observed that the network lifetime of proposed hierarchical protocol is longer comparing to the conventional LEACH and other correlated clustering protocols. FND (first node dead) of the proposed protocol occurs at 1200 rounds in contrast to that of LEACH, A LEACH [22], DCHS [14] at rounds 840, 780, 1100 respectively indicating longer duration between the initial startup of the network and first death of nodes (stability) in the proposed protocol (TH-LEACH). The last node

dead (LND) of the proposed LEACH extends up to 4500 rounds as shown in Fig. 2. This stability extension in the network is mainly due to the improved threshold condition as in Eq. (2).

Figure 3 indicates that the energy of nodes in the network taken as a whole decrease slowly in the proposed protocol in contrast to the ordinary LEACH and other correlated protocols. This is mainly because of the consideration of distance factor in cluster head selection. The selection of nearer nodes as head nodes is more frequent than the far away nodes in the proposed protocol and hence, lesser overall energy consumption per round. It also shows that data transmission by far away node is also reduced which can lead to high energy dissipation and ultimately leading to faster death of nodes.

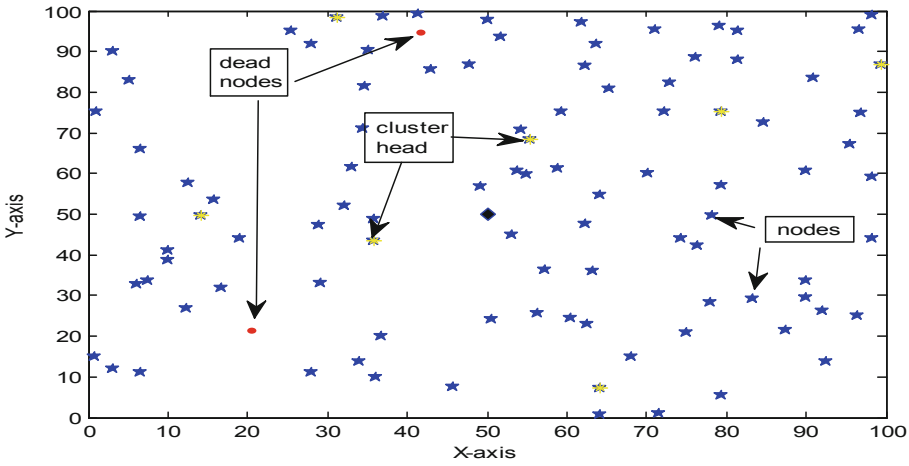


Fig. 4. Dead nodes at random round 1320 for the proposed LEACH of 100 × 100 network size

Figure 4 shows the distribution of dead nodes, cluster heads and normal nodes as cluster members (indicated by text arrow) at random rounds of clustering process. This figure shows cluster heads distribution in the network which is selected based on distance and energy dependent threshold condition. The cluster members will join to the corresponding head node which is closer to them. The distance is calculated based on received level of the signal strength by the member nodes during the advertisement process after being selected as head node for the current round. As the network size increases the separation among the nodes will also increase. The proposed protocol is compared for different network sizes to analyze its network lifetime and the effect of increasing the separation among nodes in the network.

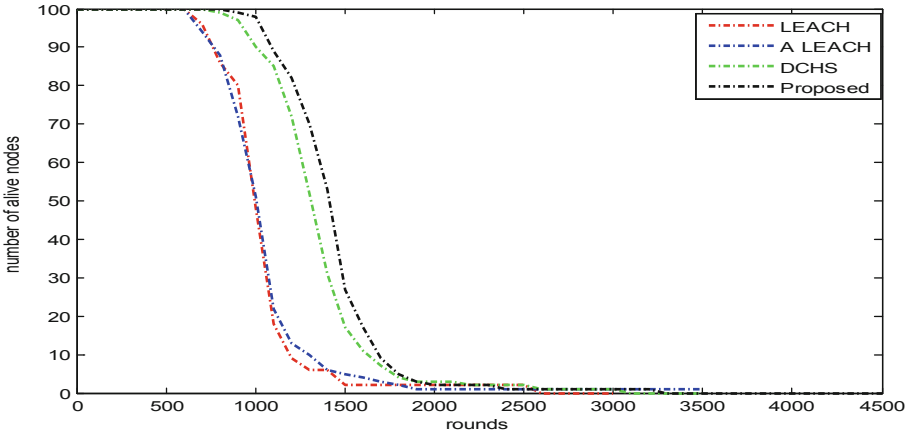


Fig. 5. Alive nodes vs rounds for 200 × 200 network size

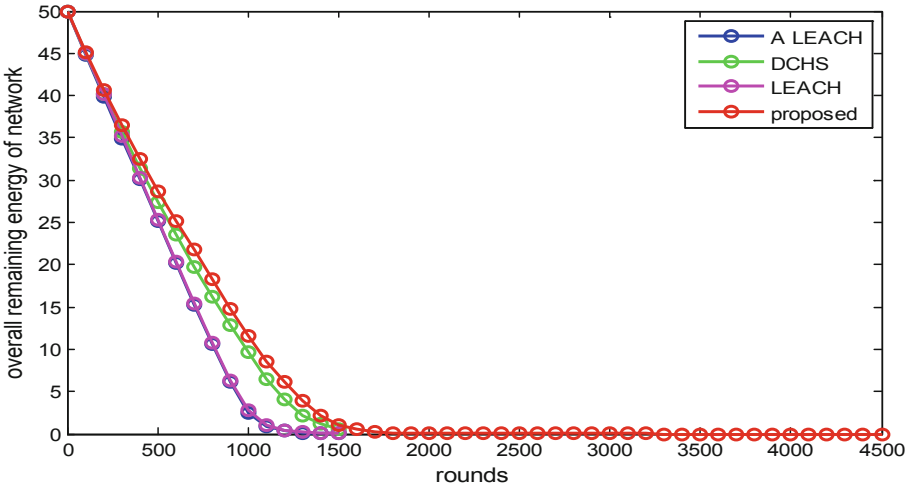


Fig. 6. Overall remaining energy of nodes per round vs rounds for 200 × 200 network size

Figure 5 indicates that the proposed protocol shows better overall lifetime than the existing ordinary LEACH and other existing connected protocols when the size of network is increased from 100 × 100 m^2 to 200 × 200 m^2 showing that the proposed method is applicable for increased network size also to have more lifetime extension. Figure 6 shows the overall unconsumed (remaining) energy of network as a whole with rounds indicating lesser energy consumption by network nodes in the proposed protocol for every clustering process than that of the other routing protocols which further leads to extension of network lifetime.

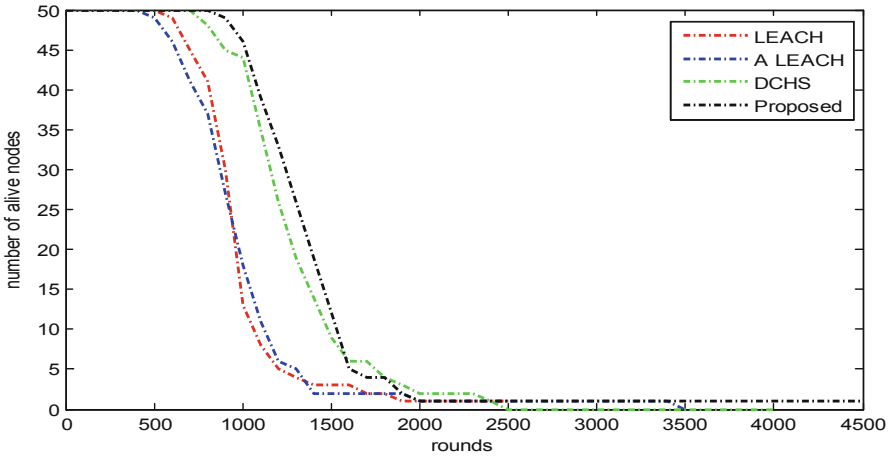


Fig. 7. Alive nodes vs rounds for 200 × 200 network size (50 nodes)

From Fig. 7 it can be noted that the proposed protocol performs better in terms of lifetime when the number of nodes (density) changes in the network, i.e., when the density of nodes decreases to 50 nodes from 100 nodes for the network size 200 × 200 m^2 keeping the base station location same (50, 50) from the centre of the network. It shows that the modified threshold condition in the proposed protocol still holds true for extending network lifetime for lesser number of nodes. This is achieved by selecting the appropriate nodes to be head nodes for the existing round. Figures 5, 6 and 7 demonstrate that the proposed protocol possesses scalability property of wireless sensor networks.

From Fig. 8 it can be shown that the data packets delivered to the base station in every round process are more in proposed protocol comparing with other related routing protocols for the same network energy level. In IDE [23] and RED LEACH [22] the packets received by base station is much lesser with rounds for the same overall network energy level since the nodes elected as cluster head becomes lesser with decrease in energy levels of the nodes as the round proceeds and hence, lesser packet is received by the base station. In Fig. 9 it is seen that the overall packets obtained by base station from the nodes (with rounds) i.e., from the existing number of existent nodes are more in the proposed method when compared to other associated clustering based protocols. It indicates the selection of appropriate nodes as head nodes in every clustering process and proper formation of clusters in the method proposed in this chapter in comparison to other connected protocols. The graph is plotted for only up to 50% alive nodes however it can be extended up to 1% alive nodes with more number of rounds.

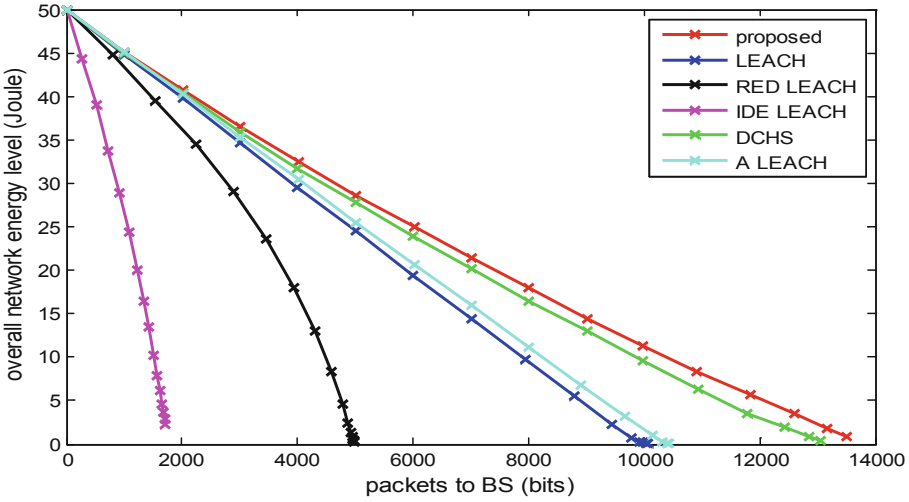


Fig. 8. Energy consumption per round vs packets to BS for 200 × 200 network size

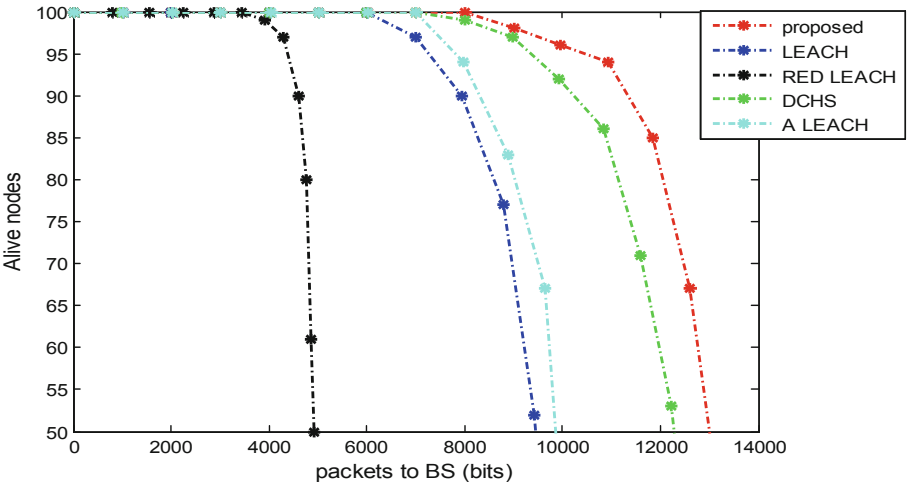


Fig. 9. Alive nodes vs packets transmission to BS for 200 × 200 network size

6 Conclusion and Scope of Future

This chapter describes an enhanced threshold condition for LEACH protocol for extending network lifetime. This proposed protocol produces better performance than the traditional LEACH and other connected protocols in network parameters like stability, packets throughput to the base station and network lifetime. Distance and energy are the two most important factors that have to be considered when the matters come to energy efficiency of the network. It also indicates better adaptation to the

changing of network densities and network sizes. This proposed protocol can be applicable to those sensing network which is application specific and where cost function is the main factor.

In future this proposed protocol can be combined with some delay and coverage related techniques so that the overall service of the routing protocol in the network is improved with high accuracy and the performance can be analyzed for different WSN properties, different energy level of nodes for heterogeneous networks and also the performance can be studied considering the mobility condition of nodes. Even though many improved protocols have been proposed based on conventional LEACH proper coverage of the whole network by cluster heads during clustering process, uniform distance distribution of cluster heads in complete self organizing process with less computation, analyzing the most appropriate nodes distribution in the network for such distributed cluster based protocol are some of the considerable issues still yet to be improved.

References

1. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**, 325–349 (2003)
2. Karl, H., Willig, A.: Protocols and Architecture for Wireless Sensor Networks. Wiley, Hoboken (2005). ISBN 0470095105
3. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. IEEE Press (2000)
4. Singh, P., Paprzycki, M., Bhargava, V., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. Communications in Computer and Information Science, vol. 958, Springer, Singapore (2018)
5. Ajay, K.T., Suraj, G.P., Nilkanth, B.C.: A survey on data routing and aggregation techniques for wireless sensor networks. In: IEEE International Conference on Pervasive Computing (2015)
6. Pantazis, N.A., Nikolidakis, S.A., Vergados, D.D.: Energy-efficient routing protocols in wireless sensor networks: a survey. IEEE Commun. Surv. Tutorials **15**(2), 551–591 (2013)
7. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks. IEEE Trans. Mob. Comput. **3**(4), 909–914 (2004)
8. Singh, S.P., Sharma, S.C.: A survey on cluster based routing protocol in wireless sensor networks. In: IEEE International Conference on Advanced Computing Technologies and Applications (2015)
9. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**(4), 660–670 (2002)
10. Xu, J., Jin, N., Lou, X., Peng, T., Zhou, Q., Chen, Y.: Improvement of LEACH protocol for WSN. In: 9th IEEE International Conference on Fuzzy Systems and Knowledge Discovery (2012)
11. Lmdsey, S., Raghavendra, C.S.: PEGASIS: power-efficient gathering in sensor information systems. IEEE AC Paper (2002)

12. Manjeshwar, A., Agrawal, D.P.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: IEEE International Parallel and Distributed Processing Symposium (2001)
13. Handy, M., Haase, M., Timmermann, D.: Low energy adaptive clustering hierarchy with deterministic cluster-head selection. In: 4th IEEE International Workshop on Mobile and Wireless Communications Network, pp. 368–372 (2002)
14. Haseeb, K., Bakar, K.A., Abdullah, A.H., Darwish, T.: Adaptive energy aware cluster-based routing protocol for wireless sensor networks. Wirel. Netw. **23**, 1953–1966 (2017)
15. Kumar, D.: Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks. IET Wirel. Sens. Syst. **4**(1), 9–16 (2014)
16. Sharmaa, R., Mishraa, N., Srivastava, S.: A proposed energy efficient distance based cluster head (DBCH) algorithm: an improvement over LEACH. In: 3rd IEEE International Conference on Recent Trends in Computing (2015)
17. Hong, J., Kook, J., Lee, S., Kwon, D., Yi, S.: T-LEACH: the method of threshold-based cluster head replacement for wireless sensor networks. Inf. Syst. Front. **11**, 513 (2009)
18. Darabkh, K.A., Al-Rawashdeh, W.S., Hawa, M., Saifan, R., Khalifeh, A.F.: A novel clustering protocol for wireless sensor networks. In: IEEE International Conference on Wireless Communication, Signal Processing and Networking (2017)
19. Elshrkawey, M., Elsherif, S.M., Wahed, M.E.: An enhancement approach for reducing the energy consumption in wireless sensor networks. J. King Saud Univ. – Comput. Inf. Sci. **30**, 259–267 (2018)
20. Kang, S.H., Nguyen, T.: Distance based thresholds for cluster head selection in wireless sensor networks. IEEE Commun. Lett. **16**(9), 1396–1399 (2012)
21. Arumugam, G.S.: EE-LEACH: development of energy-efficient LEACH protocol for data gathering in WSN. EURASIP J. Wirel. Commun. Netw. **2015**(1), 1–9 (2015)
22. Chit, T.A., Zar, K.T.: Lifetime improvement of wireless sensor network using residual energy and distance parameters on LEACH protocol. In: The 18th International Symposium on Communications and Information Technologies. IEEE Press, Yangon (2018)
23. Gupta, S., Marriwala, N.: Improved distance energy based LEACH protocol for cluster head selection in wireless sensor networks. In: 4th IEEE International Conference on Signal Processing, Computing and Control, Solan, India (2017)
24. Ngangbam, R., Hossain, A., Shukla, A.: Improved low energy adaptive clustering hierarchy and its optimum cluster head selection. Int. J. Electron. (2019). https://doi.org/10.1080/00207217.2019.1661023
25. Ngangbam, R., Hossain, A., Shukla, A.: An improved Clustering based hierarchical protocol for extending wireless sensor network lifetime – EG LEACH. In: IEEE International Conference on System, Computation, Automation and Networking, Pondicherry, India (2018)

Medium Access Control Protocols for Mission Critical Wireless Sensor Networks

Gayatri Sakya[1] and Pradeep Kumar Singh[2(✉)]

[1] Department of Electronics and Communication Engineering,
JSS Academy of Technical Education, Noida, UP, India
gayatri.sakya@rediffmail.com
[2] Department of Computer Science and Engineering,
Jaypee University of Information Technology, Waknaghat, Solan, HP, India
pradeep_84cs@yahoo.com

Abstract. Wireless sensor networks have variety of applications in military and civilian tracking, habitat monitoring, patient monitoring and industrial control and automation. Many protocols have been developed to support these applications. For applications such as gas leakage detection system, volcanic activities alerts, fire safety systems, border surveillance and tsunami alert systems where apart from energy saving, timely information delivery is also important, an efficient MAC protocol is required. These are termed as mission critical applications. Reducing energy consumption, efficient utilization of bandwidth, Throughput, Latency, Scalability and Adaptability, Reliability, and Degree of Intelligence are the most important parameters of a good MAC protocol designed for mission critical applications. The degree of intelligence is the parameter which is novel to these protocols and will be provided by introducing the Machine learning and Artificial Intelligence. The chapter addresses the design issues for MAC layer, different MAC protocols designed for wireless sensor networks, mission Critical Applications of WSNs and the performance parameters required for Mission Critical MAC Protocols. Various MAC protocols based on contention based and contention free channel access mechanism are discussed in detail in the chapter. Now we are in the era, where each application demands intelligence and automation. For this purpose, there is need to design smart protocols adaptive to critical scenarios. In the chapter the existing MAC protocols and the performance parameters for a mission critical MAC protocol such as throughput, packet delivery ratio, packet loss rate, efficient bandwidth utilization, scalability and adaptability are discussed. A review of machine learning techniques is also done which shows that MAC protocols may be enhanced for their suitability in mission critical scenarios. The chapter also discussed the case study of one mission critical MAC protocol and its comparison with SMAC protocol. The application of mission critical MAC protocol in pipeline leakage detection system is also discussed with its design model. Finally the chapter ends with discussion of recent issues and challenges and future scope of intelligent ML based MAC protocol design.

Keywords: Mission critical · Wireless sensor networks · MAC protocols · Machine learning techniques · Performance parameters · Pipeline leakage

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 67–86, 2020.
https://doi.org/10.1007/978-3-030-40305-8_5

1 Introduction

1.1 Overview of WSN

WSN nodes [1] consist of sensing elements, microcontrollers/microprocessors, storage/memory, a power supply, a transceiver, and an actuator as shown in Fig. 1.

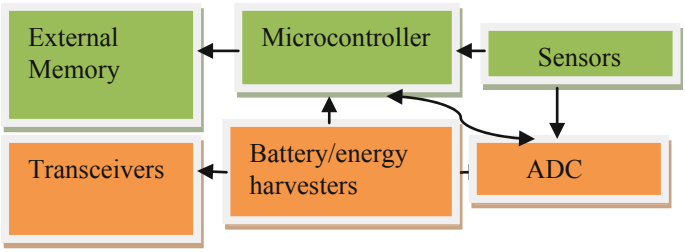


Fig. 1. Architecture of Wireless Sensor Node [3]

Battery is the main source of power in a sensor node [2, 3] and the radio is implemented in WSN node to transmit data as it cannot store much data. Solar panels attached to sensor nodes can also be one source of power, according to the deployed conditions of the environment. WSNs are used in various applications of monitoring, tracking and surveillance. Figure 2 discuss the mechanism of WSN working.

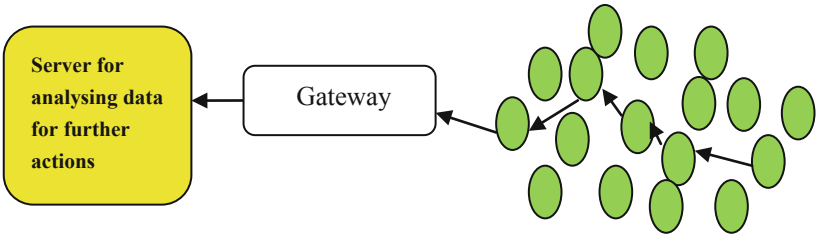


Fig. 2. Wireless Sensor Network

1.2 Background and Motivation

The transmitter/receiver of WSN node consumes more power so a better transmitting/receiving protocol design can be a way to reduce it as discussed in [3, 4]. Wireless sensor network like other networks has a protocol stack shown in Fig. 3. Because of the infinite applications of WSNs, the protocols at each layer must be designed accordingly. Hence the research work is continued on each layer still and the stack is under development as discussed in [4]. The physical layer deals with frequency allocation, modulation and demodulation schemes, channel models and source and channel encoding and decoding, and receiver design etc. Whereas the DLL layer combined the MAC Layer and Logical Link control layer. The protocols at MAC layer

are the MAC protocols which set the rules for coordinating the sharing of channel among number of nodes. The MAC protocol design is highly dependent upon the physical properties used for WSNs.

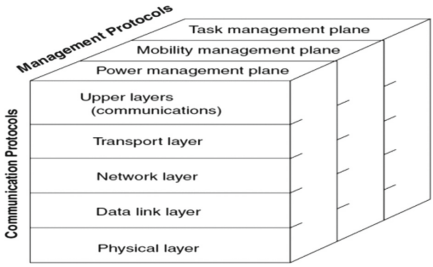


Fig. 3. Protocol stack for Wireless Sensor Networks [3]

Following are the main attributes of the medium access control protocols as discussed in [5]

- Residual Energy hence network lifetime
- Scalability to changing in number of nodes
- Station synchronization
- Channel utilization
- Response delay and throughput

So managing the communication on the channel can save large amount of energy which can be done by designing a good MAC protocol.

The MAC layer deals with the issues of designing a better communication protocols in terms of above discussed attributes.

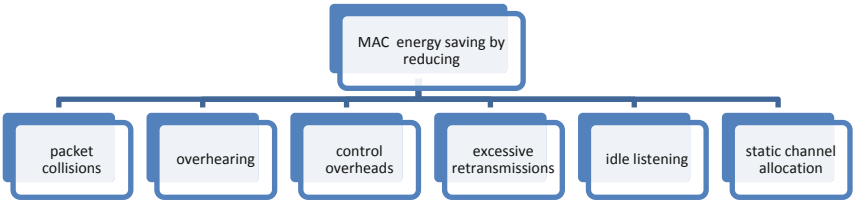


Fig. 4. Energy wastage factors in MAC

Figure 4 discusses the energy wasting factors in MAC communication protocols [6]. The MAC protocol design basically includes energy saving aspects and adaptive behavior to dynamically changes in topologies of WSN. First is to find energy waste causes and second is topology of network which decides behavior of traffic which will be handled by MAC protocol. A large number of efficient MAC protocols in [6–11] are proposed. These are scheduled free contention based MAC, scheduled based and

TDMA-based MAC, scheduled and contention free (hybrid), and cross layer MAC protocols. In Mission critical applications such as in border surveillance, in oceans for tsunami alert system or in volcanic monitoring applications our protocol should be energy efficient and should also should be able to deliver data on time and in reliable manner.

1.3 Wireless Sensor Networks in Mission Critical Applications

In this work Mission critical applications are defined as the applications in which the energy efficiency is of prime concern along with the data delivery performance. The wireless sensor networks found their applications in monitoring and surveillance on borders [12], military target tracking, in gas leakage detection systems [13], in Tsunami alert systems [14], in volcanic activity monitoring systems [15] and in weather monitoring activities. In such applications, the wireless sensor networks when deployed once need to be alive for years. There are some areas in which nodes are not frequently accessible once deployed. Hence residual energy of the nodes is an important area of concern, making the network path alive for years. This work defines the mission critical application as the applications which require efficient energy saving of nodes and network along with the improved data delivery performance of the network.

2 Review of Existing MAC Protocols and Their Mechanism

In MAC protocols such as IEEE 802.11 designed for wireless LAN's, listen time of the nodes for receiving the possible traffic dissipate about 50% of the energy [4, 5, 16]. But [6] SMAC tries to reduce the waste of energy from all the sources discussed in Fig. 4. It is very important dynamic and contention based MAC protocol which overcomes the lacuna of 802.11 in WSN. SMAC protocol consists of three major components: periodic listen and sleep, collision and overhearing avoidance, and message passing.

SMAC Protocol: The frame structure of SMAC protocol is divided into Listen and Sleep period.

The listen period further divided into SYNC and DATA period as shown in Fig. 5.

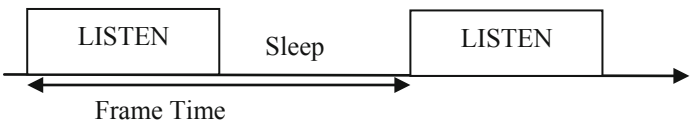


Fig. 5. Frame for SMAC Protocol

Synchronization Phase:

- In Sensor – MAC protocol the nodes are deployed at duty cycle and the duty cycle will not change once fixed.
- The nodes choose their schedule on their own using the scheduling algorithm.

- The nodes forms virtual cluster by having synchronization among the neighbors. A schedule table is prepared by each node to share its wakeup/sleep information and nest time to wakeup.
- The neighbor node gets the schedule and it decides whether to follow it or to follow other schedules also.

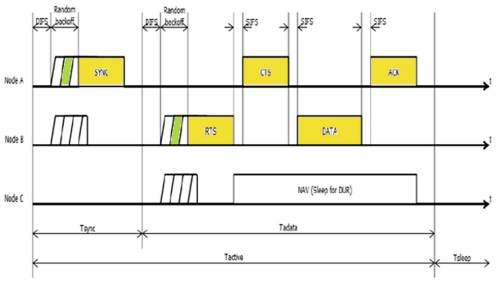


Fig. 6. SMAC protocol mechanism

As shown in Fig. 6, The CTS/RTS/DATA/ACK mechanism is used for contention in SMAC protocol.

$$\text{Ds (Average sleep delay on the sender)} = T_{\text{frame}}/2 \tag{1}$$

$$T\_(\text{Frame}) = T\_(\text{Listen}) + T\_(\text{Sleep}) \tag{2}$$

$$\text{Duty cycle} = T\_(\text{listen})/T\_(\text{Frame}) \tag{3}$$

$$\begin{aligned} \text{So Relative Energy Saving} &= T\_(\text{sleep})/T\_(\text{frame}) \\ &= 1 - \text{duty cycle} \end{aligned} \tag{4}$$

So to save the energy, the duty cycle of the protocol at the time of deployment should be low. This duty cycle concept is introduced in SMAC protocol which changed the designing of contention based MAC protocols.

Drawback: Connecting nodes consumes more energy due to synchronization. Also the border nodes need to follow more than one schedule and consumes more energy as they need to awake more times to monitor traffic. During simple SMAC study the mission critical parameters like packet delay/packet loss rate are not studied. [7] Wei Ye et al. solved the problem of delay by using coordination of nodes for awakening them early and receive next incoming packet. Here the nodes who receives RTS/CTS packets which are not destined for those (overhear), will wake up for some little amount of time. If the node is next neighbor, then waiting time is reduces and the packet get delivered to it. The mechanism of adaptive listen in S-MAC is shown in Fig. 7.

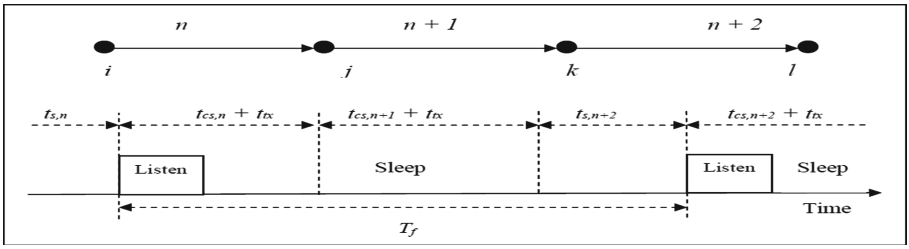


Fig. 7. Adaptive listening in three hop network [7]

A drawback of SMAC nodes includes many schedules following by one node, which increases awakening time and hence such nodes consumes more energy. At heavy loads it works as no sleep protocol and hence reducing the network lifetime which makes it unsuitable for mission critical applications.

Jamieson et al. [17] discussed Sift protocol. **Sift** is a MAC protocol for event-driven sensor network where when an event is sensed, the first R of N important reports send with low latency. There is another mechanism discussed by El-Hoiydi et al. [18] based on preamble sampling technique. All sensor nodes do listen to the channel for constant period $T_{w.}$ If medium is busy, then node listens till the packet is received or till the medium becomes idle. The wakeup preamble of size T_w added in front of every data frame at the transmitter to wake up the receiver when data is received. The throughput is reduced because of this mechanism and also the power consumption is more because all nodes listen to the channel and overhears the transmission.

Lu et al. [19] in 2004 proposed **DMAC** protocol in which the active and sleep time of nodes depends upon the depth in the tree to allow uninterrupted forwarding of data packets. DMAC protocol is applicable to only specific data gathering tree for unidirectional traffic from multiple nodes to the single sink. Similar to DMAC, there are other protocols whose designs are aware of a packet transmission path like protocol given by Li et al. [20] based on GSA (global schedule algorithm) which helps large network to follow a common schedule to save energy. To reduce latency in multi-hop paths, the fast path algorithm (FPA) is used. FPA does this by adding additional listen slots to the nodes which completes the paths from sources to sinks. **LEEMAC** [21] is MAC Protocol which is an improvement of DMAC protocol designed for data gathering trees. These protocols need improvement to become suitable in dynamic topological scenarios of mission critical nodes. Dam et al. [22] proposed a **Timeout-MAC (T-MAC)** protocol where active period is expired when for a definite amount of time no critical event occurs. Rajendran et al. [23] proposed a MAC protocol **TRAMA** using TDMA-based algorithm. The idea is to divide the time into random-access and scheduled-access periods and to use scheduled access period for transmission. A random access period followed by scheduled access period forms a cycle. Random-access period is used for two-hop topology information. Lin et. al. [24] proposed Dynamic Sensor-MAC **(DSMAC)** protocol based on dynamic duty cycle feature to S-MAC protocol. Ezzedine et. al. [25] proposed an **ELE-MAC** hybrid protocol to reduce the control packets overhead along with preserving the merits of adaptive listen SMAC. The analytical approach refers the energy calculations done in [26]. The RTS and

SYNC packets may further be combined for improving ELE-MAC. Hamady *et al.* [27] discussed improvement of the SMAC Protocol by minimizing interaction between connecting nodes. Only selective intermediate nodes will follow two schedules (Fig. 8).

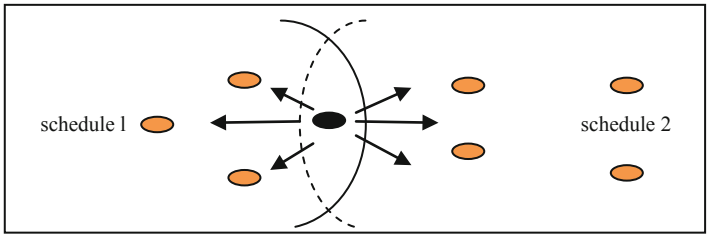


Fig. 8. Intermediate node [27]

So the number of shared energy-wasting nodes will be decreased. Ibrahim et al. [28] proposed an improved S-MAC protocol, **PS-MAC** for high traffic. The energy saving is achieved using the parallel transmission concept. In mission critical scenarios, the latency and packet loss rate increases. So it needs improvement to b suitable for critical events.

Xia et al. [29] used fuzzy logic based algorithm in MAC protocols. Also Yusuf [30] used fuzzy based algorithms in routing for wireless sensor networks. Misra et al. [31] also proposed MAC protocol which uses fuzzy logic techniques to dynamically change the listen period and cycle time of the nodes keeping their duty cycle constant. The adaptive listening is done using fuzzy logic which changes the slot time based on the residual energy and network traffic on node. The SMAC has static listen period which is made adaptive in **FALMAC** protocol. To further reduce the synchronization overhead another fuzzy algorithm adaptively manage the synchronization period based on number of neighbours of the node and residual energy of network. This protocol reduces energy consumption but does tradeoff with throughput and latency. The complex fuzzy algorithm demands more memory space.

Ku et al. [32] proposed **EX-SMAC** protocol, which is an advanced version of SMAC protocol and designed for low latency. The active period is sub-divided into M non-overlapping extensions. Each cluster assigned one extension which is shorter than S-MAC listen period. The strategy proposed is shown in Fig. 9.

The Latency and energy efficiency performances are discussed while ignoring the throughput. The effect of sleep time in wireless sensor networks MAC protocol is addressed by Ramakrishnan et al. [33]. The effect of sleep in a sensor MAC protocol is discussed by using queuing analysis and simulation. Ramchand et al. [34] did hybrid of S-MAC and T-MAC protocols to reduce energy consumption. The mathematical model is proposed for reducing the energy consumption.

Another significant mechanism used for designing the MAC protocols is **TDMA** Based technique for sharing the channel by multiple users. TDMA Based MAC [35] technique works on clusters and gateway strategy in the network. The Gateways play

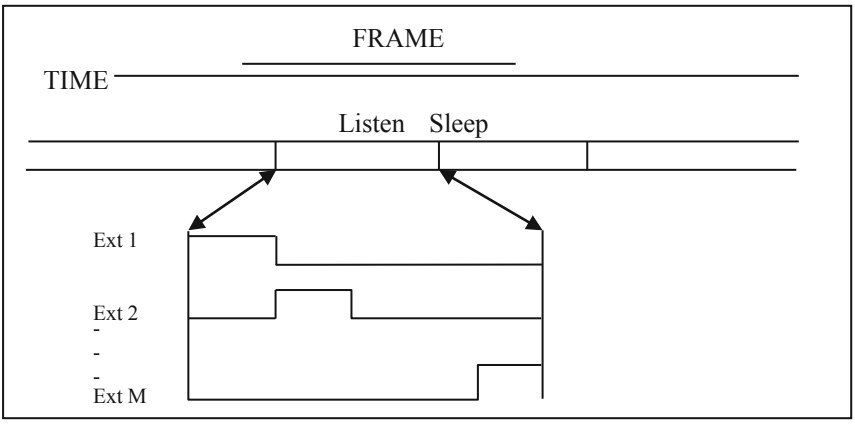


Fig. 9. EX-MAC mechanism [32]

the role of allotting time slots to the cluster nodes. Main TDMA-based MAC protocols are discussed in [9, 36] and [37].

The static nature of channel allocation scheme makes TDMA inefficient for mission critical scenarios. So we have some hybrid protocols proposed by researchers. Rhee et al. [38] proposed a new hybrid MAC scheme, called **Z-MAC** for sensor networks which combine the strengths of TDMA and CSMA. In low traffic, it behaves like CSMA, and under high traffic, like TDMA. Some Multichannel TDMA based protocols are also proposed to increase the throughput of wireless sensor networks. Researchers have proposed few multi-channel MAC protocols [39–43] that use multiple channels. These multichannel protocols increases the BW of wireless sensor node. Some researchers proposed Cross-Layer Based MAC protocols which use the information from upper or lower layers to improve the performance of protocols.

Du et al. [44] proposed **Routing enhanced duty cycle MAC** protocol which uses control frame (PION) instead of RTS and carries the information from network layer. It has all information of RTS control packet but also includes the cross layer information from network layer. This information includes the destination address and the number of hops the PION has travelled.

Cho et al. Proposed another cross-layer based approach based protocol named **HE-MAC** [45]. This protocol extends transmission in a single duty cycle by two more hops which results in reduction in power consumption and packet latency. Though cross layer protocols tried to enhance the QoS of MAC protocols but they introduce complexity in handling the data transmission.

Suriyanchai et al. discussed some mission critical applications which demands high time bound performance and reliable data delivery. The simulations in various reviewed chapters are done using Network Simulator (NS-2). So during the survey [46–52], it is observed that we can implement a new protocol using Network Simulator and can analyse the protocol performance without using a real hardware.

Wireless sensor networks have been a growing research area from last few years. This is because they are ad-hoc in nature and can be deployed in unattended areas to

collect the information. Therefore they have variety of applications in military and civilian tracking, habitat monitoring, patient monitoring and industrial control and automation. There are many protocols which have been developed to support these applications. But when the applications demand better data transport performance along with the energy efficiency, they become mission critical. So an efficient MAC protocol is required for mission critical applications in wireless sensor networks.

3 Need for Mission Critical MAC Protocol

Wireless sensor networks support applications such as industrial process monitoring, patient monitoring, and military target tracking, Volcanic Monitoring, Tsunami alert Systems etc. These are the mission critical applications of following attributes:

- Nodes cannot be replaced frequently, once deployed. So residual energy of nodes need to be improved.
- Improved data delivery is required in time and reliability domain. So the network performance parameters such as delay, packet loss rate, packet delivery ratio and throughput should be taken into consideration.

A medium access control can improve the residual energy of nodes by managing the active time of nodes in which transceiver is in on state. Also by choosing the best contention mechanism for accessing the channel, it can reduce the collision of packets and hence can improve energy performance. In mission critical MAC protocol, on sudden occurrence of an event, the data traffic increases. So according to the traffic behavior the MAC protocol can provide a mechanism to increase the listen period of the nodes to handle the traffic in critical scenarios. Retransmission algorithm can also be included in MAC protocol to make the data transmission more reliable.

A good mission critical MAC protocol should save the energy of the nodes in high traffic scenarios along with improved data transport performance. In low and medium traffic rates, they should be designed to preserve the residual energy of the nodes.

In most of the protocols reducing energy consumption is the main objective. Only few have considered the energy and data transport performance both. There are very few protocols in the survey which has talked about the energy, Throughput, Latency, Packet delivery ratio and Packet loss rate for the reliable data transmission which is the requirement of a MAC protocol suitable for mission critical applications. Some mission critical MAC protocols are discussed in [9] and compared for their reliability and data delivery performance. Also Sakya et al. [69] proposed analytical model of a regression based MC-MAC protocol. After that they provided another mission critical MAC protocol model which was the improved version of MC-MAC. G. Sakya et al. gave ADMC-MAC mission critical MAC protocol [58] which provided 71% energy saving in mission critical scenarios. It also provided comparable throughput and PDR performance to SMAC protocol when operated at 40% duty cycle in mission critical scenarios.

4 Performance Metrics

The Mission Critical MAC protocol should be tested for its performance both analytically and using simulation tool for the following performance matrices.

- **Average Residual Energy of Node and Total Residual Energy of the Network**

$$\begin{aligned}&\textbf{ARE (average residual energy of node)}\\&= \sum (\text{remaining energy of the node})/(\text{total number of nodes in the network})\end{aligned} \tag{5}$$

$$\begin{aligned}&\textbf{TRE (Total residual energy of the network)}\\&= \sum (\text{remaining energy of all the nodes in the network}).\end{aligned} \tag{6}$$

- **Throughput**
  In Many wireless sensor network applications such as patient monitoring or battle field surveillance, it is required to have data delivery in a limited time period. This may be considered as a matrix for timely data delivery also.

$$\textbf{Throughput in Kbps} = (\text{Packets received})/\text{Total time} \tag{7}$$

- **Latency**
  Latency is the delay counted since a senor node has a packet to send till the packet is successfully received at the receiver node. Monitoring applications can tolerate some latency but in mission critical applications like monitoring pressure in gas pipelines, the latency becomes an important issue to be handled by MAC protocol.
- **Packet Delivery Ratio and Packet Loss Rate**

$$\begin{aligned}\textbf{Packet delivery ratio} = {}&\text{Number of packets successfully received at the sink}/\\&\text{Number of packets sent by the source node}\end{aligned} \tag{8}$$

  The packet loss rate counts the number of packets lost in the path from source node to the Sink node. So this may be considered as a matrix to measure the reliability.
- **Scalability and Adaptability**
  Sensor nodes are battery operated low power nodes and deployed in the order of hundreds and thousands. The links may be disappearing if the node dies after some time. So a good MAC protocols should be adaptive to changes in network size, node density and topologies.
- **Reliability**
  This is very important parameter for mission critical MAC protocols as the data which is delivered to the base station for further action should be trustworthy.
- **Degree of Intelligence**
  This is the parameter which is new to these protocols and will be provided by introducing the Machine learning and Artificial Intelligence to the MAC models. The degree of intelligence will be formulated according to the application in each mission critical protocol.

The degree of intelligence can be provided using the machine learning (ML) techniques in MAC protocols. It's the processes which if induced in the protocol, provide self learning from the past experiences.

4.1 Case Study of ADMC-MAC

4.1.1 Comparative Performance Analysis of ADMC-MAC with SMAC Protocol by Varying Duty Cycles

The SMAC protocol gives the packet delivery ratio at 40 s packet inter arrival rate or greater than that, fails at high traffic rates. MAC protocol sends packets only at 40 s packet inter arrival time when duty cycle is 10%. But ADMC-MAC works for very high traffic rate also when the packet inter arrival time .1 s at 10% duty cycle. ADMC-MAC gives the throughput and PDR at all traffic rates starting from .1 s packet inter arrival time. The performance parameters for mission critical MAC are calculated and compared with SMAC protocol for 20% duty cycle.

4.1.1.1. Residual Energy at 20% Duty Cycle

Network residual energy of SMAC and ADMC-MAC protocol are compared in Figs. 10 and 11. Here it's observed that the residual energy performance of ADMC-MAC is better in high traffic. At 1 s packet inter arrival time in high traffic rates, the intermediate nodes near source lose their energy. They will be at high duty cycle most of the time. Same is the case in low traffic rate of 30 s packet inter arrival time. The intermediate nodes are in medium value of duty cycle but for longer time. So they lose their energy. Hence ADMC-MAC is unable to perform better than SMAC on few points at 20% duty cycle.

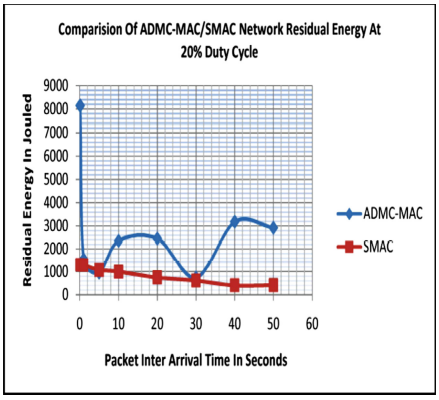


Fig. 10. ADMC-MAC/SMAC network residual energy

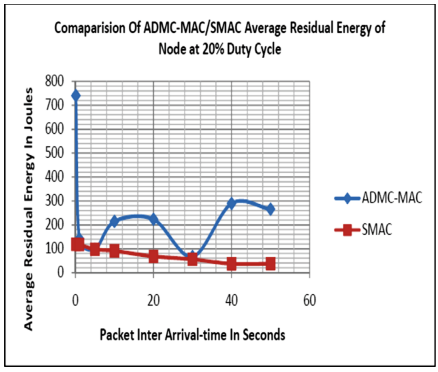


Fig. 11. ADMC-MAC/SMAC Average Residual Energy of node

4.1.1.2 Packet Delivery Ratio and Throughput Performance at 20% Duty Cycle

As observed from graph in Fig. 12, the PDR performance of ADMC-MAC at 20% duty cycle is better in very high traffic scenario only.

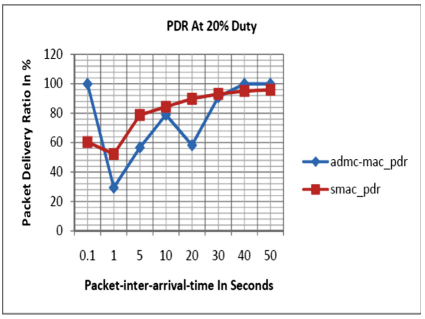


Fig. 12. PDR comparisons at 20% duty cycle

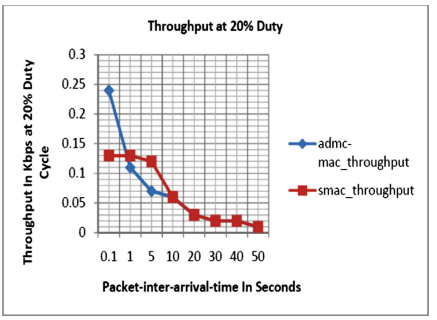


Fig. 13. Comparison of throughput at 20% duty cycle

So it's depicted from graph in Fig. 12 that ADMC-MAC may not be used at 20% duty cycle for mission critical scenarios. Its observed in graph drawn in Fig. 13, that ADMC-MAC has almost equivalent throughput performance to SMAC protocol except at very high traffic scenario (0.1 s).

It has been observed in the graphical representations, that at very low packet inter arrival time, the energy saving, PDR and throughput performance of ADMC-MAC is better than SMAC. At medium and low traffic rates, the throughput performance is almost equivalent to SMAC and PDR performance is deteriorating as packet inter arrival time increases. So if we choose duty cycle of ADMC-MAC 20%, then the performance is good only at high traffic rates and almost equivalent to SMAC at medium and low traffic rates.

4.1.1.3 Residual Energy Performance for 40% Duty Cycle

The ADMC-MAC protocol is tested for mission critical scenarios when operated at 40% duty cycle.

- At very high traffic the energy saving is enhanced by 71.45% and at high traffic rate, enhanced by 13%.
- In medium and low traffic rates, the energy saving performance is enhances by average 25%.
- Using proposed algorithms, the ADMC-MAC protocol improved energy saving in very high traffic by 70%, in medium traffic by 13% and in very low traffic by 25%.

4.1.1.4 Throughput Performance Comparison at 40% Duty Cycle

- SMAC protocol when operate at 40% duty cycle give best throughput but since it has static duty cycle so the nodes stay at same duty cycle in low traffic too. The throughput is achieved at the cost of energy wastage.
- At 40% duty cycle the ADMC-MAC protocol minimize the energy losses and gives comparable throughput as SMAC does in 40% duty cycle. So the purpose of mission critical applications is served using ADMC-MAC.

4.1.1.5 Packet Delivery Ratio Performance at 40% Duty Cycle

In mission critical case the PDR of ADMC-MAC is 100% whereas of SMAC protocol is 84.801%.

5 The Machine Learning Techniques Used for MAC Protocols

Machine learning solves many complex problems with simple programming [68]. As discussed in [71] by Sun et al. that ML can be used in resource management at MAC layer long with networking and security at upper layers also. We will first review the basic machine learning techniques to develop an understanding to apply them in MAC protocols for their improvements. Based on the learning mechanism, the ML techniques are categorized mainly into supervised and unsupervised learning. The unsupervised learning, semi supervised learning and reinforcement learning techniques also comes under ML. Here we will review only the supervised learning as these are the simple techniques and give an overview of using ML in WSN for solving the issues at MAC level.

5.1 Machine Learning Techniques

In supervised learning, a relation is developed between the given set of inputs and outputs during learning process. A function is derived from input x and the estimated output y. Supervised learning provide the solution for wireless sensor networks in mission critical scenarios at each layer related to for deployments strategies, data aggregation, security, routing, end to end connectivity etc. But for MAC layer it can play a role in designing intelligent MAC protocols for event detection, energy harvesting, increasing the energy efficiency and lifetime of network, latency improvement and timely and reliable data delivery performance. Various techniques are discussed in [53–57] for designing the MAC protocols related to traffic management and power managements using machine learning techniques.

Regression and classification are the two types of supervised learning.

Regression: It is one of the type supervised learning used for designing a mission critical MAC protocol for wireless sensor networks as discussed in [58]. The regression model is used to build the mathematical function Y based one or multiple predictor [59]

variables(x). The work done in [58] used a regression technique and derived a function for forecasting the output as given by Eq. 6.

$$Y = f(x) + \text{possible random error} \tag{9}$$

Regression is used for duty cycle calculation of selected node. Regression is used to solve various issues in wireless sensor networks which include energy harvesting mechanisms, data aggregations, event detecting and efficient routing etc. [60, 61].

Decision Tree: This ML technique is based on if then else rules and makes the process of decision making free from ambiguity. This technique is used for solving the issues related to path finding and data aggregations in MAC and routing protocols [62]. Random Forest: In random forest algorithm, the data sets are huge and heterogeneous. The random forest is discussed in [63] in detail. In [64] the RF technique is used for developing a protocol in monitoring the devices for health assessments at industrial level. In offline phase, the algorithms collect the features of devices and make decision tress. The process continues till the maximum number of tress is reached. In the online phase the health of the devices are tested and classified accordingly. So this work is used for assessment of health of the devices by monitoring the parameters of devices using wireless sensor networks. RF can be further used to solve MAC issues in WSN for making the protocols more intelligent as discussed in [53].

Artificial neural network is a ML technique based on neurons in the brain of human body. This is a layered architecture, having nodes on each layer and these nodes are connected through function and provide connectivity among layers. In [65] a technique for finding the energy exhaustion attacks is developed using ANN. It is developed for cluster-based WSN and includes energy harvesting systems. Many issues on MAC layer like link failure, event detection, network residual energy improvements are solved using ANN. Deep learning is also one category of ML with multilayer representation. It has also been used to resolve the issues at MAC level in WSN. Support machine vector is a powerful ML algorithm and is used to find the hyperlane in N-dimensional space that classify the data points. The dimension of hyperlane depends upon the number of features. The SVM model can be developed in PYTHON language for the data set. The redundant data can be identified using this SVM technique. So in MAC layer this technique can help to reduce the redundant traffic on the network and hence can enhance the timely and reliable data delivery performance. The work done in [66, 67] uses SVM to solve the issues related to link quality and congestion control for wireless sensor networks. Other ML techniques like **Bayesian and k-nearest neighbor** also comes under supervised learning and well used for solving the MAC issues for WSN. Also Singh et al. discussed [70] some latest trends for network communication. So accordingly the machine learning algorithm can be chosen to achieve the mission critical protocol requirement.

5.2 Proposed Application of Machine Learning Based Mission Critical MAC Protocol

The exponentially growing demand of oil and gases is the major factor of pipeline leakage detection system. The intelligent and automatic monitoring for pipeline leakage

is need of the hour as all our gas distribution systems, oil refineries and water distribution system using these pipelines. Hence it is an important issue to be addressed by researchers and the public. Pipeline leakage if not reported on time may cause a disaster at major level destroying the lives of million people.

According to the Research and Markets reports oil and gas pipeline leakage detection system will occupy $2.5 billion by the end of year 2019 in United States alone and will reach $4.05 billion by 2025. Wireless sensor networks (WSN) use radio communication to transmit sensed signals if leakage is detected. One of the major deployment issues of WSN is the energy consumption so we need to design protocols for maximizing the lifetime of network. Pressure analysis is a method preferably used for leak detection systems. This method requires a constant measurement of pressure in various locations along the pipe.

Using recent machine learning techniques, Mission Critical intelligent MAC protocol will be designed to deliver the data timely and reliably along with minimizing the overall power consumption of Wireless Sensor Nodes deployed for leakage detection.

These aspects provide motivation for designing a system which includes following

Objectives

1. Design a low power WSN node with pressure sensor and gas sensors for detection of leakage in pipes.
2. To design Energy Efficient Machine learning based Mission Critical MAC protocol for Pipeline Leakage Detection System.
3. Using Wi-Fi® single-chip microcontroller (MCU) with built-in Wi-Fi connectivity designs an Internet of Things (IoT) application to send alert to the respective nearby server location to fix the threat immediately and send warning to the people residing in the nearby location.

This is an example problem which can be solved by designing a Machine learning MAC protocol for wireless sensor networks as shown in Fig. 14.

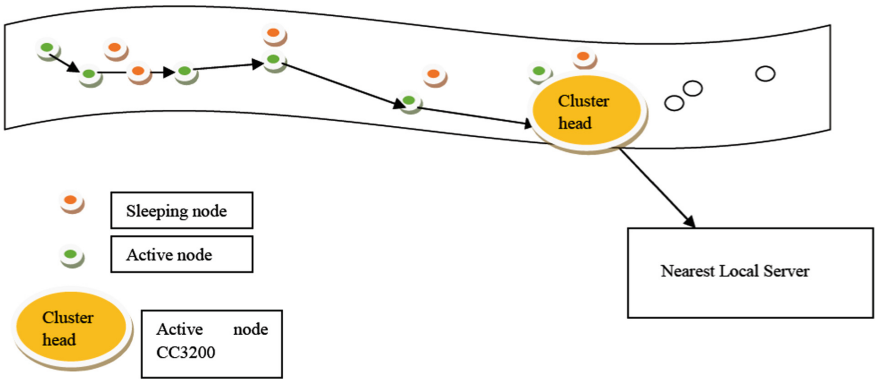


Fig. 14. A mission critical protocol model for pipeline leakage detection using wireless sensor networks.

The protocol designing will include the ML techniques for making it intelligent. According to the criticality of the leakage the information will be transferred to the local server through IoT and then to the main server through cloud application.

5.3 Recent Issues and Challenges

An efficient MAC protocol is required for mission critical applications in wireless sensor networks. Since the nodes are deployed in the areas not easily accessible so energy efficient MAC protocols are required for handling such situations. Reducing energy consumption is an important aspect. Since nodes are deployed in remote or unattended areas, and they are powered by battery or solar energy hence there energy must be preserved to enhance the network lifetime. Efficient utilization of bandwidth is also important. High channel utilization is required to deliver a large number of packets with minimum delay. Throughput refers to the amount of data successfully transferred from sender to receiver in a given time. In many wireless sensor network applications such as patient monitoring or battle field surveillance, it is required to have data delivery in a limited time period. Latency: Latency is the delay counted since a senor node has a packet to send till the packet is successfully received at the receiver node. Monitoring applications can tolerate some latency but in mission critical applications like monitoring pressure in gas pipelines, the latency becomes an important issue to be handled by MAC protocol. Scalability and Adaptability: Sensor nodes are battery operated low power nodes and deployed in the order of hundreds and thousands. The links may be disappearing if the node dies after some time. So the good MAC protocols should accommodate changes in network size, node density and topologies. Reliability: This is very important parameter for mission critical MAC protocols as the data which is delivered to the base station for further action should be trustworthy. Degree of Intelligence is the most important parameter. This is the parameter which is new to these protocols and will be provided by introducing the Machine learning and Artificial Intelligence to the MAC models.

So the observation says that energy cannot be sufficient performance parameter to design an efficient MAC protocol. In most of the protocols reducing energy consumption is the main objective. Only few have considered the energy and latency both. There are very few protocols in the survey which has talked about the energy, delay (latency) and the reliable data transmission which is the requirement of a MAC protocol suitable for mission critical applications.

6 Conclusion and Future Scope

The machine learning algorithms reviewed above can be used to enhance the existing MAC protocol models. Using these ML techniques, the protocol model will become intelligent to take decisions according to the traffic conditions, residual energy of nodes and on the bases of event priority. The ADMC-MAC is one of the protocols discussed above, which uses regression technique and works for mission critical scenarios. In smart city projects, we need to design the applications like smart pipeline leakage detection using IoT, smart security systems, smart fire detection systems etc. All these

applications use wireless sensor networks along with IoT. So accordingly the MAC protocol design needs the paradigm shift from tradition models. All this is possible with the help AI and machine learning techniques for designing the new updated protocol models according to the state-of-the-art applications.

Acknowledgement. This research is funded by AKTU Lucknow (U.P.) as award of grant under "Collaborative Research Innovation Program (CRIP) funding through TEQUIP-III of AKTU" 2019-20. The reference number of grant is AKTU/Dean-PGSR/2019/CRIP/44.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
2. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)
3. Kazem, S., Daniel, M., Taineb, Z.: Wireless Sensor Networks: Technology, Protocols, and Applications. Wiley, Hoboken (2007)
4. LAN-MAN Standards Committee of the IEEE Computer Society, Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE, New York (1997). (IEEE Std 802.11-1997 edition)
5. Demirkol, I., Ersoy, C., Alagoz, F.: MAC protocols for wireless sensor networks: a survey. IEEE Commun. Mag. **44**(4), 115–121 (2006)
6. Ye, W., Heidemann, J., Estrin, D.: An energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the IEEE INFOCOM, New York, NY, vol. 3, pp. 1567–1576, June 2002
7. Ye, W., Heidemann, J., Estrin, D.: Medium access control with coordinated adaptive sleeping for wireless sensor networks. IEEE/ACM Trans. Netw. **12**(3), 493–506 (2004)
8. Ameen, M.A., Islam, S.M.R., Kwak, K.: Energy saving mechanisms for MAC protocols in wireless sensor networks. Int. J. Distrib. Sens. Netw. **6**(1), 163413 (2010)
9. Suriyachai, P., Roedig, U., Scott, A.: A survey of MAC protocols for mission-critical applications in wireless sensor networks. IEEE Commun. Surv. Tutor. **14**(2), 240–264 (2012). (Second Quarter)
10. Karl, H., Willig, A.: Protocols and Architectures for Wireless Sensor Networks. Wiley, Hoboken (2005)
11. Mishra, S.C., Woungang, I., Mishra, S.: Guide to Wireless Sensor Networks. Springer, London (2009)
12. Ali, M., Böhm, A., Jonsson, M.: Wireless sensor networks for surveillance applications – a comparative survey of MAC protocols. In: The Fourth International Conference on Wireless and Mobile Communications, Athens, pp. 399–403 (2008)
13. Stoianov, I., Nachman, L., Madden, S., Tokmouline, T.: PIPENET: a wireless sensor network for pipeline monitoring. In: 6th International Symposium on Information Processing in Sensor Networks, Cambridge, MA, pp. 264–273 (2007)
14. Casey, K., Lim, A., Dozier, G.: A sensor network architecture for tsunami detection and response. Int. J. Distrib. Sens. Netw. **4**(1), 27–42 (2008)
15. Tan, R., Xing, G., Chen, J., Song, W.Z., Huang, R.: Quality-driven volcanic earthquake detection using wireless sensor networks. In: 2010 31st IEEE Real-Time Systems Symposium, San Diego, CA, pp. 271–280 (2010)

16. Kumar, S., Raghavan, V.S., Deng, J.: Medium access control protocols for ad hoc wireless networks: a survey. AdHoc Netw. **4**(3), 326–358 (2006)
17. Jamieson, K., Balakrishnan, H., Tay, C.: Sift: a mac protocol for event-driven wireless sensor networks. ESWN **6**, 260–275 (2006)
18. El-Hoiydi, A., Decotignie, J.D.: WiseMAC: an ultra low power MAC protocol for multi-hop wireless sensor networks. In: Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2004). Lecture Notes in Computer Science, vol. 3121, pp. 81–31. Springer, Berlin (2004)
19. Lu, G., Krishnamachari, B., Raghavendra, C.S.: An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In: Proceedings of the 18th International Parallel and Distributed Processing Symposium, p. 224, April 2004
20. Li, Y., Ye, W., Heidemann, J.: Energy and latency control in low duty cycle MAC protocols. In: Proceedings of IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, vol. 2, pp. 676–682 (2005)
21. Hussain, S.W., Khan, T., Zaidi, S.M.H.: Latency and energy efficient MAC (LEEMAC) protocol for event critical applications in WSNs. In: Proceedings of International Symposium on Collaborative Technologies and Systems, Las Vegas, NV, USA, pp. 370–378 (2006)
22. Dam, T.V., Langendoen, K.: An adaptive energy-efficient MAC protocol for wireless sensor networks. In: The First ACM Conference on Embedded Networked Sensor Systems (Sensys 2003), Los Angeles, CA, USA, pp. 171–180, November 2003
23. Rajendran, V., Obraczka, K., Aceves, J.J.: Energy efficient, collision-free medium access control for wireless sensor networks. In: Proceedings of ACM (SenSys 2003), Los Angeles, California, pp. 181–192, November 2003
24. Lin, P., Qiao, C., Wang, X.: Medium access control with a dynamic duty cycle for sensor networks. In: IEEE Wireless Communications and Networking Conference, vol. 3, pp. 1534–1539, 21–25 March 2004
25. Ezzedine, T., Miladi, M., Bouallegue, R.: An energy-latency-efficient MAC protocol for wireless sensor networks. Int. J. Electr. Comput. Eng. **4**(13), 816–821 (2009)
26. Tseng, H.W., Yang, S.H., Chuang, P.Y., Wu, H.K., Chen, G.H.: An energy consumption analytic model for a wireless sensor MAC protocol. In: Proceedings of the IEEE Vehicular Technology Conference (VTC 2004), pp. 4533–4537 (2004)
27. Hamady, F., Sabra, M., Sabra, Z., Kayssi, A., Chehab, A., Mansour, M.: Enhancement of the S-MAC protocol for wireless sensor networks. In: 2010 International Conference on Energy Aware Computing, Cairo, pp. 1–4 (2010)
28. Ammar, I., Awan, I., Min, G.: An improved S-MAC protocol based on parallel transmission for wireless sensor networks. In: Proceedings of 13th International Conference on Network-Based Information Systems (NBIS 2010), pp. 48–54. IEEE Computer Society, Washington (2010)
29. Xia, F., Zhao, W., Sun, Y., Tian, Y.C.: Fuzzy logic control based QoS management in wireless sensor/actuator networks. Sensors **7**, 3179–3191 (2007). (Basel Switzerland)
30. Yusuf, M., Haider, T.: Energy-aware fuzzy routing for wireless sensor networks. In: Proceedings of the IEEE Symposium on Emerging Technologies, pp. 63–69 (2005)
31. Misra, S., Mohanta, D.: Adaptive listen for energy-efficient medium access control in wireless sensor networks. J. Multimed. Tools Appl. **47**(1), 121–145 (2010)
32. Mishra, C.K., Acharya, B.M., Das, K., Pati, P.S.: EX-SMAC: an adaptive low latency energy efficient MAC protocol. Int. J. Comput. Sci. Eng. IJCSE **3**(4), 1485–1489 (2011)
33. Ramakrishnan, S., Mullen, J.: Impact of sleep in wireless sensor MAC protocol. In: Vehicular Technology Conference, VTC2004-Fall. IEEE 60th Conference, vol. 7 (2004)

34. Ramchand, V., Lobiyal, D.K.: An analytical model for power control T-MAC protocol. Int. J. Comput. Appl. **12**(1), 975–8887 (2010)
35. Arisha, K.A., Youssef, M.A., Younis, M.F.: Energy aware TDMA based MAC for sensor network. In: IEEE Workshop on Integrated Management of Power Aware Communications Computing and Networking (2002)
36. Barroso, A., Roedig, U., Sreenan, C.: μ-MAC: an energy efficient medium access control for wireless sensor networks. In: Proceedings of the Second European Workshop on Wireless Sensor Networks, pp. 70–80 (2005)
37. Campelli, L., Capone, A., Cesana, M., Ekici, E.: A receiver oriented MAC protocol for wireless sensor networks. In: Proceedings of IEEE MASS 2007, pp. 1–10, 8–11 October 2007
38. Rhee, I., Warrier, A., Aia, M., Min, J.: ZMAC: a hybrid MAC for wireless sensor networks. In: Proceedings of the Third ACM Conference on Embedded Networked Sensor System (Sensys 2005), pp. 90–101 (2005)
39. Hamid, M.A., Wadud, M., Chong, I.: A schedule-based multi-channel MAC protocol for wireless sensor networks. Sensors **10**, 9466–9480 (2010)
40. Zhou, G., Huang, C., Yan, T., He, T., Stankovic, J.A., Abdelzaher, T.F.: MMSN: multi-frequency media access control for wireless sensor networks. In: Proceedings of IEEE INFOCOM, 25TH IEEE International Conference on Computer Communications, Barcelona, Spain, pp. 1–13 (2006)
41. Incel, O.D., Dulman, S., Jansen, P.: Multi-channel Support for dense wireless sensor networking. In: EUROSSC, LNCS, vol. 4272, pp. 1–14 (2006)
42. Chen, X., Han, P., He, Q.S., Tu, S.L., Chen, Z.L.: A multi-channel MAC protocol for wireless sensor networks. In: The Sixth IEEE International Conference on Computer and Information Technology (CIT 2006), Seoul, p. 224 (2006)
43. Incel, O.D., Jansen, P.G., Mullender, S.J.: MC-LMAC: a multi-channel mac protocol for wireless sensor networks. Technical Report TR-CTIT-08-61, Centre for Telematics and Information Technology, University of Twente, Enschede (2008)
44. Du, S., Saha, A.K., Johnson, D.B.: RMAC: a routing-enhanced duty-cycle MAC protocol for wireless sensor networks. In: Proceedings of the 26th IEEE International Conference on Computer Communications, pp. 1478–1486 (2007)
45. Cho, K.T., Bahk, S.: Optimal hop extended MAC protocol for wireless sensor networks. Comput. Netw. **56**, 1458–1469 (2012)
46. SCADDS: Scalable Coordination Architectures for Deeply Distributed Systems web page. http://www.isi.edu/scadds/projects/smac/
47. The Network Simulator - ns-2 homepage. http://www.isi.edu/nsnam/ns/
48. The VINT project. The NS Manual. UC Berkeley, LBL, USC/ISI, and Xerox PARC. http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf
49. Greis, M.: Tutorial for the network simulator ns. http://www.isi.edu/nsnam/ns/tutorial/index.html
50. Smac-users – Discussions by users of S-MAC web page. http://mailman.isi.edu/mailman/listinfo/smac-users
51. Energy Model Update in ns-2 web page. http://www.isi.edu/ilense/software/smac/ns2_energy.html
52. http://www.isi.edu/nsnam/ns/
53. Alotaibi, B., Elleithy, K.: A new MAC address spoofing detection technique based on random forests. Sensors **16**(3), 1–14 (2016)
54. Habib, C., Makhoul, A., Darazi, R., Salim, C.: Self-adaptive data collection and fusion for health monitoring based on body sensor networks. IEEE Trans. Ind. Inf. **12**(6), 2342–2352 (2016)

55. Pérez-Solano, J.J., Felici-Castell, S.: Adaptive time window linear regression algorithm for accurate time synchronization in wireless sensor networks. Ad Hoc Netw. **24**, 92–108 (2015)
56. Rezaee, A.A., Pasandideh, F.: A fuzzy congestion control protocol based on active queue management in wireless sensor networks with medical applications. Wirel. Pers. Commun. **98**(1), 815–842 (2018)
57. Sharma, A., Kakkar, A.: Forecasting daily global solar irradiance generation using machine learning. Renew. Sustain. Energy Rev. **82**(P3), 2254–2269 (2018)
58. Sakya, G., Sharma, V.: ADMC-MAC: energy efficient adaptive MAC protocol for mission critical applications in WSN. Sustain. Comput. Inform. Syst. **23**, 21–28 (2019). https://doi.org/10.1016/j.suscom.2019.05.001. (ISSN 2210-5379)
59. Vining, G.G., Peck, E.A., Montgomery, D.C.: Introduction to Linear Regression Analysis, vol. 821. Wiley, Hoboken (2012)
60. Sun, W., Yuan, X., Wang, J., Li, Q., Chen, L., Mu, D.: End-to-end data delivery reliability model for estimating and optimizing the link quality of industrial WSNs. IEEE Trans. Autom. Sci. Eng. **15**, 1127–1137 (2017)
61. Song, X., Wang, C., Gao, J., Hu, X.: DLRDG: distributed linear regression-based hierarchical data gathering framework in wireless sensor network. Neural Comput. Appl. **23** (7–8), 1999–2013 (2013)
62. He, H., Zhu, Z., Mäkinen, E.: Task-oriented distributed data fusion in autonomous wireless sensor networks. Soft. Comput. **19**(8), 2305–2319 (2015)
63. Belgiu, M., Drăguţ, L.: Random forest in remote sensing: a review of applications and future directions. ISPRS J. Photogramm. Remote Sens. **114**, 24–31 (2016)
64. Elghazel, W.: Wireless sensor networks for Industrial health assessment based on a random forest approach. Automatic. Université de Franche-Comté (2015). (English. NNT: 2015BESA2055. tel01725629)
65. Alrajeh, N.A., Khan, S., Mauri, J.L., Loo, J.: Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting. Ad Hoc Sens. Wirel. Netw. **22**(1–2), 109–133 (2014)
66. Shu, J., Liu, S., Liu, L., Zhan, L., Hu, G.: Research on link quality estimation mechanism for wireless sensor networks based on support vector machine. Chin. J. Electron. **26**(2), 377–384 (2017)
67. Gholipour, M., Haghighat, A.T., Meybodi, M.R.: Hop-by-hop congestion avoidance in wireless sensor networks based on genetic support vector machine. Neurocomputing **223**, 63–76 (2017)
68. Kumar, D.P., Amgoth, T., Annavarapu, C.S.R.: Machine learning algorithms for wireless sensor networks: a survey. Inf. Fusion **49**, 1–25 (2019)
69. Sakya, G., Sharma, V.: MAC protocol with regression based dynamic duty cycle feature for mission critical applications in WSN. Int. J. Adv. Comput. Sci. Appl. **8**(6), 198–206 (2017). (E-SCI, Thomson Reuters, Web of Science)
70. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
71. Sun, Y., Peng, M., Zhou, Y., Huang, Y., Mao, S.: Application of machine learning in wireless networks: key techniques and open issues. IEEE Commun. Surv. Tutor. **21**, 3072–3108 (2019)

QoS Routing for Data Gathering with RPL in WSNs

Miklós Molnár(✉)

LIRMM, University of Montpellier, CNRS, Montpellier, France
molnar@lirmm.fr

Abstract. Generally, data collected by sensors must be sent to a sink node using multi-hop routing. Some applications can raise different requirements, constraints for the quality of data forwarding, for instance on end-to-end delay, jitter, packet loss, etc. Often, a set of constraints must be satisfied. Several proactive and reactive routing protocols have been proposed for WSNs. One of them is the standardized proactive RPL (Routing Protocol for Low-Power and Lossy Networks) designed essentially for many to one communication. For the data gathering a destination oriented directed acyclic graph (DODAG) is used which is mainly a tree directed to the sink. The computation of the tree-like DODAG is based on an Objective Function which can also be defined on QoS metrics but is usually based on one metric. This chapter deals with QoS routing in general and in WSNs using RPL in particular and proposes the analysis of the QoS constrained routes. We demonstrate that the set of QoS routes from sensors to the sink is not always a tree. It corresponds to a generalization of trees: to a hierarchy. The QoS aware hierarchies can be considered as special DODAGs. The routes are directed to the sink, and there is no useless cycle. The configuration of them and the data forwarding need some adjustments of the routing protocol which are also presented.

1 Introduction, Motivation

The principal mission of Wireless Sensor Networks (WSNs) is measurement, monitoring and collection of data involved. In many applications data must be sent to a sink node, typically to a base station or to a border router. WSNs have many applications needing a defined Quality of Service (QoS). These applications are from environment, health and object monitoring and measurement to intrusion detection, multimedia applications in industrial control systems, real-time surveillance and alerts, etc.

From the point of view of network services, QoS characterizes the guaranties/requirements that the network should offer/satisfy to the end users of a service. QoS may be defined by a set of conditions to fulfill by a communication between a source and a destination (Crawley et al. 1998). Several elements are available to network operators to provide QoS in the network and in different OSI protocol layers. In our study, we consider that the majority of tools belongs to two main categories:

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 87–111, 2020.
https://doi.org/10.1007/978-3-030-40305-8_6

- tools using traffic engineering (TE) to manage the packet forwarding
- QoS aware routing to compute routes offering the asked guaranties.

TE proposes several tools to manage the traffic and help QoS. One can refer to classifications of flows, class based and/or priority based solutions, different policy based scheduling to handle queues, flow rate limitations to avoid congestions (*e.g.,* flow control in TCP or traffic shaping). For reliability, acknowledgment based solutions are implemented to avoid packet losses in TCP and also in the CSMA/CA mechanism in some MAC layer protocols in wireless networks. Fault tolerance and reliability can be improved with multi-path routing and sending several copies of a message using independent routes.

The most known QoS aware solutions in the Internet are Intserv and Diffserv. Integrated Services (IntServ) is based on an individual reservation of resources for each flow using RSVP. This solution is not scalable, needs high resource consumption on the network nodes and can not be applied in WSNs. Differentiated Services or DiffServ is a more affordable solution to meet the QoS requirements in the Internet. The DiffServ approach operates on the principle of traffic classification, ensuring preferential treatment for higher-priority traffic classes (The Cisco Learning Network, 2017). The Software Defined Network concept permits to apply sophisticated mechanisms. A review of TE tools both in classic networks and Software Defined Networks can be found in (Abbasi et al. 2016).

Unfortunately, due to the limited capacities of the components, resource-intensive solutions of TE can not be applied to sensor networks.

Generally, WSNs are composed of autonomous, battery-powered, small and cheap sensors partially far from the base station. Sensors use short radio range to communicate. To collect data, multi-hop routing is needed. Moreover, some of the applications can raise different requirements for the quality of the measured data and also for the quality of the data forwarding mechanism. In our chapter we talk about the quality of the data forwarding, more especially of the routing in WSNs. The required QoS may include end-to-end delay, jitter, packet loss, or other critical parameters.

Frequently, the requirements are formulated as constraints and to forward data with respect to the QoS, not only one constraint but a set of constraints must be satisfied. Often, low power consumption is the primary objective of the routing decision, since the transmission of data from sensors to the sink is consumes important energy. For route computation, the used model is the topology graph with values assigned to the edges and nodes. Each constraint is based on a link or node metric and the set of constraints can be represented by vectors. The routing decision can be seen as a mono/multi objective multi-constrained optimization problem. In common cases, we suppose only one objective (*cf.* Sect. 2). The computation of a simple path satisfying more than one constraint or an optimal (shortest) path under an additional constraint in the graph is NP-hard. In our scenario, a set of sensors should transmit data to the sink: the routing concerns a set of paths directed to the sink. We will use the term of *incast* communication to describe it. We consider the general case of the multi-constrained

incast route computation when several QoS criteria are concerned in the optimization. The QoS incast route should contain a feasible path from each sensor to the sink node. An important property of the optimal (and also for some non optimal but feasible) solutions is that the set of feasible paths is not always a tree as it is expected, but may correspond to a generalization of trees: to a hierarchy (Molnár 2011).

In this chapter we deal with QoS routing in general and QoS routing in WSNs using RPL in particular. The background of the multi-constrained path (and more generally route) computation is discussed shortly in Sect. 2. The optimal solution of the incast routing problem is also presented. QoS aware solutions in WSNs are over-viewed in Sect. 3. One of the standardized routing protocols proposed for low-power and lossy networks is the protocol RPL (Routing Protocol for Low-Power and Lossy Networks) designed essentially for incast (many to one) communication (Gaddour and Koubâa 2012). In Sect. 4 RPL is briefly presented and the QoS aware propositions using RPL are discussed in Sect. 5. For the data gathering a destination oriented directed acyclic graph (DODAG) is used which is mainly a tree directed from the sensors to the sink. The computation of the tree-like DODAG is based on an Objective Function which can be defined on some QoS metrics. Only a few Objective Functions are proposed and the existing functions are usually based on one metric (*cf.* examples in (Farooq et al. 2017)). In Sect. 5 we present how to satisfy several QoS constraints for data gathering using RPL. It is shown that the QoS aware hierarchies correspond to special DODAGs, the routes are directed to the sink, and there is no useless cycle. The configuration of these routes and the data forwarding need some adaptations of the routing protocol which are also presented.

2 QoS Constrained Routing

A lot of practical applications in recent networks require QoS and an important element to obtain the required quality is to make "good" routing decisions. In this section we resume the theoretical base of the QoS aware route computation. We are motivated by the computation of incast route. To introduce the multi-constrained incast routing problem, at first we propose a brief study of the multi-constrained path computation. Since there are important similitudes between broadcast and incast routes, we also present some significant results for QoS constrained broadcast/multicast routing, then we formulate the incast routing. In both cases (broadcast and incast), the optimal (and sometimes the existing feasible) solutions are not always trees. We present the route structure called hierarchy to precisely define the solution we are looking for.

2.1 Graph Model

The appropriate model for route computations is based on the topology graph $G = (V, E)$ of the network representing the node set V and the links by the set E. The graph can be directed or not, depending on the real conditions of links.

To simplify, we suppose an undirected graph with edge set E. Let us suppose that the state of the network is partially or entirely known to make routing decisions. Namely, the state of the links and nodes is described by appropriate parameters. Some of them correspond to QoS related metrics like the delay of transmission, the corresponding jitter, the probability of packet losses, etc. For the route computation, we suppose that:

- only the links have QoS parameters; if eventually there are parameters for the nodes, then each node can be replaced by an equivalent small complete graph in which the internal links are associated with the parameter set;
- the parameters are additive; multiplicative values can be transformed into additive ones using the logarithm function and bottleneck type parameters can be treated by link eliminations.

Frequently, the requirements are formulated as constraints on the end-to-end parameter values and not only one constraint but a set of constraints must be satisfied for the QoS. Often, low power consumption is the primary objective of the routing decision, since the transmission of data from sensors to the sink is very energy consuming. In these cases, the routing decision can be seen as a mono objective multi-constrained optimization problem in the valuated topology graph.

2.2 Computation of Constrained Paths

In the simplest case a QoS path should be found for a (source, destination) pair. The computation of a simple shortest path satisfying at least one additional constraint is an NP-hard problem. The determination of optimal paths is not suitable in large networks despite the fact that efficient models and methods have been proposed to solve it (Lozano and Medaglia 2013). A significant part of QoS aware applications require multi-constrained routes. In a WSN, a set of sensors should transmit data to the sink: the routing concerns a set of paths directed to the sink satisfying a set of QoS constraints such as limited delay, jitter, bandwidth, loss rate etc. Evidently the computation of an optimal or even a feasible solution is a hard problem.

In order to facilitate the discussion of the QoS aware incast route, in the next sub section, we propose a brief presentation of the optimal multicast route for two reasons. (1) The QoS aware multicast route computation has already been deeply analyzed, (2) Due to important similitudes, this analysis permit the definition of the optimal incast route for WSNs.

2.3 Constrained Multicast/Broadcast

It is well known that routes for multicast and broadcast are usually directed trees relaying the source to the destinations. Especially, these trees may be shortest path trees, minimum spanning trees (MSTs) which can be computed in polynomial time or approached minimum Steiner trees, knowing that the Steiner problem is NP-hard.

The QoS constraints strongly impact the multicast/broadcast routes. Since the computation of a single constrained shortest path is expensive, the shortest path tree under a QoS constraint is also difficult to compute. It is easy to see that the minimum cost multicast/broadcast route under a single QoS constraint is also a tree but this computation is NP-hard. To illustrate, the delay constrained multicast routing problem was first formulated in (Kompella et al. 1992). The diameter constrained Steiner tree problem is resumed in (Ding et al. 2010), where the diameter is the maximal distance of any node pair in the tree. The weight constrained minimum cost Steiner tree is analyzed in (Chen et al. 2003) where an additive arbitrary weight is limited on the arcs of the tree. Inversely, the minimum diameter cost constrained Steiner tree problem is presented in (Ding and Xue 2012). The delay constrained minimum spanning tree (DCMST) problem where all the nodes in the network are concerned was introduced in (Salama et al. 1997). It is an interesting case for our study, because the data gathering in a WSN must cover the entire set of the nodes with the difference that in the data gathering the communications are oriented to the sink (root) node. Figure 1 illustrates the DCMST for a broadcast in blue arrows and the delay constrained minimum cost incast tree in red. All the mentioned problems are NP-hard.

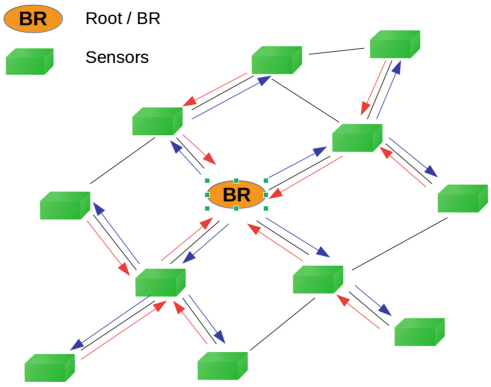


Fig. 1. Illustration of a DCMST directed from a source to the other nodes (with blue arrows) and a delay constrained minimum cost incast tree directed from the nodes (sensors) to the sink (with red arrows) in the same non directed graph. The base of the two tree is the same DCMST, only the direction is different in the two cases

The computation is a more challenging and hard task when the communication should respect several constraints. Often, the proposed algorithms aim at the construction of a (minimum) spanning tree satisfying the set of QoS constraints. A recent work illustrates this construction of the spanning trees (Kumar and Singamsetty 2018). Let us formulate the multi-constrained multicast/broadcast routing problem as follows.

Definition 1 (The minimum cost multi-constrained multicast/ broadcast problem)

Let $G = (V, E)$ be a connected topology graph. A positive cost $c(e)$ and a vector $\overrightarrow{w}(e) = (w_1(e), w_2(e), ..., w_k(e))^T$ of positive, additive weights are associated to each edge/arc $e \in E$. Let $s \in V$ be the source node and $D \subseteq V \setminus \{s\}$ the set of destinations. Let $\overrightarrow{L}$ be the vector of tolerated maximal QoS values on any path. Consequently, a path from s to $d \in D$ is a feasible QoS path, if its weight vector respects $\overrightarrow{w}(p_{s,d}) \overset{d}{\leq} \overrightarrow{L}$, where $\overset{d}{\leq}$ is the Pareto dominance. The minimum cost multi-constrained multicast/broadcast problem is to find a route offering a feasible path from the source to each destination minimizing the cost of the route.

Notice that the cost of the route should be defined. If the route is a sub-graph (a tree) and the packets take each edge of the sub-graph only once, then the cost of the route is the sum of the cost of edges composing it. We will demonstrate hereafter, that some optimal and also some feasible solutions are not trees nor sets of trees nor sets of QoS paths; they are not always sub-graphs and the communication cost should carefully be defined.

Deep analyses have been made for QoS constrained multicasting. Remember, multicast needs partial spanning (only the source and the destinations should be covered, the eventual intermediate relay node set is not fixed). The generalization for broadcasting is easy: the set of destinations corresponds to the set of nodes except the source. It was demonstrated, that a feasible partial spanning structure for multi-constrained QoS multicasting may be a sub-graph containing feasible paths from the source to the destinations (Kuipers and Mieghem 2002). Unfortunately, the sub-graph is not sufficient to define the routes. It is true, a multi-constrained multicast route should provide a feasible path toward each destination but this route may not correspond to a sub-graph as it was demonstrated in (Molnár et al. 2012). The appropriate solution of the multi-constrained QoS routing problem is a graph-related structure, which can precisely describe multicast/broadcast, and in our case, incast routes (*cf.* in sub Sect. 2.4 for incast communications). The solutions always correspond to *hierarchies* (Molnár 2011). In some cases, the hierarchies can correspond to simpler routes: to paths and trees, which are particular cases of hierarchies. Similarly to multicasting, the spanning hierarchy concept enables to define the optimal solution. An illustration can be found in Fig. 2(d). Notice that the multi-constrained (partial) minimum spanning hierarchy problem is also NP-hard. Before going over the definition of hierarchy based QoS routes, let us define incast communications.

2.4 Multi-constrained Incast Route

Many to one communication without QoS constraints (or with a single constraint) can use a tree for data forwarding to the root node. In our case the root of the tree is the sink in the WSN (*e.g.,* a Border Router in RPL). The QoS constrained incast tree-based on one metric (*e.g.,* on the latency) can be considered

as an "inversed multicast/broadcast tree" as Fig. 1 suggests. The optimal incast route definition can be similar to the formulation in Definition 1, but there is an important difference.

The QoS constrained incast route, even if there is only one constraint, can be different from the inversed broadcast tree. The difference is due to the communication cost and the followed objectives.

- For cost optimized multicast/broadcast trees, the cost reflects the usage of the network resources: *e.g.,* the sum of the edge costs in the tree. It is because an edge of the tree is used to transmit a message only once from the source to the destinations. This message is distributed, duplicated by the branching nodes in the tree.
- In incast routes (following the incast trees) the different messages traversing an edge near the sink and coming from different sensors use several times the edge: each message involves the cost represented by the edge (here we suppose that there is no aggregation of the messages in the network). The cost of the communication is the sum of the edges present in the set of paths.
- Several sets of paths for incast communication can implicate the same cost, and a different, routing related objective (*e.g.,* the simplification of the routing tables) can also be interesting.

Here too, the presence of several QoS constraints modifies the problem and its solution. We propose the following formulation of the problem. In this formulation we talk about "routing aware" computation. We consider that an incast route is better for routing than another, if it contains less parent information (*e.g.,* entries) in the set of nodes.

Definition 2 (The minimum cost, routing aware multi-constrained incast problem)

In the evaluated graph $G = V, E)$ the sink is the node $d \in V$ and the sources are the nodes in $S \subseteq V \setminus \{d\}$. The end-to-end QoS constraints are given by $\overrightarrow{L}$. The minimum cost routing aware multi-constrained incast problem is to find a route offering a feasible path from the sources to the unique destination minimizing the cost and also facilitating the routing:

$$\min\left(u \cdot \sum_{p_{s,d} \in P_{QoS}} C(p_{s,d}) + \sum_{v \in V \setminus \{d\}} NP(v)\right)$$

where P_{QoS} is the set of QoS (feasible) paths in the solution, $C(p_{s,d})$ is the cost of the path $p_{s,d}$, and $NP(v)$ is the number of parents in the node v. The weight u is big enough to guarantee the priority of the cost component.

To find good solutions, it is indispensable to give the exact definition of the routes corresponding to the described optimization. This definition follows.

2.5 Hierarchies to Describe QoS Routes

At first, we demonstrate that trees can not always meet the end-to-end constraints for incast communications but in some cases, when there is no tree solution, hierarchies can.

Let a small network be considered as it is in Fig. 2(a). Two QoS related parameters are associated to the edges as it is indicated. The data gathering needs a QoS, the tolerated values are given by the vector $\overrightarrow{L} = [9, 9]^T$. Each node should send messages to the BR respecting the constraints. Figure 2(b) indicates the QoS paths from the nodes to the BR. There is only one feasible path from each node. In order to simplify the routing and share some edges, a reduced schema can be constructed as it is shown in Fig. 2(c). This schema is not a tree nor a set of paths. This structure is a destination oriented directed acyclic graph (DODAG). Figure 2(d) illustrates how to obtain this route with the help of a hierarchy.

In a graph $G = (V, E)$ a hierarchy is defined as follows.

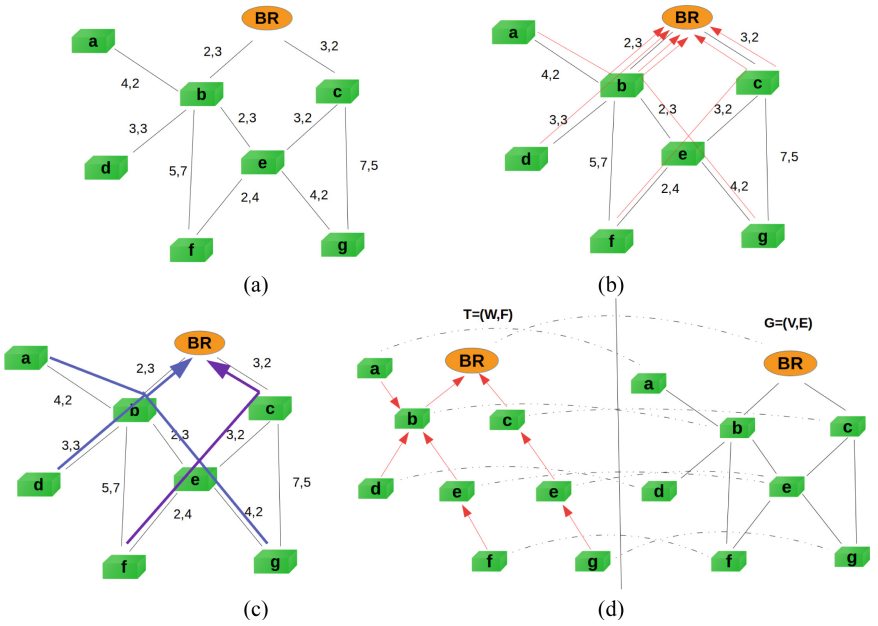


Fig. 2. (a) A WSN (b) The QoS paths to the BR (c) The route after the elimination of redundancies (d) The corresponding hierarchy

Definition 3 (Hierarchy). Let $T = (W, F)$ be a tree (a connected graph without cycle). Let $x : W \rightarrow V$ be a homomorphism which associates a node $v \in V$ to each node $w \in W$.[1] The association (T, x, G) defines a hierarchy in G.

A hierarchy is not a sub-graph, it is a graph-related structure preserving some properties of trees but nodes and edges in the graph G can be visited several times by a hierarchy. Trees are special hierarchies obtained by injective homomorphism. Thus, *a tree is a hierarchy.* Some properties in trees are true in hierarchies but all are not true. Conversely, all properties of hierarchies are true in trees. If the tree T is directed in (T, x, G), the defined hierarchy is also directed. For incast routing problems, hierarchies directed to the sink are needed.

In our first example in Fig. 2(d), Node e is visited twice by the hierarchy. Since the different occurrences of the elements can play different roles, the distinction and the identification of the occurrences is substantial. For Node e in the example: if a message is coming from Node f, it should be forwarded to c and a message coming from g should be forwarded to b to satisfy the QoS constraints.

Generally, in routing problems, the graph G is the topology of the network and the tree T represents the routing information (the data forwarding). Our routing problem can be precisely formulated with the help of hierarchies.

The minimum cost, routing aware multi-constrained incast problem consists in finding the multi-constrained minimum directed spanning hierarchy containing at most one path $p(s_j, d)$ directed from each source $s_j \in S$ to the destination d respecting the constraints: $\overrightarrow{w}(p(s_j, d)) \overset{d}{\leq} \overrightarrow{L}$.

3 QoS Routing in WSNs

The particularity of WSNs is that they are multi-hop, wireless networks without infrastructure to collect and send data to a sink or BR node using the network elements (sensors) as relays. The resources, *i.e.* the processing capacities, memories and battery powers are limited, reliability is low and the topology could change rapidly.

Route computation and selection impact strongly on the offered QoS. In the literature, several objectives are applied for QoS aware routing in WSNs. Some propositions go beyond the end-to-end quality measurement of routes. Important objectives as the energy utilization, the networks lifetime, the reliability, the stability of the paths are examined but in the recent chapter we focus our analysis on the usual set of end-to-end service oriented QoS parameters such as delay, jitter, packet loss, bandwidth, etc.

[1] A homomorphism is an association preserving the adjacencies of nodes; $w_1 \in W$ and $w_2 \in W$ can be adjacent (in T) iff the corresponding nodes $v_1 \in V$ and $v_2 \in V$ are also adjacent (in G).

Routing protocols are presented and analyzed in several surveys classifying the most known propositions (*cf.* an example in (Goyal and Tripathy 2012)). An important aspect of the protocols is the timing of the route computation: proactive and reactive routing protocols are well known for WSNs. A concurrent reactive, on demand propositions and its analysis can be found in (Clausen et al. 2017). The protocol promises extensions to maintain collection trees and fast rerouting. The inconvenient of reactive protocol is the latency at least at the beginning of the communication. A large analysis of the WSN based applications and the proactive protocols can be found in (Mohamed et al. 2018). Hybrid solutions try to use the advantages of both strategies. An example is the zone-based ZRP which partitions the domain into a set of zones. Intra-zone routing uses a proactive protocol, and inter-zone routing is based on a reactive protocol diminishing the proactive image of the entire network. The QoS aspect of proactive, reactive and hybrid protocols for Mobile Ad Hoc Networks (MANETs) is compared in (Bhatia and Verma 2015). Generally, reactive protocols outperform proactive ones in terms of throughput and packet delivery ratio whereas proactive protocols are better regarding end-to-end delay and traffic load.

Routing protocols in WSNs can also be classified as follows (there are only some aspects taken into consideration in this classification, it is not exhaustive). *Destination-oriented* routing is the usual solution in which the routing decision is based on a unique "address" and routing tables are often used to decide the next hop toward the destination. Routes can be constructed by a proactive procedure or on demand. *Cost (or distance) - based* solutions associate with each node a value proportional to the distance from the destination and the decision of the next hop tries to diminish this cost. For instance, the cost can be a rank as we will see in RPL (*cf.* Sect. 4). *Geographic location* (*e.g.,* GPS) information can also be used to decide the next hop neighbor for data forwarding to the destination.

Often, cross-layer designs are proposed to achieve efficient solutions taking into account mechanisms in the neighbor layers (mainly in the MAC layer). We limit our study to the network layer.

Due to the very limited resources, the QoS aware routing in WSNs is a challenging task. The different applications require the satisfaction of different constraints. The energy minimization and the networks lifetime maximization are often important objectives. Some routing protocols for WSNs explicitly consider QoS requirements. Typically, the minimization of the energy usage is coupled with the respect of an end-to-end delay requirement. Sequential Assignment Routing (SAR) targets the QoS in the routing decisions (Sohrabi et al. 2000). It is a destination and multi-path based protocol using trees rooted at the sink node. The data transmission is decided on the base of energy usage, an eventual QoS metric, and priority level of the packets. One QoS metric may be defined, for example, the delay, and SAR tries to minimize a weighted metric also calculated from the link cost and priority level of the packets. Moreover, this multi-path based protocol offers fault-tolerance and easy recovery, but it needs an important overhead to maintain routing tables. SPEED (He et al. 2003) is a geographic routing protocol in WSNs providing soft end-to-end guarantees

regarding the delay. Each node maintains information about its neighbors and uses geographic forwarding to find the paths. Soft real-time communication is achieved by maintaining a desired delivery speed. The end-to-end delay for the packets is estimated by dividing the distance to the sink by the speed of the forwarding. Real Time Power Aware Routing Protocol (RPAR) is an extension of SPEED to improve real time routing in WSNs. The principal element of this protocol is its capacity to adapt the transmission power and the routing decisions to the application delay requirements. For strong and short required delays it allocates more energy and capacity to respect the desired delay constraint (Chipara et al. 2006). In (Akkaya and Younis 2003), an energy-aware QoS routing protocol has been proposed. The protocol finds a least-cost, delay-constrained path for real-time data. The link cost is a function based on the energy level of nodes, transmission energy, error rate and related parameters. The data forwarding supports two classes: best effort and real-time traffic at the same time, and a class-based queuing model is employed by adjusting the service rate for both classes.

Wireless Multimedia Sensor Networks pose additional challenges because the transmission of images and videos needs strong QoS. In (Alanazi and Elleithy 2015) the authors state that the reliability and guarantee of end-to-end delay are critical while conserving energy. The propositions follow these objectives. The reader can find a large set of real-time QoS routing protocols classified into two categories, which are probabilistic and deterministic, including soft real time and hard real time QoS.

Only a few, really multi-constrained QoS routing algorithms for WSNs are known. In a few cases, algorithms to compute multi-constrained paths in wired network are proposed for WSNs. A little more often, one can find some works based on *multi-objective* QoS routing, when there are several objectives on the QoS metrics instead of multiple constraints. In (Alwan and Agarwal 2013) a Multi-Objective QoS Routing protocol (MQoSR) is proposed. Multiple metrics are taken into account: energy, delay, reliability and hop count. The packets are forwarded to the next hop which minimizes a weighted sum representing the total cost. A multi-objective evolutionary algorithm uses ant colonies to solve the energy aware routing problem taking into account some aspects of QoS in (Su et al. 2013). Two performance metrics trying the maximization of the remaining lifetime of the network and also the minimization of the transmission delay are considered. In (Kulkarni et al. 2018) a heuristic routing algorithm called QoS assured Multi-objective Hybrid Routing Algorithm (Q-MOHRA) is proposed for heterogeneous WSN. This protocol takes into account link metrics as the needed energy, hop count, link quality indicator and path metrics as the jitter and uses a hierarchical clustering and a weighted sum of the used metrics to represent the goal.

In our opinion, the multi-objective formulation can not replace the multi-constrained one. The service related, end-to-end requirements are constraints and should (or could) not always be optimized. Moreover, there is no equivalence between the solutions: a solution of a multi-objective optimization obtained by

a composite technique could not always meet all the constraints. Inversely, solutions respecting the constraints could be not optimal. The usual multi-objective optimization techniques propose trade offs: one non-dominated point on the Pareto front or a not optimal point behind this front is selected (and it depends on the applied technique: lexicographic, or weighted optimization, etc.)

In the following we focus on propositions handling multi-constrained cases. Moreover, since RPL is a standard for low-power and lossy networks (LLNs), we are interested with QoS routing using RPL. After a brief overview of the protocol, Sect. 5 presents some ideas for QoS aware RPL.

4 RPL as a Standard

One of the standardized routing protocols for LLNs is the proactive, cost based RPL (Routing Protocol for Low-Power and Lossy Networks) proposed in RFC 6550 and it is designed essentially for incast (many to one) communication (Alexander et al. 2012). For data gathering, a destination oriented directed acyclic graph (DODAG) is used which is mainly a tree directed from the sensors to the sink. Nodes are organized into a "layered" hierarchical structure starting from a single root (the sink), finding direct children and children of children, etc. A node forwards the data to a parent (that has lower cost, *i.e.* lower rank) toward the sink.

A WSN using RPL can contain several RPL Instances for different applications, measurements. An RPL Instance may contain several DODAGs. A node can only belong to a single DODAG in an RPL Instance, but it can participate to multiple RPL Instances. In the protocol, Global RPL Instances are coordinated (containing one or more DODAG), but a Local RPL Instance corresponds always to a single DODAG and can be used for constructing DODAGs in support of a future on-demand routing solution (Alexander et al. 2012).

The construction of each tree-like DODAG is based on the attribution of "ranks" [2] descending from the root applying an Objective Function (OF) which can eventually be defined on QoS metrics. The OF gives the rules for the rank computation based on the routing metrics and it defines how to select a preferred parent for each node. Only a few OFs are proposed and the existing functions are usually based on one metric (*cf.* examples in (Farooq et al. 2017)).

In RPL, the following ICMPv6 control messages are defined to construct and maintain the topology.

- *DODAG Information Object (DIO).* In order to determine the rank of nodes and select parents for data forwarding, the sink node starts the construction of its DODAG by broadcasting a DIO message to its neighbors. The rank of the sink is zero, and there is a version number for each DODAG. DIO includes information on the rank and also on the OF. This kind of messages are sent to

[2] the rank defines the position of the node in the DODAG with respect to the neighbors and the DODAG root ("hop" distance from the root).

the neighboring nodes descending from the sink in the topology. Based on the received messages and on the OF, nodes make the decision on the rank (which is incremented from the sink). A node selects a set of candidate parents (with ranks less to its rank) and a preferred parent used by default for data forwarding to the sink. Notice that DIOs may contain optional objects. For instance, an optional DAG Metric Container (DAGMC) contains eventual metrics and constraints. Metrics may be aggregated or recorded. An aggregated metric is cumulated on the path but for recorded metrics, each node adds a separated local value to the container. As the RFC indicates, "RPL supports constraint-based routing where constraints may be applied to both links and nodes. If a link or a node does not satisfy a required constraint, it is "pruned" from the candidate neighbor set, thus leading to a constrained shortest path." The computed DODAG can be used for incast communications.

- *Destination Advertisement Object (DAO).* This message prepares the routes for down traffic and is used to propagate destination information upwards along the DODAG.
- *DODAG Information Solicitation (DIS).* When a new node tries to join an existing network, it sends a DIS message to its neighbors and requests graph information from its neighbors via DIO messages. After receiving the responses, the new node then selects its parent nodes.

Each node can have a set of candidate parents but only one preferred parent. If there is a failure, a local repair can change the preferred parent if there are other candidates. RPL includes also a global repair mechanism, which rebuilds the DODAG by incrementing its version.

For data gathering, a node sends data to the DODAG root passing by the configured consecutive preferred parents. Upward communications and node to node communications are also possible but they are out of scope of our chapter. For more details, we refer (Gaddour and Koubâa 2012) and also (Kamgueu et al. 2018). The paper (Ghaleb et al. 2019) proposes a survey of some enhancements and limits of the protocol.

Arbitrary cost type metrics can be used in RPL for DODAG construction and the usage of constraints is possible but the effect of the constrained routing is limited. A constraint prevent the selection of paths passing by a node or link that do not meet the local requirement.

Basically, RPL uses special DODAGs, in which each node has one preferred parent. The data gathering follows a tree directed to the BR. For multi-constrained QoS routing more permissive solutions are needed.

5 QoS Aware Routing Using RPL

This section deals with QoS routing in WSNs using RPL. Our goal is to present solid proposals for cases when several constraints represent the QoS requirement. After reviewing previous papers illustrating the most significant propositions, we resume the theoretical bases of multi-constrained incast routing and some ideas how to compute and use the corresponding QoS routes in RPL.

5.1 Propositions for QoS Aware DODAGs

Following the documentation of RPL, some simple OFs have been proposed and new OFs can be defined, such that the solutions should insure tree-based DODAGs.

Combinations of several routing metrics (into one composed metric) for QoS using RPL have been analyzed in (Karkazis et al. 2013). After a nice path algebra based presentation of routing problems, this study covers the usage of additive and lexicographic composition of metrics to compute QoS routes.

Remember, additive composite routing metrics on a path (link) p can be defined as a weighted sum of k primary metrics $w_1, w_2, ..., w_k$, like

$$w(p) = a_1 \cdot w_1(p) + a_2 \cdot w_2(p) + ... + a_k \cdot w_k(p)$$

where $a_1, a_2, ...a_k$ are positive constants.

For lexicographical composition, we simply indicate an alternative definition of the authors: "when multiple routing metrics are combined into a composite lexicographic routing metric, this dictates that the primary routing metrics are prioritized and when a path offers a better weight with respect to the first metric then it will be preferred regardless of the path weights of the rest metrics." This prioritization technique and the additive composition are often used for multi-objective optimizations. Trivially, the additive composition with adequate weights can be a possible implementation for the lexicographical composition.

Primary metrics like latency, remaining battery power, expected transmission count (ETX), ... are analyzed and used to make composite metrics to satisfy different requirements of the applications. The conditions for convergence to optimality and acyclic graph computation are also analyzed and proposed to use in RPL.

Often, the composite objectives are efficient to solve multi-objective optimization, but as we indicated in Sect. 3, these transformations can not always offer a solution for multi-constrained route computations. In the next section, we will show that a multi-constrained QoS incast route should permit the data forwarding to different parents. This possibility can not be insured by composite metrics.

Meta-heuristics may also be candidates to design QoS aware routing protocols. A protocol applying an ant colony optimization technique to compute routes in RPL is presented in (Mohamed and Mohamed 2015). The proposed ant colony cooperation aims at finding a path at each node to the destination selecting a parent with a high probability of transition. For this, the probability of transition is expressed. The metrics used for the computation are the additive end-to-end delay and the bottleneck residual energy. Using the dynamic discovery of cooperating ants, the protocol determines energy efficient routes. The authors expect a better QoS using this solution. The respect of strict QoS constraints is not considered.

An original idea is to use a fuzzy inference system to choose the next hop of data forwarding. In (Gaddour et al. 2014) a novel objective function called OF-FL (OF based on fuzzy logic) combines a set of metrics for the routing

decision of real-time, reliable communications with energy efficiency. Four metrics are considered: delay, ETX, hop count and remaining power of nodes as fuzzy variables. Another fuzzy inference system is applied in (Kamgueu et al. 2015) combining several metrics to decide the next hop (the preferred parent) using RPL. The proposed fuzzy inference system merges for instance expected transmission count, delay and remaining power of nodes into one unique value. Other criteria can also be used combining several metrics into one. The authors state that constraints and requirements are sometimes conflicting issues under a WSN context and it is sometimes difficult to decide the characteristic values of the fuzzy variables. Trade-offs must be found to balance between the QoS considerations. Fuzzy inference systems are simple, elegant tools for optimization even if several variables are considered and values are imprecise. They permit the combination of conflicting objectives and constraints and the complexity of the algorithms is low corresponding to the limitations of WSNs. However, the propositions can not cover cases, when different parents are needed in internal nodes for data transmissions coming from different sources (*cf.* the Subsect. 5.2). Moreover, taking into account strict constraints with fuzzy logic based solution is not trivial.

Some works propose multi-path routing using RPL not only to improve QoS but also for a better fault-tolerance, enhancing reliability, and eventually decrease congestions. For instance (Iova et al. 2015) proposes a multi-path routing technique to allow RPL to forward data to multiple (preferred) parents. That is, multi-path routing in RPL involves multi-parent data forwarding. The main objective of this multi-parent routing is to improve the network lifetime by balancing the traffic load and avoiding the unbalanced depletion of the energy of nodes. For this, nodes should choose to send their traffic on the least energy limited path using an adequate path metric. Based on a given DODAG created in RPL, the data forwarding should balance the traffic toward all the existing parents. Another important statement by the authors is that frequent changes in the preferred parent may induce instability and higher energy consumption.

A combination of composite objectives and the fuzzy logic can be found in (Araújo et al. 2018). In this paper, four OFs are proposed for RPL which combine different metrics: ETX, number of hops and energy usage. The originality of the proposition is that OFs are dynamically selected based on contextual information. The authors say that fixed composition of metrics does not always correspond to the needs of an application. Information on the devices and on their environment can be used as contextual information for the route selection. The devices can select the preferred parent node (the applied OF) based on the contextual information. The paper proposes a route classifier based on fuzzy inference system to classify the possible routes and select the best one in each context. Notice, this solution can associate different next hop for data transmission, which is essential to satisfy multiple constraints being in contradiction. This proposition can be considered as a particular multi-path routing.

The most important part of the proposed solutions tries to find effective DODAGs by using composite metrics, meta heuristics and/or fuzzy systems for the data forwarding decisions. In these cases, the data forwarding uses a tree like graph with one preferred parent for each node. Trees can not always satisfy the multi-constrained QoS routing requirements. In some solutions, the set of parents can be used (multi-parent protocols) and a contextual decision making procedure has also been proposed. These propositions can help the adaptation of RPL to the more difficult multi-constrained routing cases, where a simple tree is not sufficient to meet the QoS requirement.

5.2 Propositions for Multi-constrained Incast Routing Using RPL

Section 2.4 defines the multi-constrained incast routing. As it is shown, finding a feasible solution is NP-complete and the computation of an optimal one is NP-hard. Eventual solutions are hierarchies directed to the BR. Remember, a hierarchy is defined by a triplet (T, h, G). There are some trivial properties of the hierarchies solving the multi-constrained incast routing.

- Each directed path in the hierarchies is without loops, they form a DODAG. Possible crossings of directed paths in some nodes do not implicate loops.
- A node can have several parents in the graph G, but each node occurrence has only one parent in the tree T. Consequently, the decomposition of the hierarchy is always possible into a set of RPL compatible DODAGs[3].

The adaptation of RPL Instances to meet the QoS constraints is required: a particular multi-parent solution is needed. Moreover, the computation of paths under several constraints is expensive and only non exact algorithms can be applied in WSNs.

5.2.1 Path Computation

To compute multi-constrained QoS paths (which is NP-complete), and to control the satisfaction of the QoS requirements, a non-linear scalar length function has been proposed in (Kuipers and Mieghem 2002). Let $\overrightarrow{L}$ be the m-dimensional vector of the QoS requirement and $\overrightarrow{w}(p(s,d))$ the weight vector of the path $p(s,d)$. Its non-linear length is:

$$l(p(s,d)) = \max_{i=1,\ldots,m} \frac{w_i(p(s,d))}{L_i}$$

Trivially, if all the constraints are satisfied, then $l(p(s,d)) \leq 1$ and the path is feasible. To find a feasible solution, the shortest path from s to d using the non-linear length can be computed. If this length is less than 1, the path is feasible (if the non-linear length of the shortest path is greater then 1, there

[3] We consider that a DODAG is RPL compatible, if each node has only one preferred parent.

is no feasible solution). To compute the shortest path, we follow the algorithm SAMCRA proposed in (Van Mieghem et al. 2001). It is a Dijkstra-like algorithm, but the greedy selection of shortest paths by the classical Dijkstra's algorithm can not be applied. To compare two paths arriving to a node, only the Pareto dominance can be used and all non-dominated paths should be kept to continue the computation. The non-linear length based shortest path from s to d can be selected, when all non-dominated paths between the two nodes have been computed.

5.2.2 Construction of Multi-constrained DODAGs

Unfortunately, the computation and the storage of all non-dominated paths in the nodes descending from the BR are not possible because of the limited capacities. In (Khallef et al. 2017b) a non-linear length based objective function has been presented to build a DODAG corresponding to a set of constraints. In the proposed construction, all of the non-dominated paths are not stored in the nodes. The DOI messages contain the cumulated weight vectors descending from the BR (for this, an optional DAG Metric Container in DIOs can be used). When a node received these messages from its potential parents, it computes the non-linear length of the received paths to the sink. The proposition supposes that the weights of the links are symmetric. Let $\overrightarrow{w}(p(u,d))$ be the weight vector from the node u to the sink d. Let us suppose that this vector is sent to node v via the link e relying u to v having $\overrightarrow{w}(e)$ as weight vector. Trivially, the weight vector $\overrightarrow{w}(p^u(v,d))$ associated with the path from the v to d passing by u is:

$$\overrightarrow{w}(p^u(v,d)) = \overrightarrow{w}(p(u,d)) + \overrightarrow{w}(e)$$

Based on the received values, v can select all potential parent nodes corresponding to feasible paths (with non-linear length less then 1) and one preferred parent which corresponds to the minimal non-linear length. Only the weight vector passing by the preferred parent is then transmitted to the successors in the construction. Consequently, the algorithm can not enumerate all feasible paths and some solutions may be lost. However, a usual tree-based incast route is built by using the basic mechanism of RPL.

Following the example of the network shown in Fig. 2(a), the loss of feasible paths using the greedy algorithm is illustrated in Fig. 3(a). In this case, each node forwards by DIOs only one path (the path with minimal non-linear length) to the neighboring nodes. Node e receives these single routes from b and c. Since the two routes have the same non-linear length ($NL = 6/9$), it select one of them. Let us suppose that the route selected by e to the sink is the route (e, b, BR). This route can be a valid suffix for g in the path (g, e, b, BR). This path corresponds to a value $NL = 8/9$. The same suffix is not suitable for Node f, since the path (f, e, b, BR) has a non-linear length $NL = 10/9$.

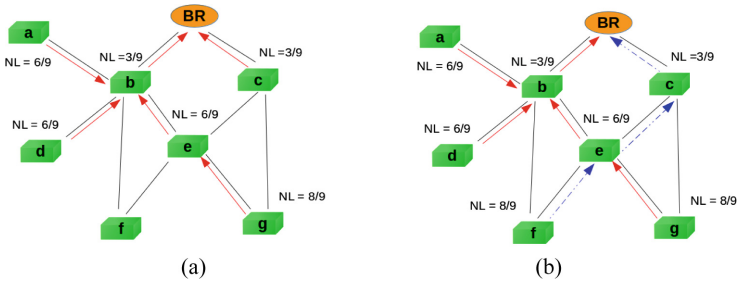


Fig. 3. (a) The result of the greedy NL based algorithm is an RPL DODAG (b) The decomposition of the exact solution into two mono parental RPL DODAGs. Notice that this solution can also be computed using the 2-limited heuristic

Since the computation of the multi-constrained incast hierarchy is NP-hard, trade-offs are needed between the quality of the routes and the computation time. In (Khallef et al. 2017a) the computation of the exact incast hierarchy is presented. To avoid the loss of theoretically reachable nodes, the exact solution does not limit the number of computed and stored feasible and non-dominated paths. To select preferred parents, the algorithm preserves all non reducible paths to the sink. In this way, a sensor can have a feasible path to the BR, if such a path exists. Since the exact algorithm can be very expensive, its interest is in the evaluation of inexact solutions. To find trade-offs between quality and computation time, parameterized polynomial time algorithms are proposed. The basic idea of the "k-limited algorithms" has been proposed for QoS path computation in the TAMCRA algorithm (Neve and Mieghem 2000). It is a question of limiting the number of non-dominated feasible paths per nodes to k paths, with a fixed positive integer k. Similarly to the exact computation, the obtained route does not always correspond to an RPL compatible DODAG but to a destination oriented directed hierarchy. In the k-limited version of the computation, a node receiving the non-dominated and feasible path propositions from the parents and computing its feasible paths can forward at most k paths to its neighbors. (Notice that the exact solution corresponds to the case when k is not limited.) As it is indicated in the paper, critical neighbors can find more probably a path corresponding to their needs, but it is always possible that there are unreached nodes because all the possible paths are not enumerated.

5.2.3 Evaluation of the Propositions

The proposed algorithms were evaluated in random network topologies. The random graphs were generated by the Waxman model. The presented results in (Khallef et al. 2017a) and presented also here are the mean values overs 100 instances. The 200 edges of the random graphs having 50 nodes were weighted by $m = 2$ and in some other cases by $m = 4$ integer QoS values. These values were also randomly generated from $\{1, \ldots, 10\}$. The most interesting results are

expressed related to a derived metric: to the constraint looseness (CL). The CL is the average value of $L_i/maxv_i, i = 1, ..., m$, where $maxv_i$ is the maximum possible value of metric of index i. A small value of CL indicates strict constraints and the maximal value of CL corresponds to cases when the constraint are not significant. Figure 4(a) illustrates how many nodes can not be covered respecting different QoS requirement. When the constraints are strict, several nodes (probably the nodes far from the sink) are missing from the incast spanning hierarchies. Contrarily, with loose constraints the QoS routes can be "easily" built. Another lesson learned from this experiment is that the proportion of missing nodes decreases as the k value of the limited heuristics increases. The average quality of the routes can be observed in Fig. 4(b). Remember that the non-linear length characterizes the most critical QoS value of the paths (it is less than 1 for feasible paths). The algorithms computing more alternative paths give better results. Moreover, in the case of strict QoS requirements, the non-linear length is greater than in the cases of loose constraints. Notice that the time of the computation is of the order of some minutes for the exact solutions and of a few milliseconds for the heuristics.

5.2.4 Adaptation of RPL

The presented solutions does not address an important element: how to use RPL to implement the computed route knowing that the latter may be a hierarchy? Remember, in the directed route, some graph nodes can have several parents as it is indicated in Fig. 3(b).

Here, the reader can find propositions for the creation and usage of the corresponding multi-parent RPL Instances.

One of the possible multi-parent data forwarding is the application of the contextual information (*cf.* the idea in (Araújo et al. 2018)). In our case, the determinant context for the data forwarding decision is the origin of the data. This is a simple deterministic decision that does not need a fuzzy logic based classifier. In the example of Fig. 3(b), the only one node needing the contextual routing is Node e. The classification is simple: if a message arrives from Node f, then it should be forwarded to the parent c, otherwise the message should be transmitted to b.

A second possibility is the creation of several RPL Instances and DODAGs inside of the instances. The objective is the implementation of the directed hierarchy at the end of the route computation. This hierarchy can be decomposed into a set of RPL compatible DODAGs (remember, the difference is that in the loop less directed hierarchy, a node can belong to several paths to the root, but can not in an RPL compatible DODAG). To create the routing scheme of the example of Fig. 3(b), two RPL compatible mono parental DODAGs should be configured: a first indicated by red arrows and another indicated by blue arrows. In the following, a centralized route computation is briefly described.

1. Construct a Local RPL Instance beginning at the Route Computation Entity as root. To simplify, this entity may be the BR.

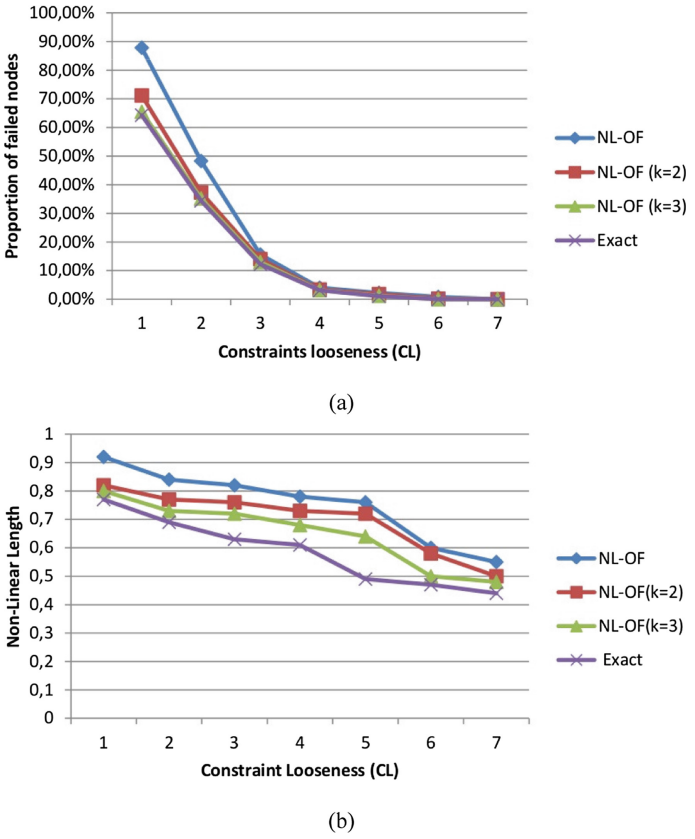


Fig. 4. (a) The ratio of missing (uncovered nodes) for different values of CL in the case of $m = 4$ uncorrelated metrics (b) The non-linear length of the successfully computed paths. Results presented in (Khallef 2017) and (Khallef et al. 2017a)

2. Propagate DIO messages and compute a k-limited set of QoS paths in the nodes, starting from the root (BR) of the future QoS constrained application. The selection of the preferred parents is temporary in this temporary DODAG.
3. Using the Local RPL Instance, send the set of k feasible paths from each node to the Route Computation Entity.
4. Compute the global directed hierarchy as follows:
   a. The paths from leaves having only one QoS path to the BR should be selected and maintained in each traversed node
   b. Leaves having a QoS path containing a shared common suffix with the existing hierarchy can be added to the hierarchy[4]. In the case of several candidate paths, select the path with minimal non-linear length. (Trivially, internal nodes of the added paths are added to the hierarchy.)

[4] Two directed paths share a suffix if the last sub-paths are the same in the two paths.

   c. If there is no more leaf from which a path shares a common suffix with the hierarchy, then select a remained leaf and add to the hierarchy using its path with minimal non-linear length. (In this step, a new DODAG is initialized and multiple non compatible parents can be produced for some nodes.)
   d. Re-iteration of the previous steps until all nodes are covered.
5. On the base of the computed hierarchy, create the needed RPL compatible DODAGs.
6. Send the RPL compatible DODAGs to the nodes to configure them.

Actually, using RPL mechanisms, RPL routers can not be configured explicitly. It can be candidate for future improvement of the protocol.

As the authors in (Iova et al. 2016) say, RPL needs a re-targeting. "For example, RPL could become a general standard framework, providing the glue for a suite of inter-related standards, each focused on specific communication technologies and/or application profiles." The QoS routing is a large domain to investigate in the protocols.

6 Recent and Future Issues and Challenges

On one hand, in the domains of WSNs and IoT networks, with the development of applications increasingly demanding QoS, QoS-aware routing still requires considerable effort. For related basic research activities, one can mention some challenging needs.

As it is indicated in this chapter, the theoretical optimum for mono-objective multi-constrained incast routing corresponds to a directed hierarchy. The case of multi-objective routing requires further analysis. Moreover, finding efficient heuristics to build QoS-aware, hierarchy-based routes is an open domain. Notice that approximation guarantees for these routes are not known.

Eventual data aggregations in intermediate nodes can also modify the routing. The selection of efficient and appropriate aggregation techniques and the selection of the nodes that can execute them following appropriate routes can improve the performance of the data gathering. A large literature analysis of data aggregation in WSNs, recent research issues and future research directions can be found in (Randhawa and Jain 2017).

Network connectivity can change quickly and unpredictably. Note as cause the mobility and possible duty cycles of nodes. The use of opportunistic networks is a recent paradigm to deal with the problem. In opportunistic networks, the nodes transmit the messages when their connectivity is restored. Routing in this type of networks is challenging. A new routing strategy based on the node's activities in opportunistic networks is proposed in (Kumar et al. 2019). Compliance with QoS constraints in this type of network is a very difficult subject.

On the other hand, the evolution of applied network management techniques and of the sensor nodes and things, the use of increasingly intelligent solutions becomes feasible.

The monitoring of the network's state permits the detection of failures and disconnections, and the collect of QoS related parameters is essential for the routing decisions. The monitoring of the network's connectivity using RPL for applications serving critical missions is proposed in (Mostafa et al. 2018). The collect of QoS related values is a possible prolongation.

Software Defined Networking proposes an intelligent network management decoupling the control plane from the data plane, and thus using a central controller. A strong Border Router can be this controller. A comprehensive review of the Software Defined Networking in WSNs and its design requirements and challenges are analyzed in (Kobo et al. 2017).

One can also notice that with the evolution of systems used in WSNs, the application of TE based solutions (priority based routing, multi-path routing, ... becomes affordable.

7 Conclusion

QoS routing is an important and challenging topics in WSNs and IoT. Often, the QoS requirements correspond to a set of end-to-end constraints to respect. The standardized routing solution in LLNs is RPL. This protocol permits the definition of different Objective Functions and also constraints to build DODAGs mainly for incast (many to one) data gathering. The constraints relate edges and nodes but they are not end-to-end path related. Several QoS aware routing protocols are known and there are propositions for RPL. This chapter presents the problems of the propositions and also the real nature of the multi-constrained incast route corresponding to a graph related solution: to a hierarchy. Some elements of the computation of hierarchy based DODAGs are also presented. However there are open challenges to successfully deploy RPL in multi-constrained QoS requirements. Future investments are needed to find simple multi-parent solutions using RPL, to handle uncertainties by multi-path and opportunistic routing and to couple the routing to traffic engineering.

References

Abbasi, M.R., Guleria, A., Devi, M.S.: Traffic engineering in software defined networks: a survey. J. Telecommun. Inf. Technol. **4**, 3–14 (2016)

Akkaya, K., Younis, M.: An energy-aware QoS routing protocol for wireless sensor networks. In: 2003 Proceedings of 23rd International Conference on Distributed Computing Systems Workshops, pp. 710–715. https://doi.org/10.1109/ICDCSW.2003.1203636

Alanazi, A., Elleithy, K.: Real-time QoS routing protocols in wireless multimedia sensor networks: study and analysis. Sensor **15**(9), 22209–22233 (2015). https://doi.org/10.3390/s150922209

Alexander, R., Brandt, A., Vasseur, J., Hui, J., Pister, K., Thubert, P., Levis, P., Struik, R., Kelsey, R., Winter, T.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550 (2012). https://doi.org/10.17487/RFC6550. https://rfc-editor.org/rfc/rfc6550.txt

Alwan, H., Agarwal, A.: Multi-objective QoS routing for wireless sensor networks. In: 2013 International Conference on Computing, Networking and Communications (ICNC), pp. 1074–1079 (2013). https://doi.org/10.1109/ICCNC.2013.6504241

Araújo, H.D.S., Filho, R.H., Rodrigues, J.J.P.C., Rabelo, R.D.A.L., Sousa, N.D.C., Filho, J.C.C.L.S., Sobral, J.V.V.: A proposal for IoT dynamic routes selection based on contextual information. Sensors **18**(2) (2018). https://doi.org/10.3390/s18020353

Bhatia, T., Verma, A.: QoS comparison of MANET routing protocols. Int. J. Comput. Netw. Inf. Secur. **7**, 64–73 (2015). https://doi.org/10.5815/ijcnis.2015.09.08

Chen, G., Burkard, R.E.: Constrained Steiner trees in Halin graphs. RAIRO-Oper. Res. **37**(3), 179–194 (2003). https://doi.org/10.1051/ro:2003020

Chipara, O., He, Z., Xing, G., Chen, Q., Wang, X., Lu, C., Stankovic, J., Abdelzaher, T.: Real-time power-aware routing in sensor networks. In: 2006 14th IEEE International Workshop on Quality of Service, pp. 83–92 (2006). https://doi.org/10.1109/IWQOS.2006.250454

Clausen, T., Yi, J., Herberg, U.: Lightweight on-demand ad hoc distance-vector routing-next generation (LOADng): protocol, extension, and applicability. Comput. Netw. **126**, 125–140 (2017). https://doi.org/10.1016/j.comnet.2017.06.025

Crawley, E., Nair, R., Rajagopalan, B., Sandick, H.: A framework for QoS-based routing in the internet. RFC 2386, Internet Engineering Task Force (1998). http://www.rfc-editor.org/rfc/rfc2386.txt

Ding, W., Xue, G.: On the minimum diameter cost-constrained steiner tree problem. In: Lin, G. (ed.) Combinatorial Optimization and Applications, pp. 37–48. Springer, Heidelberg (2012)

Ding, W., Lin, G., Xue, G.: Diameter-constrained Steiner tree. In: Wu, W., Daescu, O. (eds.) Combinatorial Optimization and Applications, pp. 243–253. Springer, Heidelberg (2010)

Farooq, M.O., Sreenan, C.J., Brown, K.N., Kunz, T.: Design and analysis of RPL objective functions for multi-gateway ad-hoc low-power and lossy networks. Ad Hoc Netw. **65**, 78–90 (2017). https://doi.org/10.1016/j.adhoc.2017.08.002

Gaddour, O., Koubâa, A.: RPL in a nutshell: a survey. Comput. Netw. **56**(14), 3163–3178 (2012). https://doi.org/10.1016/j.comnet.2012.06.016

Gaddour, O., Koubâa, A., Baccour, N., Abid, M.: OF-FL: QoS-aware fuzzy logic objective function for the RPL routing protocol. In: 2014 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), pp. 365–372 (2014). https://doi.org/10.1109/WIOPT.2014.6850321

Ghaleb, B., Al-Dubai, A.Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L.M., Boukerche, A.: A survey of limitations and enhancements of the IPv6 routing protocol for low-power and lossy networks: a focus on core operations. IEEE Commun. Surv. Tutor. **21**(2), 1607–1635 (2019). https://doi.org/10.1109/COMST.2018.2874356

Goyal, D., Tripathy, M.R.: Routing protocols in wireless sensor networks: a survey. In: 2012 Second International Conference on Advanced Computing Communication Technologies, pp. 474–480 (2012). https://doi.org/10.1109/ACCT.2012.98

Iova, O., Theoleyre, F., Noel, T.: Using multiparent routing in RPL to increase the stability and the lifetime of the network. Ad Hoc Netw. **29**, 45–62 (2015). https://doi.org/10.1016/j.adhoc.2015.01.020

Iova, O., Picco, P., Istomin, T., Kiraly, C.: RPL: the routing standard for the internet of things... or is it? IEEE Commun. Mag. **54**(12), 16–22 (2016). https://doi.org/10.1109/MCOM.2016.1600397CM

Kamgueu, P., Nataf, E., Ndie, T.D.: On design and deployment of fuzzy-based metric for routing in low-power and lossy networks. In: 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), pp. 789–795 (2015). https://doi.org/10.1109/LCNW.2015.7365929

Kamgueu, P.O., Nataf, E., Ndie, T.D.: Survey on RPL enhancements: a focus on topology, security and mobility. Comput. Commun., 1–17. https://doi.org/10.1016/j.comcom.2018.02.011

Karkazis, P., Trakadas, P., Leligou, H.C., Sarakis, L., Papaefstathiou, I., Zahariadis, T.: Evaluating routing metric composition approaches for QoS differentiation in low power and lossy networks. Wirel. Netw. **19**(6), 1269–1284 (2013). https://doi.org/10.1007/s11276-012-0532-2

Khallef, W.: Multi-constrained quality of service routing in networks. Ph.D. thesis, Université Montpellier (2017). https://hal-lirmm.ccsd.cnrs.fr/tel-01887886

Khallef, W., Molnár, M., Bensliman, A., Durand, S.: On the QoS routing with RPL. In: 2017 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), pp. 1–5 (2017a). https://doi.org/10.23919/PEMWN.2017.8308028

Khallef, W., Molnár, M., Benslimane, A., Durand, S.: Multiple constrained QoS routing with RPL. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–6 (2017b). https://doi.org/10.1109/ICC.2017.7997081

Kobo, H., Abu-Mahfouz, A., Hancke, G.: A survey on software-defined wireless sensor networks: challenges and design requirements. IEEE Access **5**, 1872–1899 (2017). https://doi.org/10.1109/ACCESS.2017.2666200

Kompella, V.P., Pasquale, J.C., Polyzos, G.C.: Multicasting for multimedia applications. In: Proceedings of the Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies on One World Through Communications, vol. 3. IEEE Computer Society Press, Los Alamitos, pp. 2078–2085. IEEE INFOCOM 1992 (1992)

Kuipers, F.A., Mieghem, P.V.: MAMCRA: a constrained-based multicast routing algorithm. Comput. Commun. **25**(8), 802–811 (2002). https://doi.org/10.1016/S0140-3664(01)00402-9

Kulkarni, N., Prasad, N.R., Prasad, R.: Q-MOHRA: QoS assured multi-objective hybrid routing algorithm for heterogeneous WSN. Wirel. Pers. Commun. **100**(2), 255–266 (2018). https://doi.org/10.1007/s11277-017-5064-8

Kumar, P., Chauhan, N., Chand, N.: Node activity based routing in opportunistic networks. In: Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies, pp. 265–277. Springer, Singapore (2019)

Kumar, T.J., Singamsetty, P.: An exact algorithm for multi-constrained minimum spanning tree problem. Int. J. Math. Oper. Res. **12**(3), 317–330 (2018). https://doi.org/10.1504/IJMOR.2018.10010953

Lozano, L., Medaglia, A.L.: On an exact method for the constrained shortest path problem. Comput. Oper. Res. **40**(1), 378–384 (2013). https://doi.org/10.1016/j.cor.2012.07.008

Mohamed, B., Mohamed, F.: QoS routing RPL for low power and lossy networks. Int. J. Distrib. Sens. Netw. **2015**, 1–10 (2015). https://doi.org/10.1155/2015/971545

Mohamed, R.E., Saleh, A.I., Abdelrazzak, M., Samra, A.S.: Survey on wireless sensor network applications and energy efficient routing protocols. Wirel. Pers. Commun. **101**(2), 1019–1055 (2018). https://doi.org/10.1007/s11277-018-5747-9

Molnár, M.: Hierarchies to solve constrained connected spanning problems. Technical Report RR-11029, LIRMM (2011). https://hal-lirmm.ccsd.cnrs.fr/lirmm-00619806

Molnár, M., Bellabas, A., Lahoud, S.: The cost optimal solution of the multi-constrained multicast routing problem. Comput. Netw. **56**(13), 3136–3149 (2012). https://doi.org/10.1016/j.comnet.2012.04.020. Challenges in High-Performance Switching and Routing in the Future Internet

Mostafa, B., Benslimane, A., Saleh, M., Kassem, S., Molnár, M.: An energy-efficient multiobjective scheduling model for monitoring in internet of things. IEEE IoT J. **5**(3), 1727–1738 (2018). https://doi.org/10.1109/JIOT.2018.2792326

Neve, H.D., Mieghem, P.V.: TAMCRA: a tunable accuracy multiple constraints routing algorithm. Comput. Commun. **23**(7), 667–679 (2000). https://doi.org/10.1016/S0140-3664(99)00225-X

Randhawa, S., Jain, S.: Data aggregation in wireless sensor networks: previous research, current status and future directions. Wirel. Pers. Commun. **97**(3), 3355–3425 (2017). https://doi.org/10.1007/s11277-017-4674-5

Salama, H.F., Reeves, D.S., Viniotis, Y.: The delay-constrained minimum spanning tree problem. In: Proceedings Second IEEE Symposium on Computer and Communications, pp. 699–703 (1997). https://doi.org/10.1109/ISCC.1997.616089

Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, G.J.: Protocols for self-organization of a wireless sensor network. IEEE Pers. Commun. **7**(5), 16–27 (2000). https://doi.org/10.1109/98.878532

Su, S., Yu, H., Wu, Z.: An efficient multi-objective evolutionary algorithm for energy-aware QoS routing in wireless sensor network. Int. J. Sens. Netw. **13**(4), 208–218 (2013). https://doi.org/10.1504/IJSNET.2013.055583

The Cisco Learning Network: QoS architecture models: IntServ vs DiffServ (2017). https://learningnetwork.cisco.com/message/650042#650042. Accessed 22 June 2019

He, T., Stankovic, J.A., Lu, C., Abdelzaher, T.: SPEED: a stateless protocol for real-time communication in sensor networks. In: 2003 Proceedings of the 23rd International Conference on Distributed Computing Systems, pp. 46–55 (2003). https://doi.org/10.1109/ICDCS.2003.1203451

Van Mieghem, P., De Neve, H., Kuipers, F.: Hop-by-hop quality of service routing. Comput. Netw. **37**(3–4), 407–423 (2001)

Comparison of Neural Network Training Functions for RSSI Based Indoor Localization Problem in WSN

Satish R. Jondhale[1(✉)], Manish Sharma[2], R. Maheswar[3], Raed Shubair[4], and Amruta Shelke[5]

[1] Department of E&TC, Amrutvahini College of Engineering, Sangamner, India
profsatishjondhale@gmail.com
[2] Department of E&TC, D Y Patil COE, Pune, India
manishsharma.mitm@gmail.com
[3] SEEE, VIT Bhopal University, Bhopal, MP, India
maheshh3@rediffmail.com
[4] Department of Electrical Engineering and Computer Science, MIT, Cambridge, USA
rshubair@mit.edu
[5] Department of Instrumentation Engineering, Pravara Rural Engieering College, Loni, India
shelke.amru@gmail.com

Abstract. Indoor target localization using received signal strength indicator (RSSI) is an important research areas in wireless sensor network (WSN) domain. The environmental issues such as reflections, multi path fading pose a major challenge in front of localization systems to achieve high localization accuracy. The important reason behind this is the noise uncertainty in RSSI measurements. The application of artificial neural network (ANN) does not necessitates the prior knowledge of noise distribution and therefore they can be successfully applied in RSSI based target localization applications in indoor environment. However, choosing an appropriate training function for training the ANN is a very crucial task. The objective of this chapter is to compare the performance of 11 different types of training functions used to train the proposed Feed Forward Neural Network (FFNT) for the RSSI based indoor target localization in WSN. The comparison of these training functions is made with respect to Average Localization Error by varying the Noise Variance in the RSSI measurements from 0 dBm to 5 dBm in the steps of 1 dBm. The simulation results conclude that out of all the proposed training functions as well as trilateration-based technique, Levenberg-Marquardt (LM) based FFNT implementation shows higher Average Localization Error and is more consistent in providing better location estimates.

Keywords: Received signal strength indicator (RSSI) · Wireless sensor network (WSN) · Artificial neural network (ANN) · Feed Forward Neural Network (FFNT) · Levenberg-Marquardt (LM)

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 112–133, 2020.
https://doi.org/10.1007/978-3-030-40305-8_7

1 Introduction

The continuous advancements in wireless technology enabled the use of WSN for various of new positioning, tracking and navigation applications [1–3]. The target Localization and Tracking (L&T) is a very hot research area of WSN with wide variety of applications including but not limited to, locating mobile objects, wildlife tracking, as well as various Location Based Services (LBS). The objective of localization is to estimate the unknown target locations and that of tracking is to estimate a complete track of the mobile target trajectory using field measurements [4]. The localization is basically a one-step solution of a multi-step tracking problem. The L&T of objects in an indoor environment with high accuracy can trigger variety of new LBS applications. However, environmental dynamicity due to RF signal propagation issues such as non-line of sight (NLOS), signal attenuation, multi path propagation makes the indoor L&T problem highly challenging. Global Positioning System (GPS) can be used for L&T, however important challenges in this process are NLOS and the cost involved [5–7]. The localization accuracy of the GPS for outdoor environment is around 3.5 m which is not suitable for the indoor LBS [5]. Therefore, the current research direction in L&T community is to develop GPS-Less system for L&T applications. Easy deployment, low cost, self-organizing capability, and unattended working make WSN important alternative solution for indoor L&T. The dominant wireless technologies to implement WSN based indoor L&T system are RFID [8–10], Bluetooth [11, 12] and Wi-Fi [13, 14].

The WSN driven localization can be broadly categorized as Range Based (relies on computation of distances between nodes) and Range Free (relies on the utilization of information other than distance (range free approach) [4]. The first category utilizes field measurements such as Angle of Arrival (AoA), Time of Arrival (ToA), Time Difference of Arrival (TDoA), and RSSI [4]. In the ToA based approach, time of arrival of signal from the transmitter to receiver is used to estimate distances, whereas the TDoA based approach uses time difference of arrival of signals traveling between transmitter and receiver. The major problems with ToA and TDoA are: requirement of the perfect time synchronization between transmitter and receiver, NLOS, interferences. The AoA based approach utilizes angles of arrival of signals between target and sensor nodes. The requirement of an array of directional antennas is the major drawback of AoA technique. As against this, the RSSI based localization approach neither need clock synchronization or any additional hardware [15–18]. Additionally, this approach is simple to use and has comparatively a lower power requirement. That's why it has been widely used measurement type for WSN based L&T applications. In the RSSI-based approach distance between transmitter and receiver are estimated by utilizing RSS using an appropriate signal path loss model [19, 20].

Thus the location estimation of the mobile target based on the RSSI measurements can't be accurately executed using traditional technique such as trilateration or angulation because of issues such as multipath propagation, NLOS, fading [21–23]. Due to sources of error, the RSSI based L&T systems shows significant localization errors because of significant fluctuations in RSSI measurements. In order to overcome these problems, these traditional techniques must be replaced by more advanced technique

such as ANN. Quick learning capability, ease of use, flexible modeling makes ANN more suitable in dynamic wireless environments [23–25]. In addition, it does not need the prior knowledge of the given wireless channel characteristics. Training algorithms of ANN are categorized into five groups such as Gradient Descent, Conjugate Gradient, Resilient Backpropagation, Quasi-Newton, and Levenberg-Marquardt. The ANN can be trained with these training functions. The major challenge in applying the ANN for the given indoor localization problem is the selection of appropriate activation function. The prime objectives of this chapter are: (i) To compare all of these activation functions based on the indoor localization performance. These localization results are also compared with that of the traditional trilateration technique, (ii) To investigate each of these implementations for highly nonlinear system dynamics and environmental dynamicity. That means the variance of the RSSI measurement noise is varied from 0 dBm to 5 dBm in the steps of 1 dBm. Unlike the trilateration technique, the proposed ANN technique with various activation functions based indoor localization approach do not necessitates the need of computing the distances between two sensor nodes. Instead of distance estimation, the proposed ANN architectures directly estimate target unknown location based on the corresponding set of RSSI measurements. The outline of this chapter is as follows: Sect. 2 discusses the existing ANN based localization systems. Section 3 presents the dominant WSN based indoor target localization techniques. Section 4 presents the system assumption and design. The discussion on results is discussed in Sect. 5. The conclusions and future scope are highlighted in Sect. 6.

2 Related Work

RSSI-based localisation approaches can be classified into Path Loss Model based methods [26–28] and RF Fingerprinting based methods [25–27],. The former approach first converts the RSSI's into distances using the path loss model, and then computes the target location using these distances and coordinates of anchor (reference) nodes. However, the accurate computation of distances using noisy RSSI measurements using the path loss model is highly challenging task. The reason behind this is the inaccurate calibration of parameters of the given path loss model. The selection of appropriate values of model parameters is highly challenging in the context of environmental dynamicity [26]. Even though the path loss model works well for a certain time period, its performance degrades if the RF environment changes further. The RF fingerprinting based approach builds a radio map in the offline stage and then estimates unknown locations by comparing online RSSI vector with radio map constructed in the former offline stage. In [30], the authors proposed a BLE fingerprinting based indoor positioning system using 19 beacons distributed in an area of 600 square meters. The authors also investigated the impact of important issues such as fast fading, beacon density, transmit power, and transmit frequency on the positioning accuracy. The proposed approach shows the improved localization accuracy than Wi-Fi fingerprinting based approach. In other fingerprinting solutions [29], the unknown location estimates are obtained using Bayesian theory and kernel functions. The major problem with the fingerprinting based approach is the requirement of comparing the input real time RSSI measurement vector for a given time instance with the offline radio map each time. This

comparison requirement for each new real time RSSI measurement vector increases the computational complexity of the overall system, making it unsuitable for obtaining real time L&T performance. The authors in [31] used the concepts of multiple frequencies and powers between the target and each anchor to get a large RSSI based radio map.

ANN is a very popular alternative to approximate multimodal and highly nonlinear models. Once trained with a suitable input and output vectors in the offline stage, the ANN has the capability to discover any linear or non-linear relationship between them. Recently, several ANN based solutions such as MLP [28], convolutional neural network (CNN) [33], Machine learning with RF signature [34, 35], multi-layer neural network (MLNN) [36], FFNT [37, 38], machine learning [39], GRNN [23, 25, 40], etc., have been proposed in the literature for L&T applications. In [28], the MLP network with 3 layers and 16 neurons is modelled to estimate the unknown locations of target using RSSI measurements. The work in [33] proposes a novel wireless signal compensation model which is based on population density, distance, and operative frequency for the considered indoor environment. Once the number of individuals (population density) is calculated using CNN based approach, then, the mapping between the signal attenuation and the population density is adopted in the proposed model. At the end, for the location estimation the traditional trilateration technique is employed. The simulation results demonstrate that the proposed model yields improved localization accuracy as compared to other existing RSSI models. The novel concept of RF signature consisting of RSSI, Channel Transfer Function (CTF) and Frequency Coherence Function (FCF), has also been tried along with machine learning approach for indoor target localization problem recently [34, 35]. In [36], the authors neither employed path loss model or RF fingerprinting for the problem of RSSI-based indoor localisation. The authors proposed MLNN based approach integrates three stages: RSSI signals transforming section, de-noising section and the localization section. The database of RSSI measurements is utilized to train MLNN to get network parameters. To further refine the localization accuracy a boosting method is designed. The research work in [37] used a FFNT based approach to estimate the position of the mobile node using a ZigBee based WSN in the indoor environment. The mobile node is supposed to collect the RSSI measurements from five anchor nodes. These RSSI measurements are used to train the proposed FFNT using Levenberg-Marquardt (LM) training algorithm. The estimation results of the proposed approach are compared with that of a weighted k-nearest neighbor method. The proposed scheme shows improved localization accuracy than ANN with the consideration of five anchor nodes. In [38], two approaches were considered to estimate the distance between the mobile sensor node and the anchor node in both the outdoor and indoor environments. The first approach was based on the log-normal shadowing model (LNSM), while the second approach was based on a proposed hybrid particle swarm optimization– ANN (PSO–ANN) algorithm. A FFNT trained with LM algorithm is used to estimate the distance between the mobile node and the anchor. The proposed algorithm yield improved estimation accuracy than the LNSM based scheme. The work in [39] adopt the combination of machine learning and KF for target tracking in which kernel-based ridge regression and least squares technique are utilized for training. In this, the RSSI measurements are collected to construct radio fingerprint which is then used with machine learning algorithms to compute a model that estimates the position of the target using only RSSI

measurements. The fingerprinting computes location estimate of mobile target, which is then refined with the KF.

The GRNN is a highly parallel neural network which can also be used for target L&T applications [23, 25, 40–44]. In [40], the GRNN based algorithm GRNNα, is proposed to estimate target locations in 3-D. The performance of the proposed algorithm is compared with that of KF using extensive simulations. The GRNN can be trained with the simulated or real time (obtained from WSN nodes) RSSI measurements received at mobile target and the corresponding actual target locations. In [25], we have proposed a novel GRNN based localization algorithms (namely GRNN+KF and GRNN+Unscented KF (UKF)) as against the traditional trilateration-based approach, to obtain location estimates in WSN, which are then refined using KF. The proposed algorithms are compared with traditional RSSI-based, GRNN-based approach, RSSI+KF and RSSI+UKF algorithms. In [23], two algorithms GRNN+KF and GRNN+UKF are proposed to locate a moving person using a hybrid network of PSOC BLE nodes and smartphone. The proposed algorithms demonstrate tracking accuracy of the order of few centimeters [23, 43].

Although ANN is widely adopted in target L&T applications, most of these above implementations are still facing the following challenges: (1) Low Localization Accuracy, (2) Requirement of large training samples, (3) Inability to accommodate uncertainty in noise in the RSSI measurements due to signal propagation issues such as fading, reflections, multipath propagation, and NLOS, (4) Inability to deal with highly nonlinear RSSI-Distance mapping. None of the above implementations have tested and verified their algorithms for the variation in the variance of the measurement noise. To address all of these important issues, this paper focuses on application of various types ANN architectures which are efficient in terms of the localization accuracy, computational complexity and are capable to deal with noise uncertainty in RSSI measurements. The comparison of localization performance of these proposed ANN architecture is made with the traditional trilateration based technique.

3 Application of Various Training Functions in Indoor Localization

3.1 Generation of the RSSI Measurements Using the LNSM

Flexibility in parameter setting makes LNSM model more popular in WSN based research community. This paper follows the LNSM to generate RSSI measurements. The LNSM is the most suitable model. Its mathematical form is presented in detail below.

The RSSI $(z_{\ell j,k})$ received at the node N_ℓ with coordinates $(x_{\ell k}, y_{\ell k})$ at time k, after being transmitted from the node N_j with coordinates (x_{jk}, y_{jk}), propagates as follows [23, 45]:

$$z_{\ell j,k} = P_r(d_0) - 10n \log(d_{lj,k}/d_0) + X_\sigma \ , \tag{1}$$

where

- $P_r(d_0)$ is RSSI measured at receiver node located at some reference distance d_0 from transmitter,
- X_σ is normal random variable (a measure of shadowing effect) with a standard deviation of σ. The σ is the square root of Variance. In this research work, the variance is varied from 0 dBm to 5 dBm in the steps of 1 dBm,
- n is the path loss exponent, and is empirically determined by field measurement. In the proposed research work, the value of n is found to be 4.5.

The distance $d_{\ell j,k}$ between nodes N_ℓ and N_j can be computed with the help of Eq. (2) as given below.

$$d_{\ell j,k} = d_0 10^{(P_r(d_0) - z_{lj,k} + X_\sigma) / 10n} \tag{2}$$

To locate target using the trilateration technique, minimum three distances of target from three anchor nodes along with their location coordinates are must [46, 47]. By measuring two RSSI values for the two known distances and $P_r(d_0)$ for the given indoor environment, one can easily compute the value of n with the help of Eq. (1).

3.2 ANN Training Functions

A training algorithm decides about the updating the weights of the ANN. There are various types of ANN training functions [48, 49]. It is very crucial task to choose an appropriate training algorithm for the underlying indoor target localization problem. In this work, the training functions are grouped into five categories as Gradient Descent, Quasi-Newton, Conjugate Gradient, Resilient Back-propagation, and Levenberg-Marquardt algorithms as shown in Table 3. All of these training functions are utilized to train the proposed FFNT architecture for the considered target localization problem (Table 1).

Table 1. Various ANN training functions with their group number

Group No	Acronym	Description
1	**GD**	Gradient descent backpropagation
1	**GDA**	Gradient descent with adaptive learning rate backpropagation
1	**GDX**	Gradient descent with momentum and adaptive learning rate backpropagation
2	**RP**	Resilient Backpropagation
3	**CGF**	Conjugate gradient backpropagation with Fletcher-Reeves restarts
3	**CGP**	Conjugate gradient backpropagation with Polak/Ribiére restarts
3	**CGB**	Conjugate gradient with Powell/Beale restarts
3	**SCG**	Scaled conjugate gradient backpropagation
4	**BFG**	BFG Quasi-Newton backpropagation
4	**OSS**	One-step secant backpropagation
5	**LM**	Levenberg-Marquardt backpropagation

Gradient Descent Algorithms (GDAs): The most basic GDA algorithm is gradient descent backpropagation (GD) is the batch steepest descent training algorithm [50]. It aims to reduce network error as early as possible. It often converges slowly, trapped in a local minimum. Therefore, it may not yield the optimum performance. In order to overcome this drawback of GD, some of its other variants such as Gradient Descent with Adaptive Learning Rate Backpropagation (GDA), and Gradient Descent with Momentum and Adaptive Learning Rate Backpropagation (GDX) are quite popular [50, 51]. Adaptive learning rate is unique feature in GDA. The possible largest learning rate is desired without triggering oscillation in GDA. The concepts of adaptive learning rate and momentum are combined in GDX.

Resilient Backpropagation (RP): In this the convergence speed is enhanced by changing only the sign of the derivative, and not the magnitude of derivative of the error function during weight update. This important change lowers the number of learning steps and other adaptive parameters [52].

Conjugate Gradient Algorithms (CGAs): It is basically an optimization method which is more efficient than GDA's. It has a low memory requirement and shows fast convergence. However, it shows unstability in large-scale problems in number of instances [51, 53].

Quasi-Newton Algorithms (QNAs): *Like* CGAs, this group exhibits fast optimization [54]. However, the computation cost of QNAs is higher than that of CGAs. The weight updation is carried out using Newton method. As it does not require computation of second derivatives, therefore it is named as Quasi-Newton.

Levenberg-Marquardt Algorithm (LM): It is standard training function which is popular for solving nonlinear least squares problems [55]. It is a combination of GD and Gauss-Newton method.

3.3 FFNT Based Indoor Localization

In FFNT, the information moves only in forward direction from the input nodes, to the output nodes. There are no cycles or loops in the network. In this research work, a three-layer FFNT with the RSSI vector $X = [RSSI1, RSSI2, RSSI3, RSSI4]$ as input, one hidden layer with H sigmoid nodes, and a linear output unit, is proposed as shown in Fig. 4. The output of the proposed FFNT is the estimated unknown location $(\hat{x}, \hat{y})$ given below in Eq. (3).

$$(\hat{x}, \hat{y}) = \sum_{i=1}^{H} \mathbf{W_i^{(2)}} \sigma\left(\sum_{j=1}^{N} \mathbf{W_{ij}^{(1)}} X(i) + \mathbf{b_i}\right) \tag{3}$$

$\mathbf{W_i^{(1)}}$ represents the weight connecting the input unit j to the hidden unit i, $\mathbf{W_i^{(2)}}$ represents the weight connecting the hidden unit i to the output unit, $b_\mathbf{i}$ represents the bias of hidden unit i, and σ is the sigmoid transfer function (Fig. 1).

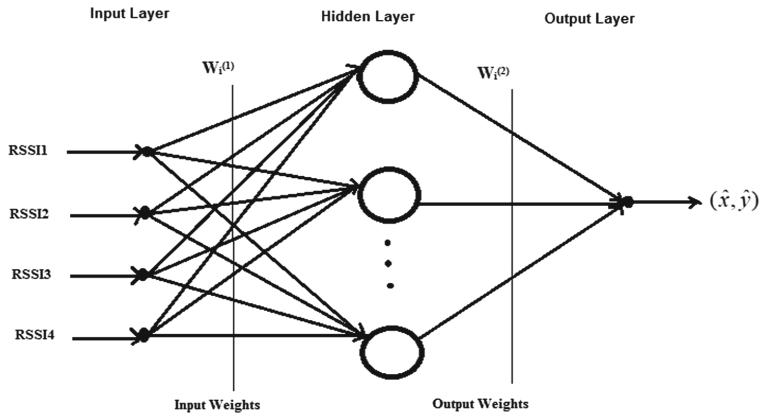


Fig. 1. The proposed FFNT architecture for localization of non-anchor nodes.

4 System Assumptions and Design

4.1 System Design

The proposed research work simulates the indoor environment of area 100 m × 100 m using MATLAB 2013a. The deployment of anchor nodes (See Table 2) and unknown target locations (See Table 3) are shown by red asterisk points and blue asterisk points respectively in the simulated indoor environment as shown in Fig. 5. The anchor density and unknown target locations are 12 and 30 respectively. The 2-D locations of the deployed anchors and non-anchors are given in Tables 2 and 3. The transmission power and communication radius for each sensor node are set to be 0 dBm and 100 m respectively. The LNSM model is used to generate RSSI values (See Eq. (1)). These RSSI measurements are utilized to estimate the unknown target locations using the traditional trilateration and the proposed FFNT architecture with various training functions as discussed in the Sect. 3 (Fig. 2).

The training database for the proposed FFNT architecture for the given indoor localization problem is generated as shown in Fig. 3. The training database contains total 30 RSSI vectors X_i $(i = 1, 2, \ldots, p)$ and corresponding p unknown locations to be estimated during online localization phase. Thus, here $p = 30$. Each set of training data contains one RSSI vector and the corresponding unknown 2-D location. The RSSI measurements utilized in the training database are those which are measured for variance of RSSI measurement noise = 0 dBm. During the online location estimation phase, the variance of RSSI measurement noise is varied from 0 dBm to 5 dBm in the steps of 1 dBm. In the simulation environment, all the 12 anchor nodes broadcast RF signal to each of the 30 unknown non anchor nodes whose locations are to be estimated. That means each of these 30 unknowns non anchor nodes receive 12 RSSI measurements. Out of these 12 RSSI measurements received at unknown location of non-anchor node, any 4 RSSI measurements from any 4 random anchor nodes and their corresponding 2-D locations are utilized to train the proposed FFNT architecture. Thus one training set contains $X_i = [RSSI1, RSSI2, RSSI3, RSSI4]$ and (x_i, y_i). The training

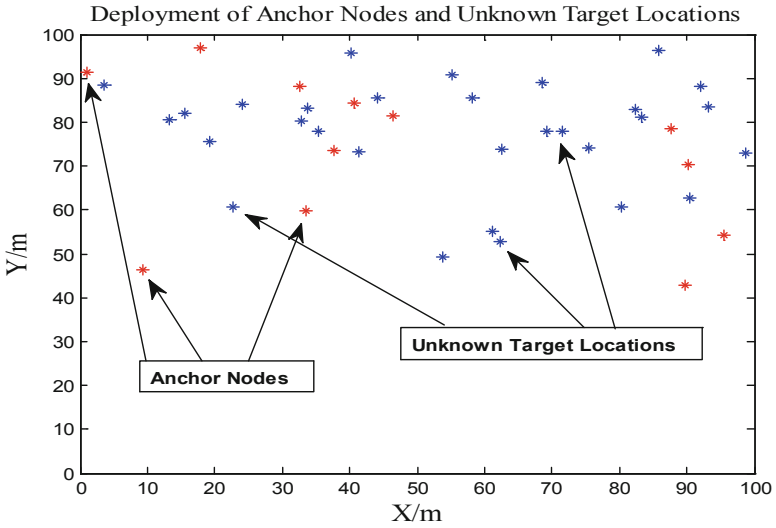


Fig. 2. The deployment of anchor and non-anchor nodes in the indoor environment of 100 m × 100 m.

Table 2. Deployment of anchor nodes in the simulations

Anchor node number	2-D location	Anchor node number	2-D location
1	(0.933, 91.50)	7	(37.75, 73.50)
2	(17.92, 96.89)	8	(90.20, 70.21)
3	(32.68, 88.03)	9	(33.43, 59.66)
4	(40.75, 84.45)	10	(95.41, 54.28)
5	(46.50, 81.40)	11	(9.299, 46.35)
6	(87.72, 78.49)	12	(89.84, 42.92)

database contains $p = 30$ such sets which are taken for Noise Variance = 3 dBm. As mentioned earlier in the online localization phase, the trilateration-based localization approach utilizes 4 real time RSSI measurements (which are higher in magnitude than rest of the others) out of 12 real time RSSI measurements. Whereas there is no such restriction of the RSSI input vector for the proposed FFNT architecture for localization during online localization phase. In other words, in case of proposed ANN architectures, any 4 random RSSI measurements can be utilized for the localization. The nodes with unknown locations receive RSSI measurements from all the 12 anchor nodes, which are utilized to estimate the unknown node locations using trilateration technique. Out of these 12 RSSI measurements received at each unknown node, only those three RSSI measurements are utilized which are highest in magnitude than the rest of the others in the case of trilateration-based estimation. Higher the RSSI value, closer the unknown node is from the given anchor node. Thus, in case of the trilateration-based estimation; we are providing selective high amplitude RSSI measurements so as to get more accurate estimations of unknown node locations. However, in case of the

Table 3. Unknown target locations to be estimated

Number of non anchor node	Unknown 2-D location of non anchor node to be estimated	Number of non anchor node	Unknown 2-D location of non anchor node to be estimated
1	(53.86, 49.17)	16	(15.57, 81.90)
2	(69.16, 77.90)	17	(33.81, 83.23)
3	(71.52, 78.05)	18	(82.41, 82.80)
4	(91.95, 88.10)	19	(93.22, 83.51)
5	(44.09, 85.62)	20	(32.79, 80.30)
6	(55.26, 90.75)	21	(62.28, 52.66)
7	(85.72, 96.36)	22	(83.18, 81.03)
8	(98.83, 72.95)	23	(35.41, 78.04)
9	(68.53, 88.95)	24	(90.48, 62.71)
10	(61.09, 55.00)	25	(40.14, 95.69)
11	(3.487, 88.54)	26	(22.60, 60.75)
12	(13.33, 80.42)	27	(19.34, 75.44)
13	(58.27, 85.49)	28	(41.44, 73.14)
14	(80.20, 60.72)	29	(62.49, 73.86)
15	(24.11, 84.14)	30	(75.51, 74.24)

proposed FFNT based implementation, any four random RSSI measurements are utilized during the training as well as online estimation phase. Thus, RSSI input requirements for the proposed FFNT architecture is less stringent as compared to that in case of trilateration-based approach.

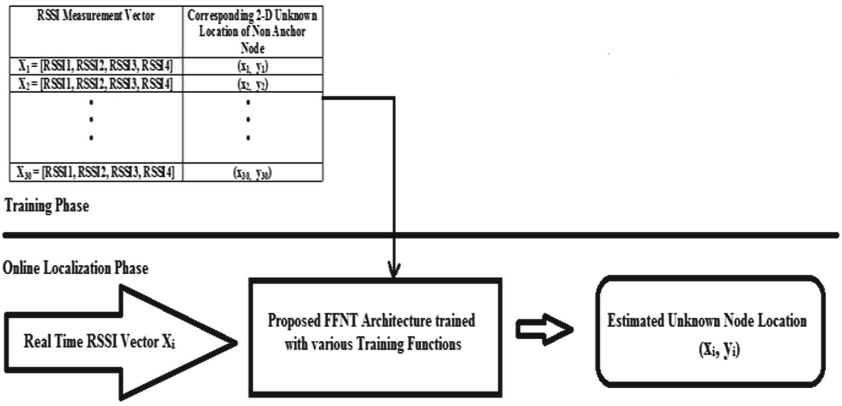


Fig. 3. Proposed FFNT based localization system with various training functions

4.2 Evaluation Parameters

The Localization Error represents the closeness between the estimated target location $(\hat{x}_i, \hat{y}_i)$ and actual location (x_i, y_i) (See Eq. (4)). The Average Localization Error is calculated by taking an average of all the Localization Errors for all the 30 estimations (See Eq. (5)). The values of these two metrics must be ideally as low as possible.

$$Localization\,Error = \sqrt{(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2},\ i = 1, 2, \ldots p. \tag{4}$$

$$Average\,Localization\,Error = \frac{\sum_{i=1}^{p} Localization\,Error}{p} \tag{5}$$

4.3 Flow of the Proposed Supervised Learning Based Localization Algorithms

The detailed flow of the proposed algorithm for unknown location estimation include three parts as shown below in Table 4.

Table 4. Flow of target localization with trilateration and the proposed approach

I. Offline Training Stage
Step 1: The proposed FFNT architecture is trained with 30 sets of four RSSI measurements from randomly selected four anchor nodes and corresponding actual locations of the target, using various training functions as described in the Section III.

II. Online Estimation of Unknown Target Location
Step 2:

- *For Trilateration Based Estimation:*

The target receives RSSI measurements transmitted by all 12 anchor nodes. These RSSI values are dispatched to the Base station.

- *For Proposed FFNT Based Estimations:*

The target receives RSSI transmitted from selected four anchor nodes. These RSSI values are dispatched to Base station.

Step 3:

- *For Trilateration Based Estimation:*

The base station run trilateration algorithm to compute the position estimate of target location. The localization errors in x and y location estimates are computed using Equation (4) as well as recorded.

- *For Proposed FFNT Based Estimations:*

The base station runs the proposed FFNT algorithm to compute the location estimate of unknown target location. The localization errors in x and y location estimates are computed as well as recorded.

III. Computation of Average Localization Error
Step 4: The Average Localization Error for all simulation experiments are computed using Equation (5).

Note: (1) The Step 2 and the Step 3 are repeated for each new unknown target location (p = 30), (2) The Step 2 to the Step 5 are repeated for varying the Noise Variance from 0 dBm to 5 dBm in the steps of 1 dBm.

5 Discussion on Results

In order to differentiate the estimation results of unknown target locations with the trilateration and the proposed FFNT based implementation, different color markers are used in the simulation results (See Figs. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 and 15). The red marker "*" indicates the position of anchor nodes, the blue marker "*" represents the actual position of unknown nodes, the black marker "+" denotes the estimated position of unknown nodes using trilateration. The markers utilized to show the estimations obtained using the proposed FFNT architecture trained with various types of training functions can also be noted down using Figs. 4, 6, 8, 10, 12, and 14 for all the noise variance cases (Variation in Variance from 0 dBm to 5 dBm) of the RSSI measurements. The comparisons of Localization Errors of the proposed FFNT architecture trained with various types of training functions with the traditional trilateration based implementation are shown in Figs. 5, 7, 9, 11, 13 and 15 for all the noise variance cases respectively. The corresponding comparison of Average Localization Errors for all of these variance cases is given in Table 5.

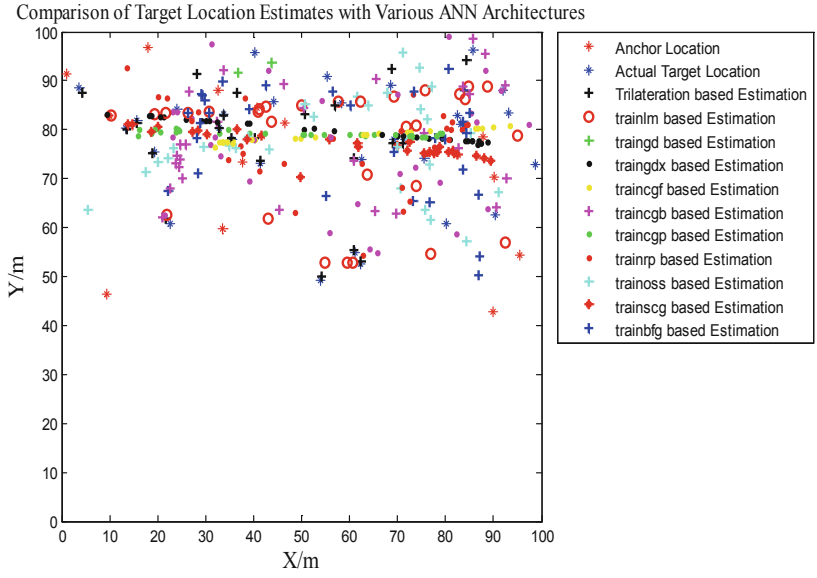


Fig. 4. Comparison of 2-D localization performances with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 0 dBm.

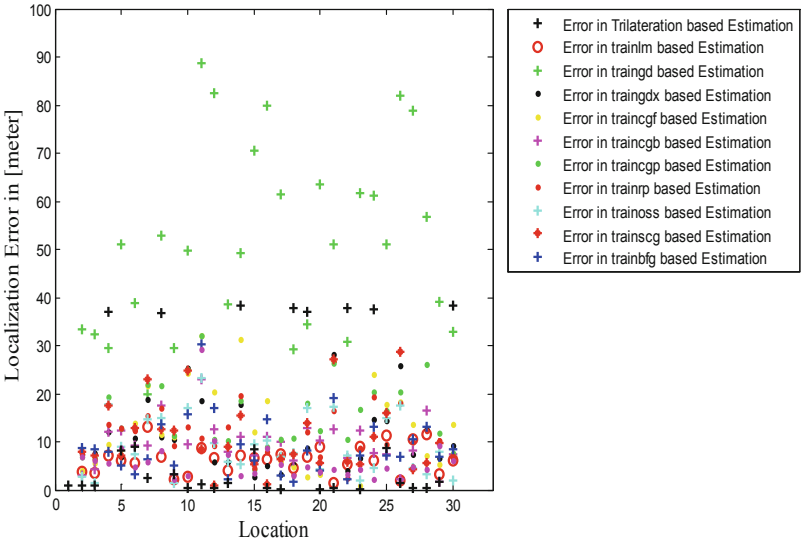


Fig. 5. Comparison of localization errors with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 0 dBm.

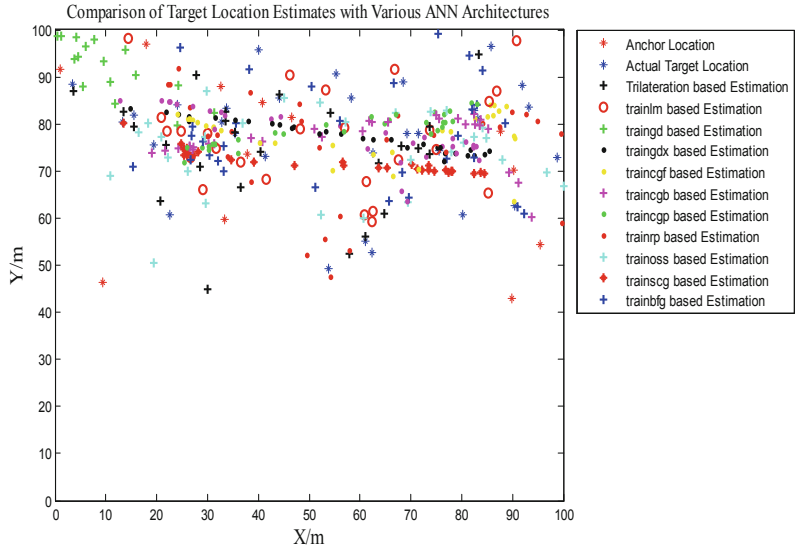


Fig. 6. Comparison of 2-D localization performances with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 1 dBm.

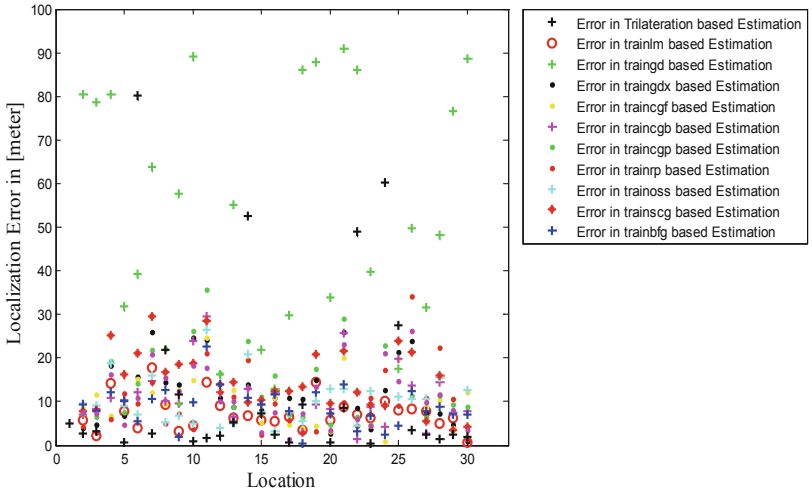


Fig. 7. Comparison of localization errors with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 1 dBm.

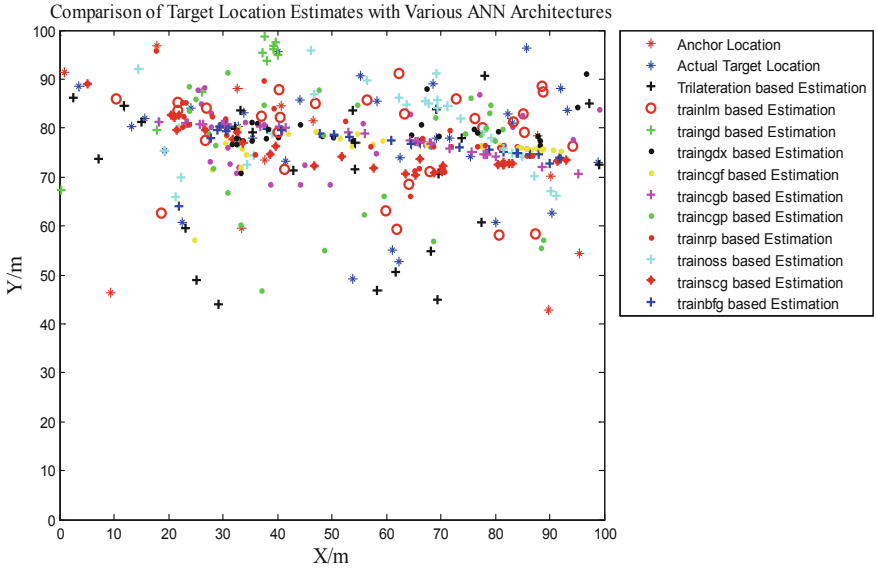


Fig. 8. Comparison of 2-D localization performances with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 2 dBm.

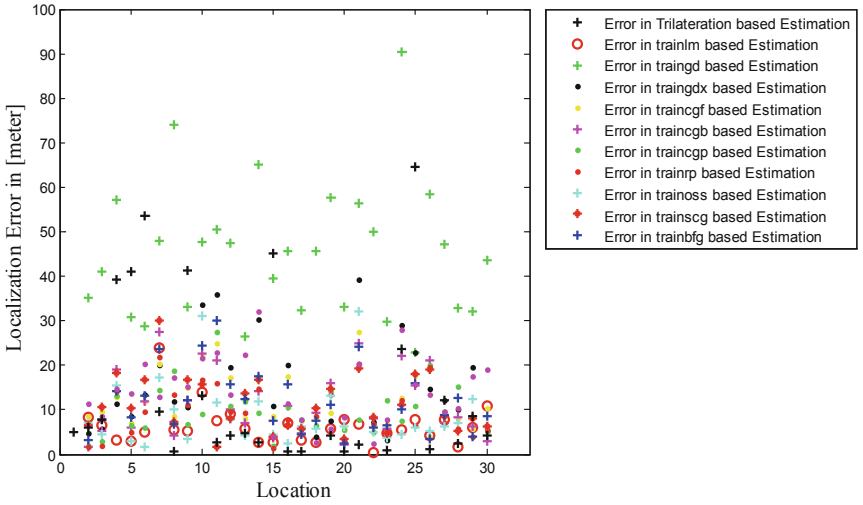


Fig. 9. Comparison of localization errors with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 2 dBm.

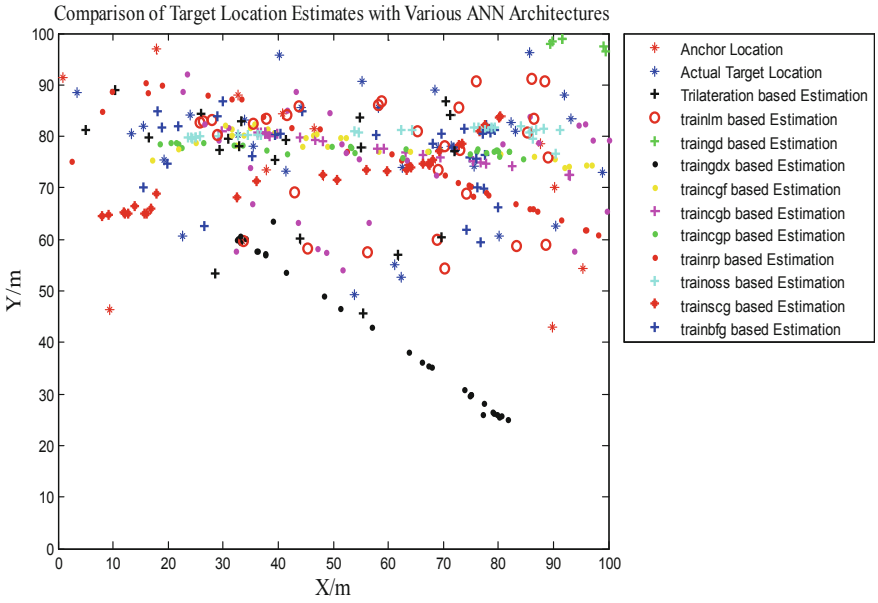


Fig. 10. Comparison of 2-D localization performances with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 3 dBm.

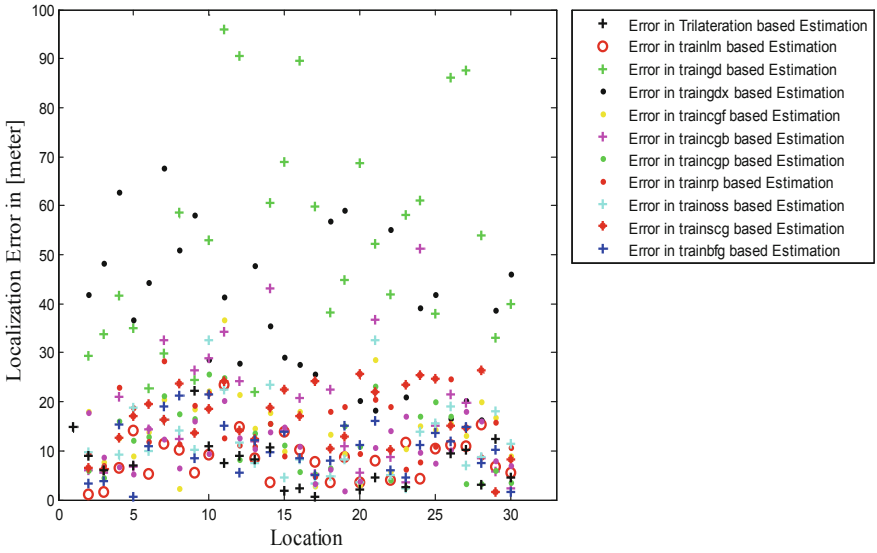


Fig. 11. Comparison of localization errors with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 3 dBm.

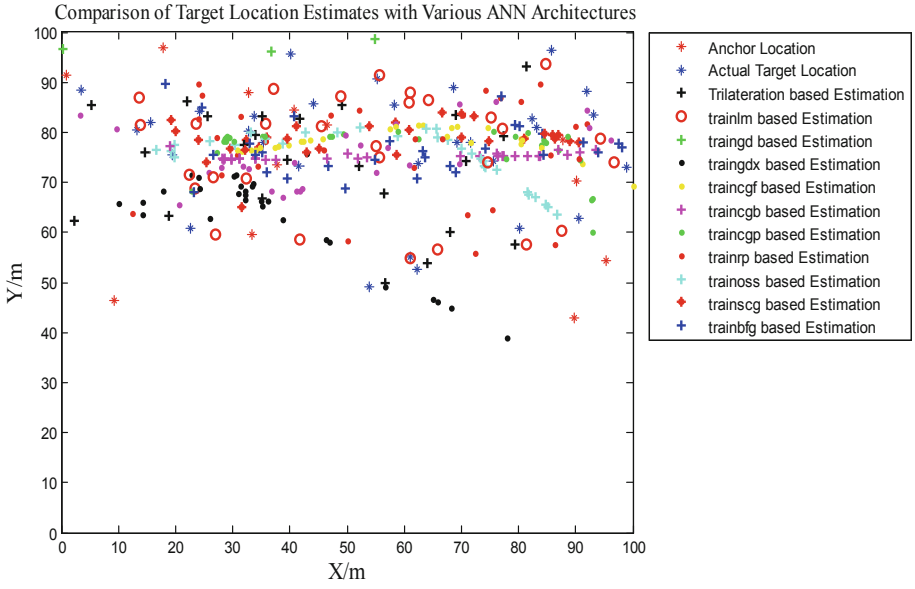


Fig. 12. Comparison of 2-D localization performances with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 4 dBm.

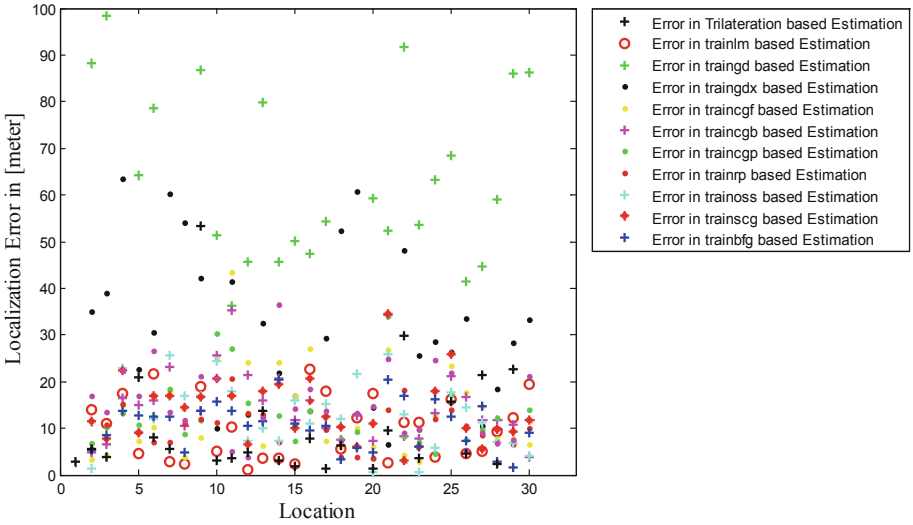


Fig. 13. Comparison of localization errors with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 4 dBm.

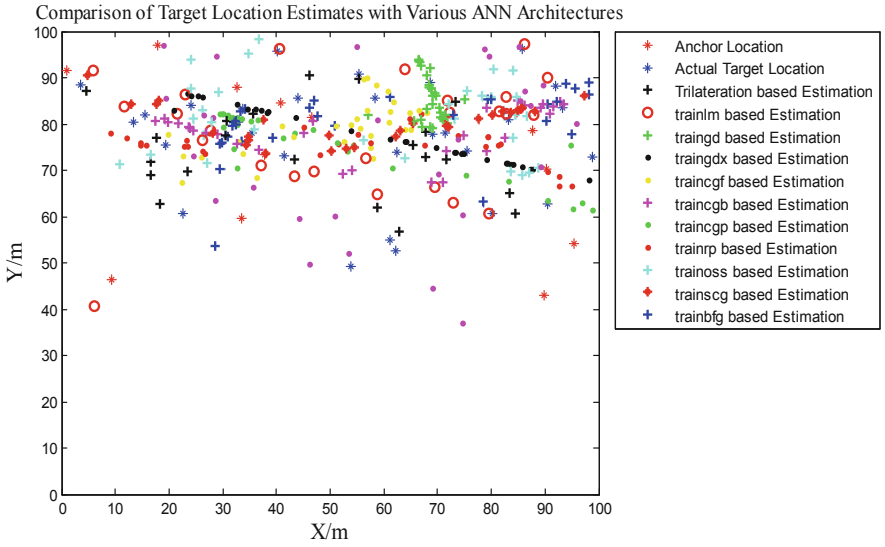


Fig. 14. Comparison of 2-D localization performances with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 5 dBm.

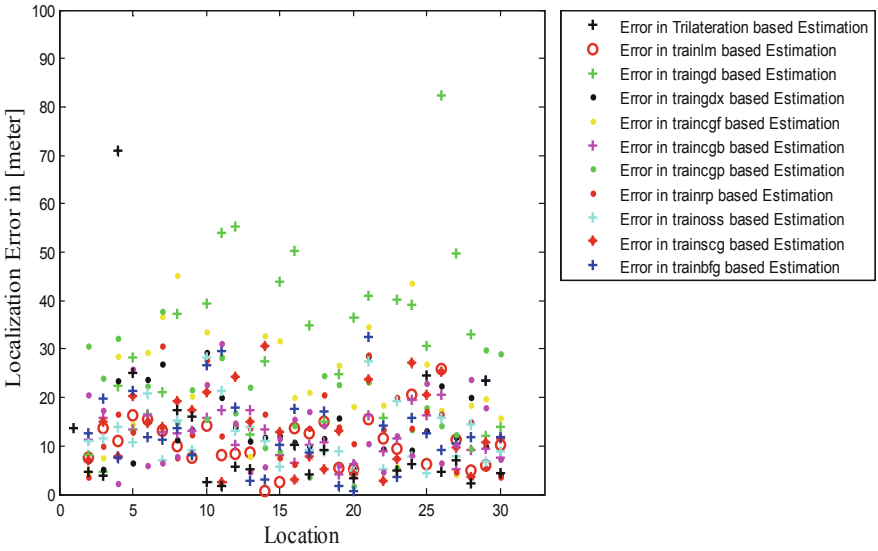


Fig. 15. Comparison of localization errors with various activation functions for the case of the RSSI measurement noise with Mean = 0 dBm, and Variance = 5 dBm.

The corresponding Numeric Results of Average Localization Errors for each of the above Noise Cases for 11 different types of training functions are as given below.

Table 5. Comparison of Average Localization Errors with the Trilateration and the Proposed FFNT with various types of Training Functions for the Variance varied from 0 dBm to 5 dBm in the steps of 1 dBm.

	Average localization error in meters with the RSSI measurement noise with Mean = 0 dBm					
Localization technique	Variance = 0 dBm	Variance = 1 dBm	Variance = 2 dBm	Variance = 3 dBm	Variance = 4 dBm	Variance = 5 dBm
Trilateration	11.7269	24.3776	22.1374	95.9116	50.1740	140.8888
LM	6.2928	7.6094	6.6615	8.6522	10.1910	10.9134
GD	51.3749	61.4095	45.0341	52.5637	71.3678	31.3934
GDX	11.6412	13.0414	15.6459	37.7128	30.5398	14.4729
GDA	13.7795	11.0416	12.5170	15.0631	14.0857	22.7338
CGF	9.7091	11.7830	12.0552	18.3379	15.2372	12.2380
CGB	15.6681	14.9180	9.8590	12.5824	13.1798	18.7902
CGP	10.8356	9.9286	9.9382	14.5911	10.4026	14.4241
RP	9.7256	10.2915	9.7631	13.0049	13.0065	12.6062
OSS	11.5900	15.2312	11.6711	17.2337	14.5276	14.0902
SCG	9.4187	9.1016	12.2480	10.9643	10.9659	14.0429
BFG	6.1638	11.8699	14.4911	10.7980	15.5179	12.5436

By observing all the simulation and the numeric results, it is clear that some of the training functions demonstrate satisfactory localization accuracy, whereas others show poor localization accuracy. The major findings from all these simulation and numeric results, following conclusions can be drawn very easily.

(1) As the variance of RSSI measurement noise increases, the increment in Average Localization Error for the Trilateration based implementation is more pronounced as compared to the rest of the other implementations (See Table 5). The Average Localization Error increases continuously as the variance of the RSSI measurement noise is increased from 0 dBm to 5 dBm in the steps of 1 dBm. In real time indoor environment, the uncertainty in noise variance in the RSSI measurements is generally very high. Therefore, the Trilateration based target localization solution for the indoor environments is not at all a suitable alternative.
(2) Out of all the localization results in the proposed FFNT based implementation with various training functions, the localization accuracy of the GD based implementation is worst. Therefore, it is not recommended for the indoor target localization problems.
(3) The results with GDA, GDX, CGF, CGB, and CGP are reported to be not consistent in providing accurate location estimates.
(4) The RP and the SCG training function based localization results are comparatively fairly better than rest of the other training function based results (Except LM based results). However, the consistency is still the issue to be resolved in these two implementations.
(5) As compared to all of the implementations (as shown in Table 5), the LM based implementation shows highest Localization Accuracy in most of the Variance cases. Additionally, the LM based results are consistent as the Variance is increased progressively. Thus, the LM based training to the proposed FFNT architecture is recommended for the RSSI based indoor target localization problems.

The major contributions of our work are: (1) The proposed research work presents the comparison of localization results with various activation functions based FFNT architecture for the RSSI based indoor target localization in the context of the nonlinear system dynamics, and the environmental dynamicity (uncertainty in noise distribution in RSSI measurements), (2) The proposed FFNT based implementation trained with various training functions are tested and compared with the traditional trilateration based localization technique by varying the variance of RSSI measurement noise from 0 dBm to 5 dBm in the steps of 1 dBm.

6 Conclusions and Future Work

This research work focus on the application of FFNT architecture trained with various training functions for the indoor target localization problem in WSN. The proposed algorithm deals with uncertainty in noise in RSSI measurements due to various issues such as NLOS, multipath propagation, reflection. The proposed FFNT architecture is trained with 30 sets of four RSSI measurements from randomly selected four anchor nodes and corresponding actual locations of the target and are validated with the help

of real-time RSSI measurements corresponding to 30 unknown locations to be estimated. In order to account fluctuation in noise in the RSSI measurements, the variance is varied from 0 dBm to 5 dBm in the steps of 1 dBm using LNSM path loss model and corresponding simulation and numeric results of localization are presented for the indoor environment area of 100 × 100 square meters. The comparison of Localization Accuracy of the proposed FFNT architecture trained with various training functions is made with traditional trilateration based technique in terms of Average Localization Error. The simulation results conclude that out of all the proposed training functions as well as trilateration based technique, Levenberg-Marquardt (LM) based FFNT implementation shows higher Average Localization Error and is more consistent in providing better location estimates.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2019)
3. Khan, M.S., Capobianco, A.-D., Asif, S.M., Anagnostou, D.E., Shubair, R.M., Braaten, B. D.: A compact CSRR-enabled UWB diversity antenna. IEEE Antennas Wirel. Propag. Lett. **16**, 808–812 (2016)
4. Hero, A.O., Moses, R.L., Patwari, N., Ash, J.K., Kyperountas, S., Correal, N.S.: Locating the nodes: cooperative localization in wireless sensor networks. IEEE Signal Process. Mag. **22**(4), 54–69 (2005)
5. Higgins, M.B.: Heighting with GPS : possibilities and limitations. Comm. Int. Fed. Surv. **5** (1999)
6. Hofmann-Wellenhof, B., Lichtenegger, H., Collins, J.: Global Positioning System: Theory and Practice. Springer, Heidelberg (2001)
7. Tariq, Z.B., Cheema, D.M., Kamran, M.Z., Naqvi, I.H.: Non-GPS positioning systems. ACM Comput. Surv. **50**(4), 57 (2017)
8. Wagner, B., Timmermann, D., Ruscher, G., Kirste, T.: Device-free user localization utilizing artificial neural networks and passive RFID. In: 2012 Ubiquitous Positioning, Indoor Navigation, and Location Based Service, UPINLBS 2012 (2012)
9. Zhang, Y., Li, X., Amin, M.: Principles and techniques of RFID positioning. In: RFID Systems: Research Trends and Challenges (2010)
10. Soltani, M.M., Motamedi, A., Hammad, A.: Enhancing cluster-based RFID tag localization using artificial neural networks and virtual reference tags. Autom. Constr. **54**, 93–105 (2015)
11. Zafari, F., Papapanagiotou, I., Devetsikiotis, M., Hacker, T.J.: Enhancing the accuracy of iBeacons for indoor proximity-based services. In: IEEE International Conference on Communications (2017)
12. Thaljaoui, A., Val, T., Nasri, N., Brulin, D.: BLE localization using RSSI measurements and iRingLA. In: Proceedings of the IEEE International Conference on Industrial Technology (2015)
13. Zhuang, Y., Li, Y., Qi, L., Lan, H., Yang, J., El-Sheimy, N.: A two-filter integration of MEMS sensors and WiFi fingerprinting for indoor positioning. IEEE Sens. J. **16**(13), 5123–5126 (2016)

14. Chen, Z., Zou, H., Jiang, H., Zhu, Q., Soh, Y.C., Xie, L.: Fusion of WiFi, smartphone sensors and landmarks using the Kalman filter for indoor localization. Sensors (Switzerland) **15**(1), 715–732 (2015)
15. Blumrosen, G., Anker, T., Hod, B., Dolev, D., Rubinsky, B.: Enhancing RSSI-based tracking accuracy in wireless sensor networks. ACM Trans. Sens. Netw. **9**(3), 29 (2013)
16. Paul, A.S., Wan, E.A.: RSSI-based indoor localization and tracking using sigma-point Kalman smoothers. IEEE J. Sel. Top. Signal Process. **3**(5), 860–873 (2009)
17. Dong, Q., Dargie, W.: Evaluation of the reliability of RSSI for indoor localization. In: 2012 International Conference on Wireless Communications in Underground and Confined Areas, ICWCUCA 2012 (2012)
18. Abouzar, P., Michelson, D.G., Hamdi, M.: RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture. IEEE Trans. Wirel. Commun. **15**(10), 6638–6650 (2016)
19. Wu, H., Zhang, L., Miao, Y.: The propagation characteristics of radio frequency signals for wireless sensor networks in large-scale farmland. Wirel. Pers. Commun. **95**(4), 3653–3670 (2017)
20. Sarkar, T.K., Ji, Z., Kim, K., Medouri, A., Salazar-Palma, M.: A survey of various propagation models for mobile communication. IEEE Antennas Propag. Mag. **45**(3), 51–82 (2003)
21. Garcia, J.L.M., Tomas, J., Boronat, F.: The development of two systems for indoor wireless sensors self-location. Ad Hoc Sens. Wirel. Netw. **8**(3–4), 235–258 (2009)
22. Viani, F., Rocca, P., Oliveri, G., Trinchero, D., Massa, A.: Localization, tracking, and imaging of targets in wireless sensor networks: an invited review. Radio Sci. (2011)
23. Jondhale, S.R., Deshpande, R.S.: GRNN and KF framework based real time target tracking using PSOC BLE and smartphone. Ad Hoc Netw. **84**, 19–28 (2019)
24. Irfan, N., Bolic, M., Yagoub, M.C.E., Narasimhan, V.: Neural-based approach for localization of sensors in indoor environment. Telecommun. Syst. **44**(1), 149–158 (2010)
25. Jondhale, S.R., Deshpande, R.S.: Kalman filtering framework-based real time target tracking in wireless sensor networks using generalized regression neural networks. IEEE Sens. J. **19** (1), 224–233 (2019)
26. Coluccia, A., Ricciato, F.: RSS-based localization via bayesian ranging and iterative least squares positioning. IEEE Commun. Lett. **18**(5), 873–876 (2014)
27. Dai, H., Zhu, Z.M., Gu, X.F.: Multi-target indoor localization and tracking on video monitoring system in a wireless sensor network. J. Netw. Comput. Appl. **36**(1), 228–234 (2013)
28. Patwari, N., Hero, A.O., Perkins, M., Correal, N.S., O'Dea, R.J.: Relative location estimation in wireless sensor networks. IEEE Trans. Signal Process. **51**(8), 2137–2148 (2003)
29. Fang, S.H., Lin, T.N., Lee, K.C.: A novel algorithm for multipath fingerprinting in indoor WLAN environments. IEEE Trans. Wirel. Commun. **7**(9), 3579–3588 (2008)
30. Faragher, R., Harle, R.: Location fingerprinting with bluetooth low energy beacons. IEEE J. Sel. Areas Commun. **33**(11), 2418–2428 (2015)
31. Zheng, X., Liu, H., Yang, J., Chen, Y., Martin, R.P., Li, X.: A study of localization accuracy using multiple frequencies and powers. IEEE Trans. Parallel Distrib. Syst. **25**(8), 1955–1965 (2014)
32. Yoo, J., Kim, H.: Target localization in wireless sensor networks using online semi-supervised support vector regression. Sensors (Switzerland) **15**(6), 12539–12559 (2015)
33. Jiao, J., Li, F., Deng, Z., Ma, W.: A smartphone camera-based indoor positioning algorithm of crowded scenarios with the assistance of deep CNN. Sensors (Switzerland) **17**(4), 704 (2017)

34. AlHajri, M.I., Ali, N.T., Shubair, R.M.: Classification of indoor environments for IoT applications: a machine learning approach. IEEE Antennas Wirel. Propag. Lett. **17**(12), 2164–2168 (2018)
35. AlHajri, M.I., Ali, N.T., Shubair, R.M.: Indoor localization for IoT using adaptive feature selection: a cascaded machine learning approach. IEEE Antennas Wirel. Propag. Lett. (2019)
36. Dai, H., Ying, W.-H., Xu, J.: Multi-layer neural network for received signal strength-based indoor localisation. IET Commun. **10**(6), 717–723 (2016)
37. Gogolak, L., Pletl, S., Kukolj, D.: Neural network-based indoor localization in WSN environments. Acta Polytech. Hung. **10**(6), 221–235 (2013)
38. Gharghan, S.K., Nordin, R., Ismail, M., Ali, J.A.: Accurate wireless sensor localization technique based on hybrid PSO-ANN algorithm for indoor and outdoor track cycling. IEEE Sens. J. **16**(2), 529–541 (2016)
39. Mahfouz, S., Mourad-Chehade, F., Honeine, P., Farah, J., Snoussi, H.: Target tracking using machine learning and Kalman filter in wireless sensor networks. IEEE Sens. J. **14**(10), 3715–3725 (2014)
40. Kaplan, G.B., Lana, A.: Comparison of proposed target tracking algorithm, GRNN α, to Kalman filter in 3D environment (2013)
41. Kişi, Ö.: Generalized regression neural networks for evapotranspiration modelling, vol. 6667 (2010)
42. Zhong, M., et al.: Gap-based estimation: choosing the smoothing parameters for probabilistic and general regression neural networks (2007)
43. Jondhale, S.R., Deshpande, R.S.: Kalman filtering framework based real time target tracking in wireless sensor networks using generalized regression neural networks. IEEE Sens. J. **19** (1), 224–233 (2018)
44. Rahman, M.S., Park, Y., Kim, K.D.: RSS-based indoor localization algorithm for wireless sensor network using generalized regression neural network. Arab. J. Sci. Eng. (2012)
45. Jondhale, S.R., Deshpande, R.S.: Modified Kalman filtering framework based real time target tracking against environmental dynamicity in wireless sensor networks. Ad-Hoc Sens. Wirel. Netw. **19**(1), 224–233 (2018)
46. Yang, Z., Liu, Y., Li, X.Y.: Beyond trilateration: on the localizability of wireless ad hoc networks. IEEE/ACM Trans. Netw. **18**(6), 1806–1814 (2010)
47. Uren, J., Price, W.F.: Triangulation and trilateration. In: Surveying for Engineers (2015)
48. Cömert, Z., Kocamaz, A.: A study of artificial neural network training algorithms for classification of cardiotocography signals. Bitlis Eren Univ. J. Sci. Technol. **7**(2), 93–103 (2017)
49. Günther, F., Fritsch, S.: neuralnet: training of neural networks. R J. **2**(1), 30–38 (2010)
50. Bengio, Y., Simard, P., Frasconi, P.: Learning long-term dependencies with gradient descent is difficult. IEEE Trans. Neural Netw. **5**(2), 157–166 (1994)
51. Glorot, X., Bengio, Y.: Understanding the difficulty of training deep feedforward neural networks. J. Mach. Learn. Res. (2010)
52. Patnaik, L.M., Rajan, K.: Target detection through image processing and resilient propagation algorithms. Neurocomputing **35**(1–4), 123–135 (2000)
53. Nazareth, J.L.: Conjugate gradient method. Wiley Interdisc. Rev. Comput. Stat. **1**(3), 348–353 (2009)
54. Ghaffari, A., Abdollahi, H., Khoshayand, M.R., Bozchalooi, I.S., Dadgar, A., Rafiee-Tehrani, M.: Performance comparison of neural network training algorithms in modeling of bimodal drug delivery. Int. J. Pharm. **327**(1), 126–138 (2006)
55. El-Nabarawy, I., Abdelbar, A.M., Wunsch, D.C.: Levenberg-Marquardt and Conjugate Gradient methods applied to a high-order neural network. In: Proceedings of the International Joint Conference on Neural Networks (2013)

Performance Assessment of the Fixed Node Assisted Collection Tree Protocol (FNA-CTP) in a Mobile Environment

Ramiro Liscano(✉), Aryan Kukreja, and Abdul Zainul-Abedin

Ontario Tech University, Oshawa, ON L1G 0C5, Canada
rliscano@ieee.org, {aryan.kukreja, abdul.zainulabedin}@ontariotechu.net

Abstract. The Fixed Node Assisted Collection Tree Protocol (FNA-CTP) is a Collection Tree Protocol (CTP) for sensor network that has been augmented with special fixed nodes in order to support mobility. The algorithm functions like the conventional CTP algorithm taking advantage of the fixed nodes only when it loses a parent. Prior simulation analysis of CTP in mobile environments demonstrated that conventional CTP has significant overhead when the sensor nodes are mobile even if some nodes are fixed. On the other hand, FNA-CTP reduces the overhead due to fixed nodes and alterations to the trickle algorithm. This chapter presents experimental analysis of the FNA-CTP algorithm implemented on a set of sensor nodes that support tinyOS in an indoor sports field. Unlike the simulation results, the experimental results show that CTP outperforms the FNA-CTP algorithm though this primarily because it was not possible to recreate an experiment where the sink node was out of range of the mobile nodes resulting in less parent changes in CTP than FNA-CTP. In this chapter we present details and challenges of these experiments such as capturing and preprocessing of the packets captured by a sniffer in the field as well as at the sink.

Keywords: Mobile sensor networks · Collection Tree Protocol · Experimental analysis

1 Introduction

Wireless Sensor Network (WSN) routing and energy consumption is still an area of importance in future networks and very relevant to the Internet of Things (IoT) as evidenced in a recent conference in futuristic trends in network and communication technologies [1]. One of the tracks in that conference was on wireless sensor networks and many of those papers were focused on routing and energy conservation. This chapter presents an experimental evaluation of a modified Collection Tree Protocol (CTP) [2] routing algorithm in order to reduce the number of control packets sent in the network that is proportional to the consumption of energy of the sensor nodes.

WSN data collection algorithms can be categorized into flat, hierarchical, and location based topologies [3]. Of these three topologies, flat and hierarchical are the most common. Flat network topologies, such as the Collection Tree Protocol (CTP) [2], are the simplest multi-hop topologies for WSNs as they can easily support dynamic

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 134–154, 2020.
https://doi.org/10.1007/978-3-030-40305-8_8

changes to the network such as addition and removal of nodes and changes in the quality of the communication links between the sensor nodes.

Hierarchical topologies, such as clustering algorithms, typically outperform other collection algorithms in saving energy and extending the lifetime of WSNs but at the cost of increased messaging overhead to maintain the clusters. This savings in energy is usually realized by the adoption of a Time Division Multiplexing (TDMA) scheduling algorithm for the clusters as well as data aggregation when suitable. This has resulted in many clustering algorithms adopting a cluster tree topology in order to support multi-hop communications. The overhead to maintain the clusters can be significant and this led the authors to investigate deeper the performance of collection tree topologies such as CTP in mobile environments.

CTP has been shown to be a very efficient data collection protocol for applications in static WSNs [4, 5]. However, wireless sensors are often used in mobile environments as well. Examples include Vehicular Ad hoc Networks VANETs, wild life monitoring, body area networks, and pollution monitoring. In such applications, sensors are usually deployed on mobile objects such as vehicles, animals or humans.

Even though CTP was designed for static scenarios, it exhibits both pro-active and reactive behaviours to compensate for the dynamic changes in the quality of the wireless communication links between the sensor nodes. However, when used in a mobile scenario we observe more frequent topology changes and hence more frequent re-calculations of the ideal path to the sink [6]. This inspired the creation of the Fixed-Node Assisted-CTP (FNA-CTP) [7] with the goal of modifying CTP to reduce the overhead and still maintain a comparable Packet Receive Ratio (PRR) as that achieved in mobile CTP.

The basis of FNA-CTP is based on two simple premises: Every deployment of the WSN has a few fixed sensor nodes distributed in the network region and these fixed nodes are leveraged by the network when a node loses its connection to a parent node by connecting first to the a fixed node prior to a nearby mobile node.

Some extended simulation analysis of FNA-CTP [8] showed that the an equivalent PRR value can be achieved with FNA-CTP as compared to standard CTP with the same number of static nodes but with substantially less overhead (about 85% beacon messages), less packet re-transmissions (about 78%), and less parent changes (about 79%.) The PRR values are nearly equivalent because CTP leverages packet re-transmissions therefore the reduced overhead would result in less power consumption and delays in the data.

In order to further validate the better performance of FNA-CTP to CTP in mobile environments an actual set of experiments were performed by leveraging actual sensor nodes in a large open field. The results were surprising as the scenarios showed that CTP in fact performed better than FNA-CTP. This chapter details these experiments and challenges faced in the implementation of the experiments and analysis of data captured.

This chapter is organized on the following manner. In Sect. 2 related work papers are reviewed particular to those works that manage a tree topology for mobile sensor nodes. Section 3 presents an overview of the FNA-CTP routing algorithm. Section 4

gives a description of the experimental setup and procedures utilized. Section 5 focuses on the data collection methodology and cleansing that was required in order to process the network data. Section 6 presents the analysis of the network data as Packet Reception Ratio (PRR), number of beacons, and number of parent changes and compares these to the simulation results. Section 7 offers some general observations of the data and issues encountered during the experimentations. Finally Sect. 8 concludes the chapter and offers some insight into future work.

2 Related Work

A significant amount of work has occurred in hierarchical topologies for mobile wireless sensor networks with a good recent survey presented by Sabor et al. [9]. In that paper they stress the overhead and computational time required to maintain a distributed clustering algorithm. In our work we are primarily interested on flat tree-based topologies rather than clustering approaches. Even so those clustering algortihms that support the formation of tree topologies among the cluster heads (typically referred to as cluster tree topologies) are closely related as the tree-based algortihms used to route data from the cluster heads to the sink are akin to a flat topology.

Many cluster-based topology papers focus on the formation of the clusters and adopt a periodic re-evaluation of the clusters and cluster heads in order to deal with the loss of connectivity from the cluster heads to the sink and as such few of them change the overlay tree based on link quality. Connectivity of the overlay tree among the cluster heads is a significant concern.

In this section we review a number of works that support flat tree-based network topologies like CTP and FNA-CTP and support wireless sensor networks.

In the work by Cakici, et al. [10] a Mobility Adaptive Cross-layer Routing (MACRO) algorithm was designed specifically for the MWSNs. Similar to CTP, the MACRO algorithm exhibits reactive and pro-active behaviours. The route discovery process is performed in a manner similar to reactive routing algorithms and the established routes are kept in adaptive-term routing tables as in proactive routing. Route quality metrics are maintained related to the nodes' mobility and speed as well as the physical RSSI values. It also periodically broadcasts beacons on an adaptive interval based on node speed as well as quality of links among the nodes determined through data transfers. This is similar to the trickle algorithm in CTP but containing mobility information. MACRO provides significant improvements on the packet delivery ratio and end-to-end packet delay performances compared to those of the classical AODV MANET protocol [11], CBR-Mobile [12] and LEACH-Mobile [13] routing protocols. We also compared the packet delivery ratio of CTP and FNA-CTP to AODV [7] and our PDR values for FNA-CTP as close to that of MACRO and better than CTP.

A Cluster Independent Data collection Tree (CIDT) was designed by Velmani et al. [14] based on the construction of a Data Collection Tree (DCT) that collects data from cluster heads. The DCT discovers an optimal path between the cluster head and the

sink based on the distance, connection time, threshold value, and residual energy. In CIDT the clusters and collection tree are kept separate but have a symbiotic relationship through particular nodes in the DCT known as Data Collection Nodes (DCN) that are used to collect the data from the cluster head and send it to the sink. The simulation results showed that the CIDT algorithm provides more stable links, high throughput, and good packet delivery ratio as compared to LEACH-Mobile [13].

An extension of the CIDT algorithm [15] known as the Velocity Energy-Efficient and Link-Aware Cluster Tree Protocol (VELCT) improved on the construction and maintenance of the DCT in CIDT by taking into account the location and motion of the cluster head nodes with the DCN. This combination of relatively stable cluster heads and DCNs results in a collection tree that is relatively stable comparted to the other sensor nodes. What is not well explained on both CIDT and VELCT is the need for a secondary collection tree rather than choosing the cluster heads as collection tree nodes. Both these algorithms take advantage of data aggregation which is not the case for FNA-CTP.

A novel multi-hop routing protocol for the MWSNs, called Proactive Highly Ambulatory Sensor Routing (PHASeR) was developed by Hayes et al. [16] that leverages a global TDMA-MAC layer to maintain a gradient metric from the sensor nodes to the sink. This method of using a fixed time slot assignment creates a collision free global TDMA MAC layer, which does not require any dynamic scheduling. PHASeR is similar to gradient-based flooding mechanisms that do not require any particular network topology but take advantage of the neighbor of the sensor nodes as well as distance to the sink to reduce network traffic. Because it uses TDMA and redundant paths the reliability of the network is fairly high. PHASeR was compared to several other mobile sensing algorithms and demonstrate slightly poorer results than MACRO but better than OLSR [17] and AODV [11] though the latter two are not collection algorithms so tend to exhibit more overhead in order to maintain two way communication in mobile networking scenarios.

Most tree-based routing algorithms presented for mobile sensor networks take advantage of the nodes positions and relative velocities among the nodes such as the simple approach demonstrated by Singh et al. [18] that creates a tree-based routing algorithm using spatial positioning of the nodes and Kusy et al. [19] and Lee et al. [20] that leverage prediction of mobile nodes to improve routing efficiency. All these approaches require spatial knowledge of the nodes of which FNA-CTP does not leverage.

Particular to modifications or comparisons to CTP, Li et al. [21] modified a collection tree protocol to take advantage of the spatial correlation of a sensor node to efficiently build and update the data collection tree. They performed a set of experiments on actual sensor nodes demonstrating that their approach could reduce updates required throughout the network. They show their work reduces the time to acquire data compared to CTP as the tree only updates the area that has been affected by the mobile node. Their approach does not address a large number of mobile nodes.

Jambli et al. [22] conducted a performance study for a mobile WSN executing the CTP routing protocol, they concluded that mobility caused a decrease in the data delivery ratio and an increase in the Energy consumption which we also validated in

our work [6] however, the authors didn't go into further details on the effects of mobility on the network and the routing protocol.

In Chen and Yu [23], the authors proposed a new architecture for better handling of mobility in wireless sensor networks. They proposed a hierarchical network architecture including a low level sensing layer with mobile sensor nodes and a high level routing layer with fixed routing nodes. The nodes in the sensing layer are mobile and they transmit their sensed data to the static routing nodes in the routing layer which are located at a one hop distance from them. The static routing nodes then further process and forward the data to the sink. This approach is closer to the FNA-CTP approach in that FNA-CTP also leverages fixed nodes with the difference that FNA-CTP does not enforce the use of the fixed nodes.

This idea of having a mix of static and mobile nodes has been used before in a number of applications, in particular in Vehicular Ad-hoc Networks [24]. However, in those applications, static nodes are primarily used as gateway/cluster heads, to collect data from mobile nodes within their range. Such arrangement requires static super nodes that can support a continuously high volume of traffic and corresponding bandwidth. Instead, FNA-CTP uses static nodes that simply act as backup parent nodes.

Very few of the related work have performed experiments with actual sensor nodes for the exception of the work by Li et al. [21]. The main reasons for that is the effort it takes to do so and the challenge in replicating the simulation results. In this chapter the focus is on the experimental analysis of FNA-CTP as compared to previously published simulation results.

3 Overview of Fixed Node Assisted-CTP (FNA-CTP)

In this section an overview of the FNA-CTP algorithm is presented along with a summary of performance measures based on simulations. These results have been recently published [8] and reproduced in this section.

The basic idea of FNA-CTP is to leverage a number of fixed nodes in the network to act as backups, when the links between the mobile nodes are disconnected. These static nodes may be used as a primary parent if their Expected Transmission value (ETX) value is less than other neighbours. However, in special cases they become a temporary parent when the node's parent becomes disconnected. The emphasis is on using the static nodes as backups and not as cluster heads. We are not forcing the nodes to forward their data to the static nodes. These static nodes typically do not have to handle more traffic, except when parts of the network become disconnected.

The ETX algorithm to determine the best path to the sink is a very simple algorithm consisting of basically calculating a sensor nodes neighbour ETX values and calculating a path to the sink with the smallest ETX value. The ETX values are periodically updated using both routing beacon and the unicast data packets. The CTP implementation uses adaptive beaconing based on a trickle algorithm [25] that basically reduces the beaconing rate when link quality is stable. In mobile sensor node scenarios the value of the trickle algorithm diminishes as the link qualities between the moving

sensors can quickly change. We have experimented with the beacon interval time and have implemented it in the static nodes in FNA-CTP.

The basic behaviour in FNA-CTP is rather simple: every deployment of WSN has a few fixed sensor nodes distributed in the network region. The location of fixed wireless sensor nodes is roughly evenly distributed based on their transmission range to cover the entire network region or area of interest. All other mobile source nodes in the network will be in the transmission range of at least one of the fixed nodes.

The tree routing used in CTP remains the same except that now every mobile node will have at least one fixed node ETX entry in its link estimation neighbour table and routing table in which the fixed node will be identified by a special flag bit. After each unicast data transmission, if the source node does not receive an acknowledgement after reaching the maximum number of retransmissions, the packet will be forwarded to the fixed static node rather than triggering the transmission of routing beacons and recalculation of the tree.

Figure 1 shows a typical FNA-CTP simulation set up where the circles represent fixed nodes and the diamonds mobile nodes. The top center node is the sink. This particular node layout is one showing 9 fixed nodes arranged in an equally distributed rectangular pattern grid.

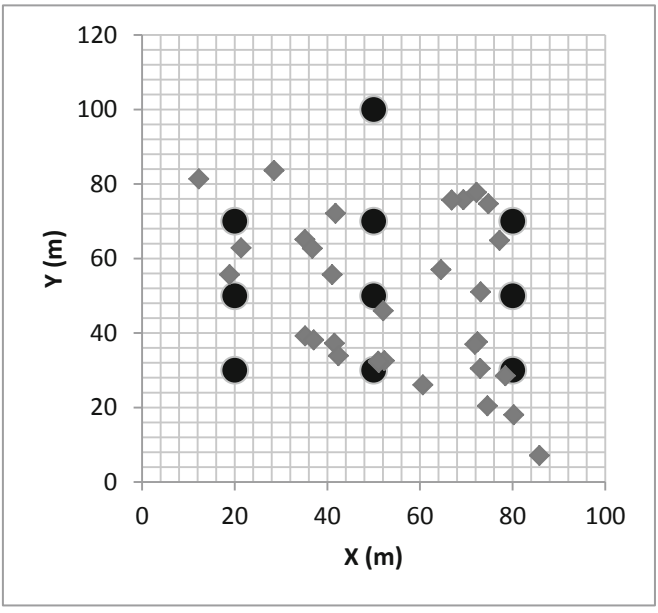


Fig. 1. A typical nine-node FNA-CTP simulation field layout. The fixed nodes are shown as black circles with the top node being designated as the sink node. The mobile nodes are shown as diamond shapes.

A comprehensive set of simulations were performed on FNA-CTP [8] varying the total number of nodes from 45 to 108 as well as varying the ratio of fixed/total number of nodes. Different node ranges and speeds were also tested. The best results were found to correspond to a 9 fixed node pattern as shown in Fig. 1. In summary the results showed that FNA-CTP matched the packet delivery ratio of CTP that contain the same number of fixed to mobile node ratio but utilizing less routing beacons (about 85%), less packet re-transmissions (about 78%), and less parent changes (about 79%).

4 Implementation Experimental Set up

Field evaluation of FNA-CTP was carried out in an indoor field using a set of IRIS Crossbow sensor networks [26] running the TinyOS operating system [27]. The CTP collection algorithm is available with the TinyOS environment while the FNA-CTP had to be converted from the original "C" language implementation of FNA-CTP developed for the Castalia simulation environment [28], into the NesC code supported by the TinyOS environment. Fortunately the CTP implementation in Castalia [29], of which FNA-CTP is based on, is a replication of the CTP available in the TinyOS environment. Even so the porting of this code took approximately one year to port with the help of 2 undergraduate students.

Replicating the simulation field size was a challenge in that it is not possible to effectively limit the transmission range of the IRIS radios so as to achieve a smaller range than the size of the field. In the simulations it was easy to specify node transmission ranges from 25 to 45 m. With the real nodes the lowest range was still beyond 50 m. so the density ratios used in the simulation experiments could not be reproduced. The density of the mobile nodes in the field ranged from 5 to 14 nodes in an area of about 930 m^2 (30.5 m $\times$ 30.5 m) while in the simulation environment the number of mobile nodes varied from 33 to 78 in a 22,500 m^2 (150 m $\times$ 150 m) area The field experiments are physically denser than the simulation and if the range of the radios is taken into account every radio is in range of each other in the field experiments. Even so, multi-hop communications was achieved in the field experiments due to the quality of the links. Also in the simulation experiments the fixed to mobile node ratio ranged from 0.27 to 0.67 while in the field experiments this value ranged from 0.071 to as high as 0.8.

The field size was approximately 30.5 m $\times$ 30.5 m and was configured as per Fig. 2. Node mobility was achieved by requesting for volunteer students to walk about the field holding a radio in the palm of their hand. All nodes transmitted data packets at 0.333 packets/s which was equivalent to the simulation experiments. The sink was located in the middle of the field and static nodes were located at the 4 compass directions at the edge of the field as noted in Fig. 2. There was also a sniffer node that actively capturing data packets throughout the experiments located in the south-west corner of the field. All the nodes were at about a height of 1 m off the ground.

A total of 14 volunteers holding one sensor node each participated in the experiment. Each one has a mobile node given to them in the switched off state and would turn the node on and off when instructed to do so. These 14 participants (nodes) were

split into three groups: a North Group (5 nodes), a West Group (5 nodes), and a South Group (4 nodes).

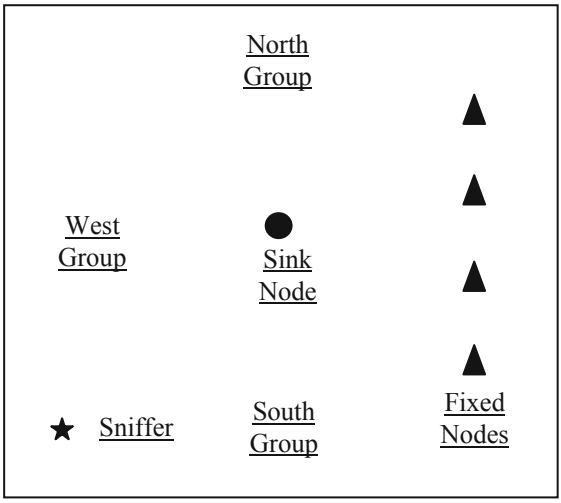


Fig. 2. Field experiment layout showing approximate location of the fixed and sink nodes and the start of the mobile nodes.

Prior to the experiments, each participant of the North and West groups were given a number between 1 and 5 and the South group participants each got a number between 1 and 4 since they had only four participants. This was done since the mobility pattern required one member of each group to activate their node and commence walking about the field. Approximately 15 to 20 s later the second group of participants turned on their radios and joined the other ones in the field. This created a mobility model consisting of nodes moving at human walking speed (1.4 m/s) in random directions, appearing in groups of 3, 6, 9, 12, and 14 nodes. An effort was made to make certain the human subjects were not mingling and talking among themselves so as to minimize the tendency for human's to gather into groups. As location information was not required none was captured.

A total of five separate experiments were performed consisting of: (1) FNA-CTP with one fixed node; (2) FNA-CTP with two fixed nodes; (3) FNA-CTP with three fixed nodes; (4) FNA-CTP with four fixed nodes; and (5) CTP with no fixed nodes. The nodes were reset at the end of each of the experiments.

5 Data Collection

Data was collected from 2 sources, the root node and the sniffer node. From the root node it is possible to compute the Packet Reception Ratio (PPR) as each packet sent by each node is tagged with the sender's identification and sequence number. The packets

captured at the sniffer is analyzed using the Wireshark packet analyzer looking for beacon routing packets and parent changes.

For these experiments we had to develop our own Wireshark packet dissector for CTP as well as FNA-CTP messages. This requires a detailed understanding of the format of the CTP packet and its relation to the 802.15.4 protocol as CTP takes advantage of the 802.15.4 ACK messages in order to eliminate the need of a CTP ACK message. The dissector has the ability to dissect 802.15.4, TinyOS Active Messages (AM), and CTP event and beacon messages. Even though a relatively detailed description of the CTP packet is available it was quite challenging to decipher the AM message from the packets as it is not truly a protocol but simply 2 bytes sandwiched in between the IEEE 802.15.4 header and the CTP Frame. It was discovered that the original description of the CTP message in the literature was not correct. After careful analysis of the data is was discovered that the TinyOS I-Frame format was being used to identify the network.

Data acquired at the root node consisted of data events that had to be filtered and clustered. Because the mobile nodes were inserted at different time periods during the experiment it was necessary to cluster the event data packets received at the root into groups that represented a time period where there were a consistent number of mobile nodes transmitting data. This was also necessary because consistent performance of a sensor node cannot be guaranteed. It might not function properly or persons would forget to turn the node on. This led to the definition of event-message graphs that would help to define time periods of consistent data.

5.1 Data Cleansing

Data acquired from the sniffer had to be filtered in the following manner:

1. The destination field for any broadcasted beacons was changed to 255 as it is easier to detect numeric values using the parser that we developed.
2. The source field of a packet was modified so that all of its values would be in decimal format instead of hexa-decimal format.
3. For beacon messages:
   a. The Origin ID Field and CTP Sequence Number field were set to “N.A.”
4. For Event Messages:
   a. The Parent ID Field and Sequence Number field were set to “N.A.”
5. All messages with a bad FCS (frame checksum) were discarded
6. All messages with an invalid node ID for the Origin ID were also discarded

5.2 Event-Message Graphs

A scatter plot was made of the packet data captured for each experiment. The scatter plot had the event numbers on the x-axis (as a timeline), and the Origin node IDs on the y-axis. This way, it became easier to visually see which nodes turned on at which point in the experiment. Figure 3 is a sample scatter plot for the first FNA-CTP Experiment. It shows the origin node ID for a packet received at a particular event time. Five of these graphs were created, one for each experiment.

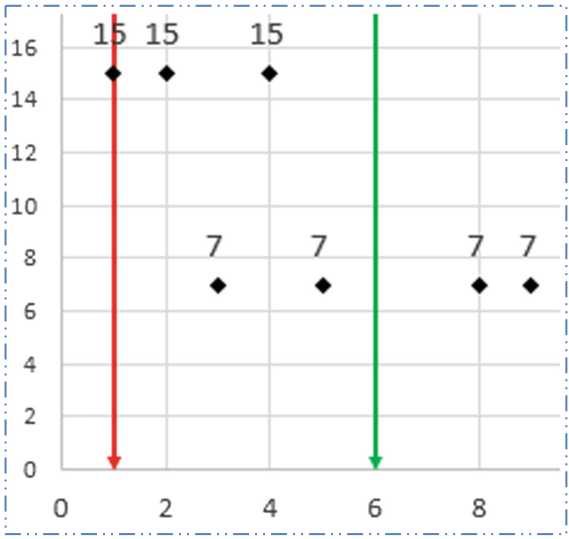


Fig. 3. An example of the data packet events labeled with the node IDs and a segment defined from event 1 to 6.

It was now possible to parse through the event-message graphs and divide the data into meaningful segments that indicate the regions at which the number of actively-transmitting nodes would not change.

Typically, the segments were expected to follow a similar structure to what was followed in the experiment. For example, the FNA-CTP experiments were expected to begin with events from fixed nodes that were transmitting before the participants were asked to turn on their nodes and move into the field. Following that, 3 mobile nodes would turn on. This would be repeated four times with the last two nodes introduced as the last group. Such a pattern was being sought out in the groupings and it is not a simple thing to detect given the irregularities in the data. In order to automate this process the following rules were applied based on visually studying the data. The aim of this grouping was to achieve the largest grouping segment as possible so as to have more events within each group. Note that we are looking for instances where 3 nodes appear in the data so references to 1^{st}, 2^{nd}, 3^{rd}, and 4^{th} in the rules refers to a sequence of data packet events from 4 different nodes.

R-1. If the number of events that occurred between the 2nd and 3rd node's first message is greater than the number of events between the 3rd and 4th node, then the group in question only consists of the 1st and the 2nd node, and the 3rd and 4th node fall in the next group.

R-2. If the number of events that occurred between the 2nd and 3rd node's first message is less than the number of events between the 3rd and 4th node, then the group in question only consists of the 1st, 2nd and 3rd node, while 3^{rd} and 4th node fall in the next group.

5.3 Observations Concerning the Data Segmentation

Once the data was filtered it was observed that particular nodes failed or were not turned on during the experiments. The first major observation is that not all the fixed nodes in experiment #3 functioned properly. This can be observed because the stationary nodes also generate data so if they are not observed by the sniffer then there was some malfunction of the device. For this reason only observations from experiments 1, 2, and 4 are analyzed.

Some nodes had to be replaced during the experiments and hence their node ID only appears in some of the experiments. This is not an issue with the segmentation algorithm that we developed.

Synchronization between the data captured by the root node and that by the sniffer is a concern because the events are not correlated. When the data captured by the root is analyzed different segments are extracted. This is not an issue for our analysis as the data analysis we perform does not simultaneously analyze data from both the sniffer and the root. The root is used to analyze the PRR values while the sniffer was used for beacon counts and parent changes.

6 Data Analysis

6.1 Packet Reception Ratio

Figure 4 is the Packet Reception Ratio (PPR) for the different field experiments for increasing number of mobile nodes. The results for FNA-CTP 3 representing three fixed nodes are not reported as the data showed that the fixed nodes were not functioning properly. The number of mobile nodes for each segment would vary slightly among the experiments so that results are reported based on the node density (number of nodes per m^2).

Trends for scalability cannot be accurately determined as these experiments are on relatively small networks with a maximum number of 18 nodes including the fixed nodes. Even so one can see some trends in the PRR plots such as the fact that the CTP experiment was much better than the FNA-CTP experiments. This observation is counter to that observed in the simulation results where the PRR value was roughly equivalent for both CTP and FNA-CTP.

One also can see a slight trend that seems to imply that as the number of fixed nodes increases the PRR values decrease. This is not conclusive since the PRR values for FNA-CTP 2 are lower than those for FNA-CTP 4. This is also contrary to the simulation results that clearly showed a higher PRR value as the number of fixed nodes increases as witnessed from Fig. 5 that shows the PRR values of FNA-CTP in a simulated experiment for mobile node speed of 1 m/s and maximum node range of 45 m for different fixed node/total node ratios.

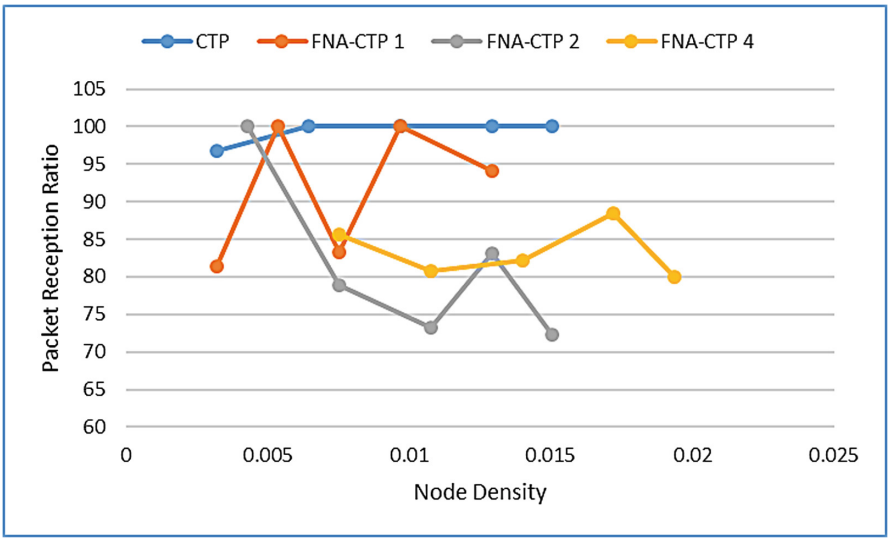


Fig. 4. Packet reception ratio vs. node density for the CTP, FNA-CTP 1, FNA-CTP 2, and FNA-CTP 4 field experiments.

Also for some unexplained reason there is an increase in PRR value in the 4th segment and then drops in the 5th segment when 2 more mobile nodes were added. This is consistent across all 3 FNA-CTP experiments but cannot be explained.

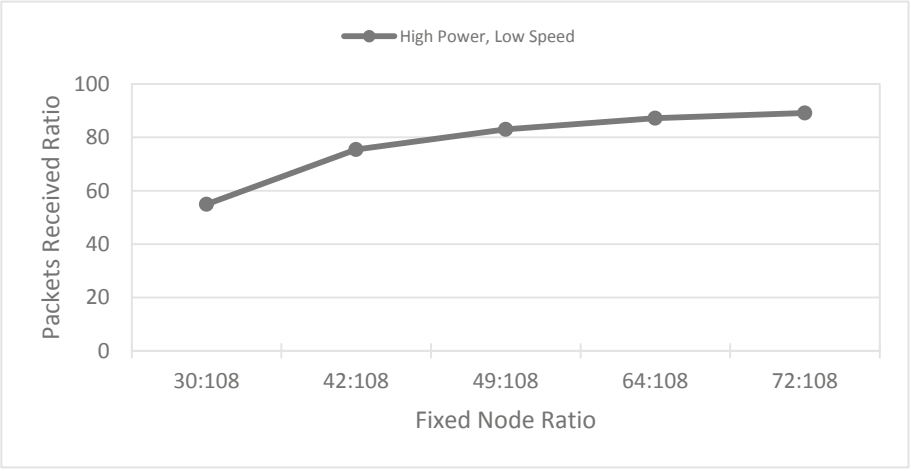


Fig. 5. Packet reception ratio for the simulated experiments for FNA-CTP for the slowest speed (1 m/s) and longest range (45 m) that closest resemble the field experiment parameters.

As previously mentioned the field experiments do not exactly replicate the simulation experiments but the parameters used to acquire the results for Fig. 5 are rather

similar. The total number of nodes for the simulation is 108 nodes in a 150 m^2 area for a node density of 0.0048 nodes/m^2. The density of the nodes for the field experiments vary from 0.004 to 0.02 nodes/m^2. The node speeds are 1 m/s which are comparable with the walking speed for humans at 1.2 m/s. Another similar metric is the node ranges of 45 m that is similar to the size of the field experiment. Another similarity is the highest fixed node ratio for the field experiments (4:18) is about equivalent to the lowest fixed node ratio (30:108) of the simulation experiments.

One clear difference between the simulation and field experiments is that the PRR value for the lowest fixed node ratio is about 55% while for the field experiments the lowest PRR values achieved were only about 71%. The simulation results are also much smoother than the field experiments that demonstrate fairly unstable PRR values as the number of mobile nodes changes.

6.2 Beacon Analysis

The beacons were captured through a sniffer and the number computed for each segment in an experiment as well as for the full length of the experiment. Because of the lack of a global clock and inconsistency in the duration of the experiments it is not accurate to compare the number of beacons sent between the experiments because of the lack of an equivalent execution time between the experiments (i.e. the longer the experiment executes for the more beacons that are sent.) The best that can be done is to compare the beacon changes within an experiment.

Figures 6 and 7 are graphs showing the number of beacons/node for different node densities for the mobile and the fixed nodes respectively. One can see some trends within each experiment in particular to the fixed nodes.

For the mobile nodes there aren't any significant trends with the number of beacons/node hovering between 6 to 20 for the exception of FNA-CTP 2 where the ratio is slightly higher than 20 at the start of the experiment.

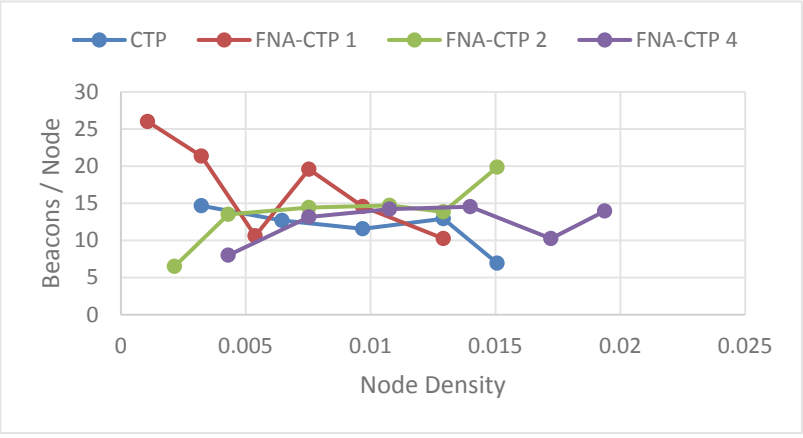


Fig. 6. Number of beacons per node for the different field experiments as related to node density.

For the fixed nodes there is a general trend downwards as the node density increases and a tapering to a steady state value. This more likely can be attributed to the improved connectivity in the network as the density increases (more mobile nodes enter in the network) and the fact that are the start of the experiment the fixed nodes are turned on prior to the mobile nodes and the fixed nodes are trying to create a path to the sink at this point and this period of time is usually a bit longer than the other time periods. If the first point is removed from experiments the beacons/node values range from 0 to 10. This is more realistic as the time between each segment is consistently about 15 s of data capture.

One way to normalize the beacons sent between the experiments is to calculate the ratio of beacons sent to data packets sent. This is not an accurate measure but since the data packet transmission rate is constant among all the nodes and the total number of nodes for all the experiments is approximately the same this metric can offer some comparative insight. These results are shown in Fig. 8.

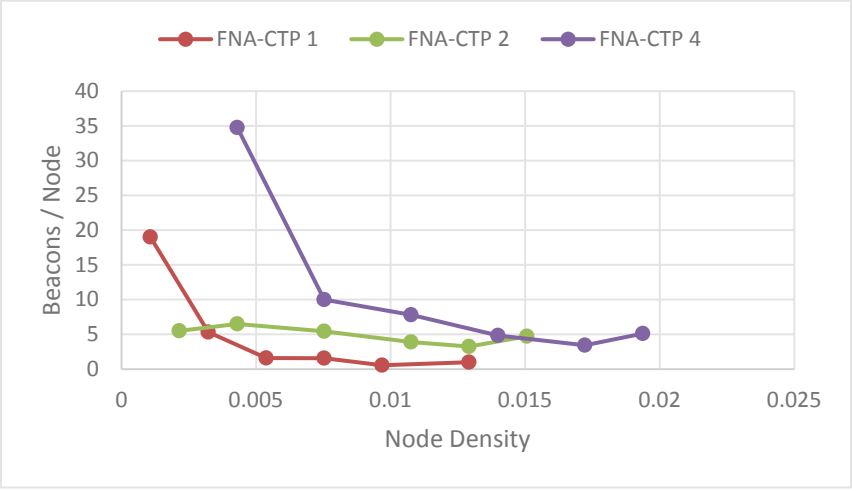


Fig. 7. Number of beacons/node for the fixed nodes as related to the node density. The CTP experiment is not included as it does not include any fixed nodes.

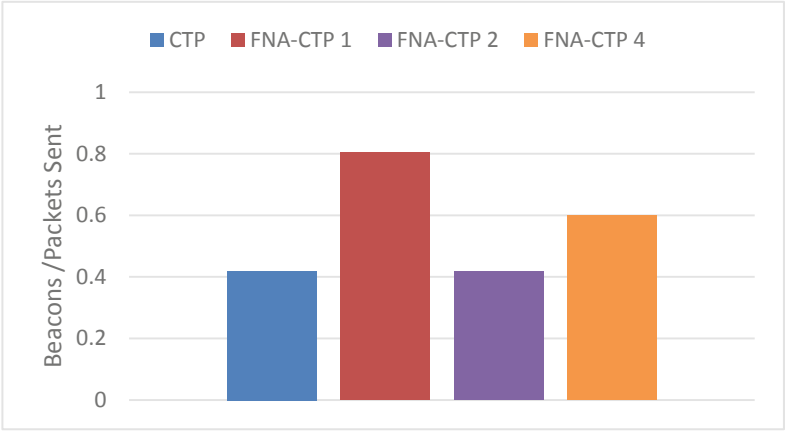


Fig. 8. Number of beacons/data packet for the different field experiments.

One can see from these results that the beacon per data packet ratio is lower for the CTP and FNA-CTP 2 experiments compared to FNA-CTP 1 and FNA-CTP 4 experiments. Again there is no trend or noticeable gain in the FNA-CTP algorithm over CTP. This is rather disappointing as the goal of using FNA-CTP is to reduce the number of beacons in the network compared to CTP but unfortunately the field experiments do not show that this was the case.

We attribute this to the location chosen for the fixed nodes. Referring back to Fig. 2 all the fixed nodes were placed at the East end of the field rather than distributed evenly across the field as in the simulation experiment shown in Fig. 1. Unfortunately this hypothesis was not validated as replicating the field experiments using other locations for the fixed nodes requires substantial volunteer effort. The conjecture is that the human bodies (mobile nodes) would act as barriers between the fixed nodes and the sink causing the mobile node links to be a better alternate route to the sink and later those nodes would move out or range of the fixed nodes. Since FNA-CTP is leveraging these fixed nodes as preferential parents this would also have an effect on the PRR values.

6.3 Parent Changes

Another metric that should replicate the beaconing metric is the number of parent node changes for the different experiments. This metric also suffers from the fact that it would need to be normalized as in the case of the beacon node count. It is though worth analyzing the parent change data.

Figure 9 is a graph of the total number of parent changes for the experiments for the fixed and mobile nodes. When comparing within each experiment it is interesting to note the relatively increase in the ratio of the fixed node parent changes to mobile nodes. This is not surprising as the number of fixed nodes increased from 1 to 4 but what is interesting is that the proportion increased in a non-linear trend. Again this can

be deceptive because these values take into account the first segment when the fixed nodes are turned on but there are no mobile nodes introduced into the network.

Figure 10 is the normalize number of parent changes based on the number of data packets sent in the network. The trend is similar to that shown in Fig. 8 as would be expected. For both these metrics it is not clear why the values for FNA-CTP 1 are much higher than the other experiments. Again the results for CTP are better than that for FNA-CTP.

7 General Observations

In this section we will present a number of general challenges and observations of the field experiments as well as the results compared to the simulations.

One of the most significant observations is that the CTP algorithm outperformed the FNA-CTP algorithm in the field experiments while this was not the case for the simulation experiments. This of course was not expected and we can only speculate that it primarily occurred because of two factors: (1) all the nodes in the field were in range of each other increasing the probability that the mobile nodes had reliable one hop connections to the sink node and (2) the location of the fixed nodes have a significant effect on the performance of FNA-CTP and should have been more evenly distributed across the field.

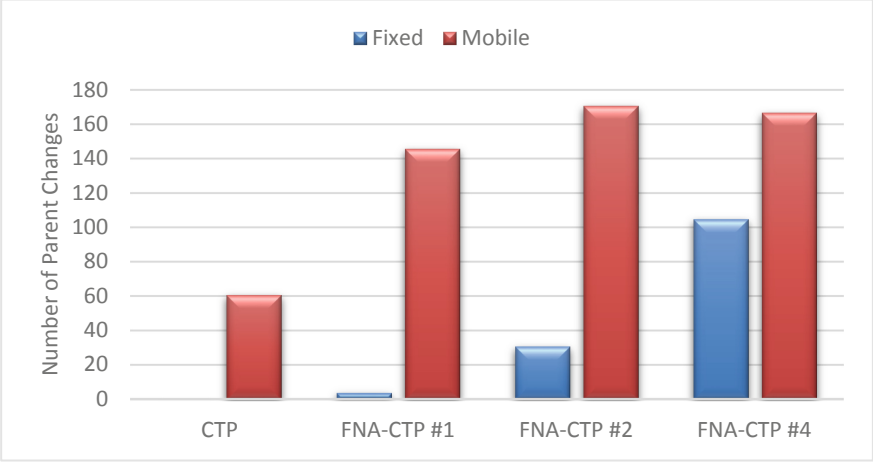


Fig. 9. Total number of parent changes for the field experiments for both fixed and mobile nodes.

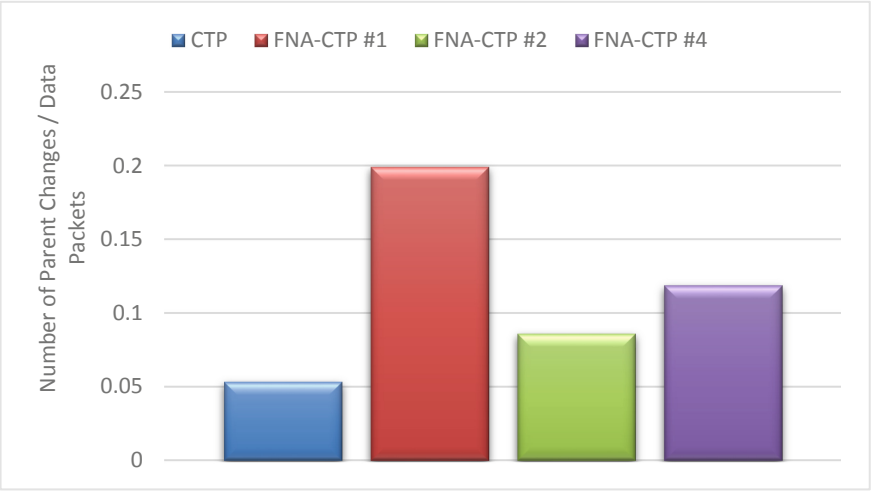


Fig. 10. Number of parent changes as related to data packets sent in the network.

Concerning observations related to the difference in the field and simulation experiments several key challenges should be noted.

1. It is very simple to specify sensor node range values in a simulated environment but rather challenging for real nodes. Because the simulation experiments were not originally designed to replicate an actual field experiment it is challenging to replicate the simulation environment in the field.
2. The lack of a globally synchronized clock made it more challenging to compare results between experiments as determining an equivalent experimental time period is not simple when only data events are captured. Because the sensor nodes transmit data in equal time periods it is possible to use data packet counts as a measure of time. The challenge that was encountered is that not all the nodes consistently functioned for each time segment and nodes were turned on at different times making segmentation of the data more challenging.
3. Remote management of sensor nodes is challenging. In our case the turning off and on of the sensor nodes was performed by human subjects reacting to a verbal command as opposed to a request through the network. In retrospect it would have been much more reliable to create a sensor node data management program where the sensors could be remotely requested to turn on at known periods of time as opposed to verbal commands given to the volunteers.
4. The programming language of the Castalia network simulator is not the same as that used to program the nodes. There is no concentrated effort in the community to focus on the use of network emulators that support the actual code executing on the sensor nodes. In this manner one can guarantee that the code ported is the same between the simulation and field experiments.

5. Node mobility is very challenging. In our case we used human subjects but they can create obstructions in the signal that are not replicated in the simulation. It is also a challenge to scale the field experiment as one requires many volunteers.
6. Lack of good real-time data analysis tools. Because all the data was analyzed after the data was collected it is rather difficult to re-create an experiment. For example we visually tried to confirm that all the nodes were functioning but it would have been best to have an automated program do that for us. As such it would have been possible to quickly determine that the fixed nodes in the FNA-CTP experiment had mal-functioned.

8 Conclusions

This chapter presented analysis of the FNA-CTP algorithm executing on an actual set of sensor nodes deployed in an open field and compared these results to that captured form a similar simulated scenario. The most striking result of this analysis is that CTP outperformed FNA-CTP in the field experiments while all the simulation results showed the opposite.

Based on these experiments a set of general observations were reported most related to the challenges associate with replicating the simulation scenarios in a real environment. Since we took the classical approach of demonstrating the performance of FNA-CTP in a simulation environment prior to a field trial on an actual environment replicating the simulation environment and scenario was challenging.

It is understood that in the research community for wireless sensor networks there is still a lack of actual experimental analysis with researchers often opting for the flexibility that protocol simulators can offer. It has been the experience of the author that one has to be very aware of how simulators model the physical wireless transmission as well as the interference among the nodes. A very common misconception by students is that the simulator can mimic the physical transmission of bits which it cannot so the approach taken by the simulator to determine the bit loss is very important. It is very easy to get 100% transmission and receive rates if the physical parameters are not properly set of the interference model of the simulator is not properly configured. Achieving a model that resembles the actual environment is very challenging so simulation results have to be followed by actual experimental tests.

Simulators are used primarily to support physical scalability but their flexibility is not always easy to replicate. In the actual experiments it was challenging to reduce the transmission range of the actual sensors that is easily done in a simulator and therefore it was not possible to replicate the field size of the simulator unless the experiment was performed on a large open field. Very few wireless simulators available for academics can replicate an actual terrain.

Another aspect that is very challenging and experienced in this work is that the code used in a simulator can be different than that deployed in the real deployment. In this work we chose a simulator that contained code that was very similar to the actual CTP deployment used on the tinyOS environment. Even so, the physical layer had to be added back to the FNA-CTP code that was developed in Castalia and this took about

1 year of man power and significant amount of reverse engineering of code. The trend is to develop simulations independent of the actual deployment environment and then somehow expect a complete re-write of the algorithm into the deployed sensor node. The result is that the extra effort to deploy the actual routing algorithms onto a sensor node can discourage researchers from implementing their algorithms.

A promising integrated simulation/development environment is Cooja [30] that is both an emulator for the sensor nodes as well as a simulator. The down side is that the sensor nodes need to support the Contiki [31] operating system. Contiki also supports the 6LowPAN [32] protocol that is compatible with IPv6 protocol facilitating integration of the sensor network into an IP enabled network infrastructure. This aligns with the trend for sensor networks to be integrated and managed with the rest of the network.

For future work it would be of interest to implement the key concepts of FNA-CTP into the RPL [33] routing protocol as RPL is currently considered as the defacto routing protocol standard for IP-based sensor networks though from an energy conservation perspective it would have a challenge competing with protocols that implement TDMA communications among the nodes. For this reason we are looking closer at clustering algorithms and cluster tree algorithms and integrating these with a software defined network overlay.

References

1. Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.): FTNCT 2018. CCIS, vol. 958. Springer, Singapore (2019)
2. Gnawali, O., Fonseca, R., Jamieson, K., Mass, D., Levis, P.: Collection tree protocol. In: 7th ACM Conference on Embedded Networked Sensor System, pp. 1–14 (2009)
3. Lotf, J.J., Hosseinzadeh, M., Alguliev, R.M.: Hierarchical routing in wireless sensor networks: a survey. In: 2nd International Conference in Computer Engineering and Technology (ICCET), vol. 3, pp. 650–654 (2010)
4. Gnawali, O., Fonseca, R., Jamieson, K., Kazandjieva, M., Moss, D., Levis, P.: CTP: an efficient, robust, and reliable collection tree protocol for wireless sensor networks. ACM Trans. Sens. Netw. (TOSN) **10**(1), 16 (2013)
5. Barcelo, M., Correa, A., Lopez Vicario, J.: Joint routing and transmission power control for collection tree protocol in WSN. In: IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 1989–1993 (2013)
6. Ottman, N.B., Liscano, R., Heydari, S.S.: An analysis of the collection tree protocol (CTP) in mobile sensing environments. In: IEEE 28th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 1–7 (2017)
7. Sharma, D., Liscano, R., Shah Heydari, S.: Enhancing collection tree protocol for mobile wireless sensor networks. Procedia Comput. Sci. **21**, 416–423 (2013)
8. Liscano, R., Ottman, N.B., Heydari, S.S., Sharma, D.: Fixed node assisted collection tree protocol for mobile wireless sensor networks. Int. J. Sens. Netw. **31**(3), 133–144 (2019). Under publication
9. Sabor, N., Sasaki, S., Abo-Zahhad, M., Ahmed, S.M.: A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: review, taxonomy, and future directions. Wireless Commun. Mob. Comput. **2017**(2818542), 23 (2017)

10. Cakici, S., Erturk, I., Atmaca, S., Karahan, A.: A novel crosslayer routing protocol for increasing packet transfer reliability in mobile sensor networks. Wirel. Pers. Commun. **77**(3), 2235–2254 (2014)
11. Perkins, C.E., Bhagwat, P.: Ad hoc on-demand distance vector (AODV) routing. IETF RFC 3561 (2003)
12. Awwad, S.A.B., Ng, C.K., Noordin, N.K., Rasid, M.F.A.: Cluster based routing protocol for mobile nodes in wireless sensor network. Wirel. Pers. Commun. **61**(2), 251–281 (2011)
13. Kim, D., Chung, Y.-J.: Self-organization routing protocol supporting mobile nodes for wireless sensor network. In: Computational Sciences, pp. 622–626 (2006)
14. Velmani, R., Kaarthick, B.: An energy efficient data gathering in dense mobile wireless sensor networks. ISRN Sens. Netw. **2014**(518268), 10 (2014)
15. Velmani, R., Kaarthick, B.: An efficient cluster-tree based data collection scheme for large mobile wireless sensor networks. IEEE Sens. J. **15**(4), 2377–2390 (2015)
16. Hayes, T., Ali, F.H.: Proactive Highly Ambulatory Sensor Routing (PHASeR) protocol for mobile wireless sensor networks. Pervasive Mob. Comput. **21**, 47–61 (2015)
17. Clausen, T., Jacquet, P.: Optimized Link State Routing Protocol (OLSR), IETF RFC3626 (2003)
18. Singh, M., Sethi, M., Lal, N., Poonia, S.: A tree based routing protocol for mobile sensor networks. IJCSE Int. J. Comput. Sci. Eng. **2**(01S), 55–60 (2010)
19. Kusy, B., Lee, H., Wicke, M., Milosavljevic, N., Guibas, L.: Predictive QoS routing to mobile sinks in wireless sensor networks. In: Proceedings of ACM International Conference Information Processing in Sensor Networks (IPSN), pp. 109–120 (2009)
20. Lee, H., Wicke, M., Kusy, B., Gnawali, O., Guibas, L.: Data stashing: energy-efficient information delivery to mobile sinks through trajectory prediction. In: Proceeding of ACM/IEEE 9th International Conference on Information Processing in Sensor Networks (IPSN), pp. 291–302 (2010)
21. Li, Z., Liu, Y., Li, M., Wang, J., Cao, Z.: Exploiting ubiquitous data collection for mobile users in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **24**(2), 312–326 (2013)
22. Jambli, M.N., Azlina, A.J., Farha Anati, A.M., Lenando, H., Abdullah, J., Sinarwati, M.S.: Performance evaluation of CTP routing protocol for mobile wireless sensor network. In: IEEE Conference on Wireless Sensor (ICWISE), pp. 97–101 (2013)
23. Chen, X., Yu, P.: Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes. In: 3rd International Conference in Biomedical Engineering and Informatics (BMEI), pp. 2863–2867 (2010)
24. Ding, Y., Xiao, L.: SADV: static-node-assisted adaptive data dissemination in vehicular networks. IEEE Trans. Veh. Technol. **59**(5), 2445–2455 (2010)
25. Levis, P., Patel, N., Culler, D., Shenker, S. Trickle: a self-regulating algorithm for code propagation and maintenance in wireless sensor networks. In: 1st ACM/ Usenix Symposium on Networked Systems Design and Implementation (NSDI) (2004)
26. Crossbow IRIS Datasheet. http://www.nr2.ufpr.br/adc/documentos/iris_datasheet.pdf. Accessed 29 Aug 2019
27. Levis, P.: TinyOS/nesC Programming Reference Manual. Crossbow Inc., January 2006
28. Castalia: A Simulator for Wireless Sensor Networks. https://github.com/boulis/Castalia. Accessed 15 July 2019
29. Santini, S., Colesanti, U.: A performance evaluation of the collection tree protocol based on its implementation for the castalia wireless sensor networks simulator. Department of Computer Science ETH Technical report (Nr 681) (2010)
30. Thomson, C., Romdhani, I., Al-Dubai, A., Qasem, M., Ghaleb, B., Wadhaj, I.: Cooja Simulator Manual. Edinburgh Napier University, Edinburgh (2016)

31. Dunkels, A., Gronvall, B., Voigt, T.: Contiki-a lightweight and flexible operating system for tiny networked sensors. In: The 29th annual IEEE International Conference on Local Computer Networks, pp. 455–462 (2004)
32. Mulligan, G.: The 6LoWPAN architecture. In: Proceedings of the 4th Workshop on Embedded Networked Sensors, pp. 78–82 (2007)
33. Tsiftes, N., Eriksson, J., Dunkels, A.: Low-power wireless IPv6 routing with ContikiRPL. In: The 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN) (2010)

Energy Conservation and Management in WSN

An Effective Analysis and Performance Investigation of Energy Heterogeneity in Wireless Sensor Networks

Samayveer Singh[1(✉)], Rajeev Kumar[2], and Pradeep Kumar Singh[3]

[1] Department of Computer Science and Engineering,
Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India
samayveersingh@gmail.com
[2] Department of Computer Science and Engineering,
Netaji Subhas Institute of Technology, Dwarka, New Delhi, India
rajeevgargnsit@gmail.com
[3] Department of Computer Science and Engineering,
Jaypee University of Information Technology,
Waknaghat, HP, India
pradeep_84cs@yahoo.com

Abstract. A wireless sensor network (WSN) helps in monitoring and controlling the physical world especially useful in a situation where human contribution may be too unsafe. Prolonging the network lifetime is the furthermost significant concern in WSNs due to the availability of the very limited battery for processing and computation in the sensor nodes. A lot of research work has finished by considering various heterogeneous network models with optimization procedures for the cluster head (CH) election. In this chapter, an effective analysis and performance investigation of various models of energy heterogeneity in WSNs are discussed. This chapter discusses the different types of resources heterogeneity and network models by deliberate the energy heterogeneity i.e., 2-level, 3-level, 4-level, 5-level, and multilevel heterogeneous models. The 2-level, 3-level, 4-level, 5-level, and multilevel heterogeneous network models can designate 2-level, 3-level, 4-level, 5-level heterogeneity, and designate up to any finite level heterogeneity, respectively. The empirical investigations of LEACH, SEP, DEEC, HEED, and PEGASIS are carried out with 1-level, 2-level, and 3-level of heterogeneity in this work. Here, benefits of the heterogeneous models over the homogeneous models are also discussed. The simulation and their comparative analysis of the protocols are completed by considering the different standard performance metrics such as define stability period in terms of network lifetime, throughput, residual energy of the network's, and dead nodes per rounds. These protocols can be performing a vital role in collecting information from harsh environment conditions like i.e., water and air pollutions, early detection of volcanic, forest fire detection, etc.

Keywords: Network lifetime · Energy efficiency · Wireless sensor networks · Clustering · Heterogeneity in nodes

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 157–194, 2020.
https://doi.org/10.1007/978-3-030-40305-8_9

1 Introduction

Now a day, one of the major advancements in the revolutionary growth of wireless sensing technology technologies is wireless sensor networks. The wireless sensor networks (WSNs) are the network that connects various battery-operated nodes called sensors. The wireless sensor networks own dissimilar appearances such as aptitude to endure by node failures, energy consumption constraints in node, node deployment scalability, consists of both homogeneity/heterogeneity nodes, cross-layer design, work in harsh environmental conditions, and ease use [1]. Generally, sensor nodes in WSNs are consist of trivial size, stumpy complex, and have very little power volume which is deployed in the observing filed for gathering data or recording of targets [2]. After sensing the data these sensor nodes forwarded the gathered data to the next hop and next-hop send collected data further to the next hop. This process continues until data reached to the base station (BS) means data can be forwarded directly to the BS or it can be forwarded with the help of other sensor nodes. Commonly, BS is accomplished to deliver reliability and execution obligatory processes. Then, the information processes to the fixed server by the BS using defined communication channel. WSNs deliver various prospects in the numerous monitoring filed for gathering data such as industrial control, agricultural monitoring, military applications, home automation, environmental and civil, etc. [1, 2]. The broad categorization of WSNs is given as follows which is based on the different applications namely deterministic and non-deterministic placement of nodes. In the first scenarios, nodes are deployed in manually or physically. The various application is as follows: city sense, soil, and nursery monitoring systems etc. Whereas in the second case sensor nodes are deployed randomly with the help of some external sources such as aircraft. The various non-deterministic applications are landslide detection, battlefield surveillance etc. It is also entitled random deployment.

It is limited by the sensor power restraints due to the enormous potential and its day by day exploration. A large number of researchers are working on the efficient utilization of the sensor nodes for increasing the lifetime of the sensor nodes. For solving such problems, general question is *how energy of the network can be increased? or how lifetime of the network can be increased*. Both questions are interrelated to each other. There are two possible ways to increase the lifetime of the WSNs. The first one is the increment in the network energy by adding the additional devices in the observing filed. This increases the cost approximately ten times more than the cost of the batteries of the networks. Another way is to increase the energy of some of the existing sensors. However, adding some of the existing nodes of high energy is the more suitable and inexpensive solution. Such types of networks termed heterogeneous WSNs [2]. However, questions are how many and what types sensor nodes are deployed for proficient exploitation of the network vitality. These questions are justified by the different heterogeneous models which exist in the literature.

In this chapter, an effective analysis and performance investigation of various models of energy heterogeneity in WSNs are discussed. This chapter discusses the different types of resources heterogeneity and network models by deliberate the energy heterogeneity i.e., 2-level, 3-Level, 4-Level, 5-level, and multilevel heterogeneous

models. The 2-level, 3-Level, 4-Level, 5-level, and multilevel heterogeneous network models can describe 2-level, 3-level, 4-Level, 5-level heterogeneity, and designate up to any finite level heterogeneity, respectively. The empirical investigations of LEACH, SEP, DEEC, HEED, and PEGASIS is carried out with 1-, 2-, and 3-level of heterogeneity. Here, benefits of the heterogeneous models over the homogeneous models are also discussed.

The rest of the chapter organized as follows: Sect. 2 deliberates why heterogeneity required in WSNs and different types of resource heterogeneity are discussed in Sect. 3. Section 4 explains the different heterogeneous energy models like 2-level, 3-level, 4-level, 5-level, and multilevel heterogeneity. Section 5 discusses the radio energy dissipation model and quality of services measures are discussed in Sect. 6. A brief discussion on some communication protocols is given in Sect. 7 and their performance analysis by considering different heterogeneity models are discussed in Sect. 8. Section 9 discusses the various advantages of heterogeneous networks over homogeneous networks. The summary of the discussed work is specified in Sect. 10 and upcoming scope is discussed in Sect. 11.

2 Why Heterogeneity

The longevity of the network is the furthermost problem in WSNs that are unswervingly inclined by the network's power. Generally speaking, a network has more energy than the network will observe an area for a long span and the network has less energy than this network's lifetime will be lower. There are therefore two methods to boost network energy to boost the network lifetime. First, by adding the number of nodes in the surveillance region, network battery can be upgraded. First, by adding the number of sensors in the surveillance region, network battery can be improved. Growing the amount of nodes increases the network battery, but the price is quite high because the deployment of an additional sensor entails the sensor's price, which is ten times higher than the battery price. Another way is to boost some of the current sensors' energy. Therefore, increasing the lifetime of the network by positioning some nodes with elevated energy is more suitable and cost-effective. Sensor networks with such features are called heterogeneous WSNs, i.e. nodes with distinct battery levels. However, issues are how many and what kinds of heterogeneous resources are to be deployed for effective use of network energy in the surveillance region.

3 Type of Resource Heterogeneity

The WSNs have focused over the past few years on machinery established for homogeneous WSNs where entire sensors of the networks have identical system properties. Recently, more and more popular are heterogeneous wireless sensor networks.

Research shows that heterogeneous nodes can increase the network lifespan and enhance network consistency without raising the price considerably. Whereas the heterogeneous sensors are more proficient in clarifying, fusing, and transporting data;

however, heterogeneous sensor nodes are additional exclusive than the homogeneous nodes. A heterogeneous node may consist of one or more heterogeneous resource types, e.g. enriched ability for energy or announcement. They can be organized with more dominant microchip or more memory or both compared to normal nodes. They may also use high-bandwidth and extensive distance networks to transfer with the BS. In a sensor node there are majorly three types of resource heterogeneities that include the heterogeneity of computation, connection, and energy [3–5].

3.1 Computational Heterogeneity

It refers to the node's distinct computational ability. Some nodes, for example, may have an additional dominant microprocessor and others may have additional memory.

3.2 Link Heterogeneity

The heterogeneity of the link refers to the capacity distinction between the links. Some links, for e.g., sensor nodes may have a large bandwidth and others may provide transceiving capability for extensive distance networks.

3.3 Energy Heterogeneity

The energy heterogeneity of the sensor nodes discusses to dissimilar energy stages. The energy heterogeneity of the sensors refers to different energy levels. For example, in comparison with other nodes, some nodes may have more energy. The heterogeneities of computation and connection are implicitly dependent on the heterogeneity of energy as the nodes with heterogeneities of computation and connection dissipate additional energy. Thus, the heterogeneity based on energy can be measured in WSNs as the furthermost dominant heterogeneity.

In the absence of heterogeneity, the heterogeneities of computation and connection will have a negative impact on the entire network, which can principal to the initial shutdown of the entire system. It prolongs the residual energy of the networks; thus the network lifespan will be increased.

4 Network Energy Models of Heterogeneity

There is a sprinkling of research works that consider the WSN model of heterogeneity to escalation the network lifetime. The papers [6–8] addressed heterogeneity at two levels, and the journals [9–17] introduced heterogeneity at three levels. Four-level heterogeneity was discussed in [18, 19]. Multilevel heterogeneity is also introduced in [6], but it has hardly any meaning since the nodes are assigned to the randomly generated energy levels. In other words, all sensors have distinct concentrations of energy, which can hardly be designed. Few new multilevel models are discussed in [21–23] that can define any heterogeneity. Below is a comprehensive description of the different types of heterogeneous models.

4.1 Two-Level Heterogeneity

The stable election protocol (SEP) is proposed by Smaragdakis et al. which is a LEACH extension by introducing heterogeneity [6]. It deliberates 2-levels of heterogeneity, comprising of two sensors types, known as normal and forward sensors. Let N be the number of sensors in a surveillance region. Assume E_0 is a normal sensor that contains initial energy, and m is the advanced node fraction that has α times more energy than a normal sensor. Then $m * N$ advanced sensors are fitted with $E_0 * (1 + \alpha)$, original power, and $(1 - m) * N$ are ordinary sensors. Thus, the network energy increases, then the lifetime of the network will increase correspondingly. The consider 2-level heterogeneous network total energy [6–8], are signified as E_{total}, is provided by

$$E_{total} = N * E_0 * (1 + \alpha * m) \tag{1}$$

A factor of 1 + αm increases network energy. Every advanced node becomes exactly (1 + α) times a CH.

4.2 Three-Level Heterogeneity

Mao et al. deliberate for heterogeneous WSNs a real data collection algorithm (EDGA) [9]. It deliberates three types of heterogeneity by presenting three types of nodes namely: normal, advanced, and supernodes. In these scenarios, an advanced node's having more energy than a normal node and a super node's having more energy than that of an advanced node. The total energy denoted by E_{total}, for the 3-level heterogeneous model is given as follows [13].

$$E_{total} = N * E_0 * (1 + m * (\alpha * (1 - m_0) + m_0 * \beta)) \tag{2}$$

where, m as advanced nodes and m_0 as supernodes as advanced nodes, and E_0 is initial energy of a normal node's. The advanced and super sensor energies are α and β times greater than that of a normal sensor, respectively. $E_0 * (1 + \beta)$ and $E_0 * (1 + \alpha)$, correspondingly, are the energies of each super and advanced sensor. By considering 3-level heterogeneity [10], Kumar et al. deliberate heterogeneous clustered schemes for WSNs. A lot of works are existing which are based on energy efficiency for increasing the lifetime of the heterogeneous networks [9–17, 29–34].

4.3 Four-Level Heterogeneity

Qureshi et al. discuss the balanced energy-efficient network-integrated super heterogeneous (BEENISH) protocol which deliberating a network of four levels of heterogeneity. It is consisting of four types of sensors namely: ultra-super, super, advanced and normal nodes [18]. The total energy is given by E_{total} for the 4-level heterogeneous network model [18] is given by

$$E_{total} = N * E_0 * (1 + m * (\alpha + m_0(-\alpha + \beta + m_1(-\beta + \mu)))) \tag{3}$$

where m is fraction of N as advanced sensors, m_0 is segment of advanced sensors as super sensors, and m_1 is fraction of super sensors as ultra-super sensors. As initial energy, a normal sensor has E_0. The advanced sensors, supernode sensors, and ultra-super sensors energies are respectively α, β, and μ times greater than the normal sensors.

Thus, the energies of respectively ultra super, super, and advanced sensors are $E_0 * (1 + \mu)$, $E_0 * (1 + \beta)$ and $E_0 * (1 + \alpha)$ correspondingly. Paper [19] also presented four levels of heterogeneity that consist of four types of sensors: ultra-super, super, advanced, and normal nodes.

4.4 Five-Level Heterogeneity

In literature, most of the existing [6–19] models consider heterogeneity at either two or three levels. We are discussing the five-level model of heterogeneity in this subsection [20]. The model is sufficiently general to describe the heterogeneity 0-, 1-, 2-, 3-, and 4-level contingent on the model constraint values. In this model, N is the number of nodes in the defined networks. N is the distribution of the nodes into dissimilar figures which depends on the level of heterogeneity. The total battery power of the network model is given as follows:

$$N * \left[E_0 * sin\left(\frac{i}{3}\right) + E_1 * sin\left(\frac{i}{4}\right) + E_2 * sin\left(\frac{i}{2}\right) + E_3 * sin(3i) + E_4 * sin(2i) \right] \quad (4)$$

Here, the type-0, type-1, type-2, type-3, and type-4 nodes are having original energies designate as E_0, E_1, E_2, E_3, and E_4, correspondingly where, 'i' is the model parameter which governs the different level network heterogeneity.

When we substitute $i = 8 * \pi$, in Eq. (4) then we get one non zero terms, i.e., $E_0 * sin\left(\frac{i}{3}\right)$. It is defined one level of heterogeneity of the networks i.e., homogeneous networks. This homogeneous network consists of N_0, is given by as follows:

$$N_0 = \frac{N * sin\left(\frac{i}{3}\right)}{sin\left(\frac{i}{4}\right) + sin\left(\frac{i}{3}\right) + sin\left(\frac{i}{2}\right) + sin(2i) + sin(3i)} \quad (5)$$

When we substitute $i = 2 * \pi$, in Eq. (4) then we get two non-zero terms, i.e., $E_0 * sin\left(\frac{i}{3}\right)$ and $E_1 * sin\left(\frac{i}{4}\right)$. It is defined two levels of heterogeneity of the networks i.e., 2-level heterogeneity networks. This heterogeneity network consists of N_0 and N_1 for the defined network. The value of N_0 is defined in (5) and N_1 are specified as follows:

$$N_1 = \frac{N * sin\left(\frac{i}{4}\right)}{sin\left(\frac{i}{4}\right) + sin\left(\frac{i}{3}\right) + sin\left(\frac{i}{2}\right) + sin(2i) + sin(3i)} \quad (6)$$

When we substitute $i = \pi$, in Eq. (4) then we get three non-zero terms, i.e., $E_0 * sin\left(\frac{i}{3}\right)$, $E_1 * sin\left(\frac{i}{4}\right)$, and $E_2 * sin\left(\frac{i}{2}\right)$. It is defined three levels of heterogeneity of the networks i.e., 3-level heterogeneity networks. This heterogeneity network consists of N_0, N_1, and

N_2 for the defined network. The value of N_0 and N_1, are defined in (5) and (6), respectively and N_2 are specified as follows

$$N_2 = \frac{N * sin\left(\frac{i}{2}\right)}{sin\left(\frac{i}{4}\right) + sin\left(\frac{i}{3}\right) + sin\left(\frac{i}{2}\right) + sin(2i) + sin(3i)} \tag{7}$$

When we substitute $i = 3 * \pi/2$, in Eq. (4) then we get four non-zero terms, i.e., $E_0 * sin\left(\frac{i}{3}\right)$, $E_1 * sin\left(\frac{i}{4}\right)$, $E_2 * sin\left(\frac{i}{2}\right)$, and $E_3 * sin(3i)$. It is defined four levels of heterogeneity of the networks i.e., 4-level heterogeneity networks. This heterogeneity network consists of N_0, N_1, N_2 and N_3 for the defined network. The value of N_0, N_1, and N_2 are defined in (5), (6) and (7), respectively and N_3 are specified as follows:

$$N_3 = \frac{N * sin(3i)}{sin\left(\frac{i}{4}\right) + sin\left(\frac{i}{3}\right) + sin\left(\frac{i}{2}\right) + sin(2i) + sin(3i)} \tag{8}$$

When we substitute $i = \pi/4$, in Eq. (4) then we get five non zero terms. It is defined five levels of heterogeneity of the networks i.e., 5-level heterogeneity networks. This heterogeneity network consists of N_0, N_1, N_2, N_3 and N_4 for the defined network. The value of N_0, N_1, N_2, and N_3 are defined in (5), (6), (7), and (8), respectively and N_4 are specified as follows

$$N_4 = \frac{N * sin(2i)}{sin\left(\frac{i}{4}\right) + sin\left(\frac{i}{3}\right) + sin\left(\frac{i}{2}\right) + sin(2i) + sin(3i)} \tag{9}$$

The entire network energy of network is given by

$$E_{total} = N * \left[E_0 * sin\left(\frac{i}{3}\right) + E_1 * sin\left(\frac{i}{4}\right) + E_2 * sin\left(\frac{i}{2}\right) + E_3 * sin(3i) + E_4 * sin(2i)\right] \tag{10}$$

The energies of various types of sensors are calculated by the following:

$$E_j = E_0 * (1 + j * \beta) \tag{11}$$

This relative merely expresses that the energy of a type j node is β periods additional then type $j - 1$ node, β is a constant. The energies must satisfy the inequalities $E_0 < E_1 < E_2 < E_3 < E_4$.

In this way, it exposed that the energy model in (10) can describe 0-, 1-, 2-, 3- and, 4-level heterogeneity in networks.

4.5 Multi-level Heterogeneity

Li et al. deliberate the protocol on distributed energy-efficient clustering (DEEC) [21] by deliberating heterogeneous WSNs at 2 and multi-level. The model of 2-level

heterogeneity is the same as described in [6]. In the multilevel heterogeneous model, the battery power of each sensor is distributed arbitrarily intervals are given as follows.

$$E_{total} = \sum_{i=1}^{N} E_0 * (1 + \alpha_i) = E_0 * \left(N + \sum_{i=1}^{N} \alpha_i\right) \tag{12}$$

In multilevel heterogeneity, the sensor node's energy is arbitrarily assigned energy interval $[E_0, E_0 * (1 + \alpha_{max})]$, where E_0 is subordinate certain of energy interval and α_{max} regulates higher bound of the energy limits. Initially, the i^{th} node is furnished with an initial energy of $E_0 * (1 + \alpha_i)$, which is α_i times more energy than the subordinate bound E_0 of the energy interval. This heterogeneous multilevel model is hardly useful because every node has dissimilar energy levels and it may not be practically feasible to design sensor nodes with large numbers of energy levels.

4.6 General Multilevel Heterogeneity

A multilevel network model that can describe the n level of heterogeneity is discussed in this subsection, n is a progressive number [22, 23]. In this model there is no random allocation of the energies of the nodes. Thus, the nodes and their respective energies of the nodes are completely independent. Let n be the node which is divided into n different types of sensors, i.e., type-1, type-2, type-3, …, type-n sensors, with their respective energies as E_1, E_2, E_3, … E_n. The value of n determines the secondary parameters used for defining the level of heterogeneity in the model. An inequalities $E_1 < E_2 < E_3 < \ldots < E_n$ for defining the energy levels must satisfy for different numbers of type-1, type-2, type-3, …, type-n nodes, symbolized as $N_1, N_2, N_3, \ldots N_n$, respectively, must satisfy the inequalities $N_1 < N_2 < N_3 < \ldots < N_n$. The following equation define the energies of different nodes which are linked as below:

$$E_j = E_1 * (1 + (j - 1) * \delta) \tag{13}$$

here, E_1 signifies the energy of a type-1 sensor and E_j, j = 1, 2, 3…n, signifies the energy of a j-type sensor. Thus, the energy of a j-type sensor is δ times more than that of a (j − 1)-type sensor. δ is a constant. The energy of the network is given by

$$\begin{aligned} E_{total} = N * ((\alpha - \beta_1) * E_1 + (\alpha - \beta_1) * (\alpha - \beta_2) * E_2 + (\alpha - \beta_1) * (\alpha - \beta_2) \\ *(\alpha - \beta_3) * E_3 + \ldots + (\alpha - \beta_1) * (\alpha - \beta_2) * (\alpha - \beta_3) * \ldots\ldots * (\alpha - \beta_n) * E_n) \end{aligned} \tag{14}$$

The primary restriction is perfect (3) is α which decides the network heterogeneity level and it is associated with β_i, i = 1, 2, …, n as given by:

$$((\alpha - \beta_1) * (1 + (\alpha - \beta_2) * (1 + (\alpha - \beta_3) * \ldots\ldots * (1 + (\alpha - \beta_{n-1}))))) = 1 \tag{15}$$

$$(\alpha - \beta_i) < 1 \tag{16}$$

The values of $\beta_i s$ are related by the following:

$$\beta_i = \beta_{i-1} - 2 * \Phi \tag{17}$$

Φ is constant for a given heterogeneity level which is defined as follows:

$$\frac{\beta_1}{2(n-1)} > \Phi \tag{18}$$

Equation (14) defines $(i - 1)$ non-zero terms where α is allocated the value of β_i, $(i > 1)$, i.e., $\alpha = \beta_i$. It defines $(i - 1)$ the type of nodes and $(i - 1)$ level of heterogeneity. When we put $i = 1$, in (14) then we get zero terms and it is the progressive case. It does not specify any level of heterogeneity.

When we put $\alpha = \beta_2$, in Eq. (14) it generates one-level heterogeneity. It is called a homogenous network. The total energy is given by, (from (14)),

$$E_{1\text{-}level} = N * (\alpha - \beta_1) * \mathrm{E}_1 \tag{19}$$

N_1 is the number of type-1 nodes in the network which is given as follows:

$$\mathrm{N}_1 = N * (\alpha - \beta_1)$$

Using (16), $(\alpha - \beta_1) = 1$ gives one level of nodes denoted as N_1 as N.

When we put $\alpha = \beta_3$, in Eq. (14) it generates two non-zero terms. It is called two-level heterogeneity. The total energy is given by, (from (14)),

$$E_{2\text{-}level} = N * ((\alpha - \beta_1) * E_1 + ((\alpha - \beta_1) * (\alpha - \beta_2) * \mathrm{E}_2)) \tag{20}$$

The number of nodes in the network of type-1 and type-2 is given, respectively, as follows:

$$N_1 = N * (\alpha - \beta_1)$$

$$N_2 = N * ((\alpha - \beta_1) * (\alpha - \beta_2))$$

and the associated condition (from (16)) is given by

$$(\alpha - \beta_1) + (\alpha - \beta_1) * (\alpha - \beta_2) = 1.$$

When we put $\alpha = \beta_4$, in Eq. (14) it generates three non-zero terms. It is called the three-level heterogeneity. The total energy is given by, (from (14)),

$$E_{3\text{-}level} = N * \left((\alpha - \beta_1) * E_1 + (\alpha - \beta_1) * (\alpha - \beta_2) * E_2 + \left(\begin{matrix} (\alpha - \beta_1) * (\alpha - \beta_2) * \\ (\alpha - \beta_3) \end{matrix} \right) * E_3 \right) \tag{21}$$

The number of nodes in the network of type-1, type-2, and type-3 is given, respectively, as follows:

$$N_1 = N * (\alpha - \beta_1)$$
$$N_2 = N * ((\alpha - \beta_1) * (\alpha - \beta_2))$$
$$N_3 = N * ((\alpha - \beta_1) * (\alpha - \beta_2) * (\alpha - \beta_3))$$

and the associated condition (from (16)) is given by

$$((\alpha - \beta_1) * (1 + (\alpha - \beta_2) * (1 + (\alpha - \beta_3)))) = 1$$

The value $\alpha = \beta_{i+1}$, defines the for i^{th} level of heterogeneity and also defines i non-zero terms in (14) and it defines i^{th} level of heterogeneity, whose entire power supply is specified by, (from (14)),

$$E_{i\text{-}level} = N * ((\alpha - \beta_1) * E_1 + (\alpha - \beta_1) * (\alpha - \beta_2) * E_2 + (\alpha - \beta_1) * (\alpha - \beta_2) * (\alpha - \beta_3) * E_3 + \ldots + (\alpha - \beta_1) * (\alpha - \beta_2) * (\alpha - \beta_3) * \ldots\ldots * (\alpha - \beta_i) * E_i) \tag{22}$$

The number of nodes in the network of type-1, type-2, …, i-type are assumed, correspondingly, as follows:

$$\left.\begin{array}{c} N_1 = N * (\alpha - \beta_1) \\ N_2 = N * ((\alpha - \beta_1) * (\alpha - \beta_2)) \\ N_3 = N * ((\alpha - \beta_1) * (\alpha - \beta_2) * (\alpha - \beta_3)) \\ \ldots \\ \ldots \\ \ldots \\ N_i = N * (\alpha - \beta_1) * (\alpha - \beta_2) * (\alpha - \beta_3) * \ldots\ldots * (\alpha - \beta_i) \end{array}\right\} \tag{23}$$

and the condition (from (16)) is given by

$$((\alpha - \beta_1) * (1 + (\alpha - \beta_2) * (1 + (\alpha - \beta_3) * \ldots\ldots * (1 + (\alpha - \beta_{i-1}))))) = 1$$

Thus, the (14) described the network model is a universal multilevel heterogeneous network model that can designate any level of heterogeneity.

5 Radio Energy Dissipation Model

This section discusses an energy dissipation radio model used to calculate data transmission and receiving energy consumption over a distance, data aggregation and other circuits [24–28]. Depending on the distance, the energy a sensor consumes when transmitting L-bit message.

The energy use in message communication can be changed by short and long distances and the energy absorbed can be noted as E_{TXS} and given as follows [24–28].

$$E_{TXS} = L * \in_{elec} + L * \in_{fs} * d^2 \qquad \text{if } d \leq d_0 \tag{24}$$

$$E_{TXL} = L * \in_{elec} + L * \in_{mp} * d^4 \qquad \text{if } d > d_0 \tag{25}$$

where $\in_{elec}$, $\in_{fs}$, $\in_{mp}$, d and d_0 are the energy consumed per bit by transmitter/receiver circuit, free-space transmitter amplifier, multi-path transmitter amplifier, the distance between transmitter and receiver, and threshold between sensor and BS. The maximum distance between sensor and BS is given as follows.

$$d_0 = \sqrt{\frac{\in_{fs}}{\in_{mp}}} \tag{26}$$

The energies consumed in receiving (E_{Rx}) and sensing (E_{Sx}) for L-bits data are given as follows.

$$E_{Rx} = E_{Sx} = L * \in_{elec} \tag{27}$$

The energy disbursed by a head node for transmitting L-bit message is given as follows.

$$E_{CH} = L * E_{elec} * \left(\frac{N}{k} - 1\right) + L * E_{DA} * \frac{N}{k} + L * E_{elec} + L * \in_{fs} * d_{toBS}^2 \tag{28}$$

where N, k, E_{DA} and d_{toBS} are no of nodes, no clusters, data accumulation cost in bits, and regular distance among a CH and BS.

The energy consumed by a sensor node for transmitting L-bit data is given as follows

$$E_{non-CH} = L * E_{elec} + L * \in_{fs} * d_{toCH}^2 \tag{29}$$

where d_{toCH} is the regular distance between a cluster member and its CH as defined as follows.

$$d_{toCH}^2 = \frac{M^2}{\sqrt{2\pi k}} \tag{30}$$

Thus, the entire battery power spent by the sensor in-network is given as follows:

$$E_{tot} = L * \left(2 * N * E_{elec} + N * E_{DA} + \left(k * d_{toBS}^2 + N * d_{toCH}^2\right) * \in_{fs}\right) \tag{31}$$

6 Quality of Service Measures

- **Network lifetime** - The time taken from the start of networks to the demise of the last alive nodes.
- **A number of alive nodes per round** - It instant measurement reproduces a total quantity of sensors and the quantity of each type that has not yet spent all their energies.
- **Data packet delivery** - It concerns the information packets communicated to the BS successfully. This is also a quantity of how many sensors of data are sending to BS.
- **Energy consumption** - It is a measure of the power of the battery dissipation a round promptly. It is a difference in battery from start to finish of a round.
- **Residual energy** - The residual energy defines as the ratio among the sums of residual energy of all sensors to a total number of available sensors in the networks.
- **Stability period** - The stability period of the networks is the number of rounds that are completed by any primary node type, i.e. normal, advanced, and supernodes without their energy being completely depleted.

7 A Brief Discussion on Some Communication Protocols

In this section, LEACH [24], SEP [6], DEEC [3, 21], HEED [35], and PEGASIS [36] protocols are briefly discussed as follows. First of all, we will discuss the Low energy adaptive clustering hierarchy (LEACH) protocol.

7.1 LEACH Protocol: Low-Energy Adaptive Clustering Hierarchy Protocol

The LEACH protocol is the very first to increase the lifespan of WSNs [24]. This protocol is established on the estimated probability, the CHs are nominated in LEACH and their rotations are randomized. In this process, each and every sensor node gets a chance to be a CH in each round and has a relatively balanced energy dissipation of each node.

However, it may not have CHs dispersing evenly throughout the region and it does not consider energy in selecting the heads of the cluster. In the next sections, we will discuss the CH selection process for 2- and 3-level heterogeneity of LEACH protocol.

7.1.1 Cluster Head Selection Method for 2 Level Heterogeneity of LEACH Protocol

Initially, N number of nodes are positioned in the surveillance area. These sensors are categories into different categories based on their initial energies. The preliminary battery power of a normal node is E_0. The fraction of the other type of sensor nodes (which are called advanced nodes) is m as compares to the normal nodes. Thus, $m * N$ sensor is equipped in the monitoring filed called advanced nodes. The initial energies of advanced are $E_0 * (1 + \alpha)$, and the remaining nodes are $(1 - m) * N$ set as normal

nodes. So, the energy of 2-level heterogeneous network signified by E_{total}, is specified by $E_{total} = N * E_0 * (1 + \alpha * m)$ [6–8]. The energy of the network has been enlarged by an element of $(1 + \alpha m)$ as it is multiple factors of $N * E_0$. Each normal node becomes a CH once in every $\frac{1}{p_{opt}} * (1 + \alpha m)$ rounds and each advanced node becomes a CH exactly $(1 + \alpha)$ times in every $\frac{1}{p_{opt}} * (1 + \alpha m)$ rounds. The average number of CHs per round is equal to $N * p_{opt}$. Thus, an advanced node becomes a CH $(1 + \alpha)$ times more than a normal node at the end of each round. The weighted probabilities of the normal and advanced nodes of becoming CH, denoted by p_{nrm} and p_{adv}, respectively, are given by

$$p_{nrm} = \frac{p_{opt}}{(1 + \alpha m)} \tag{32}$$

$$p_{adv} = \frac{p_{opt} * (1 + \alpha)}{(1 + \alpha m)} \tag{33}$$

The thresholds for a normal node $T_{s_{nrm}}$ and an advanced node $T_{s_{adv}}$, for becoming CHs, are given as follows

$$T_{s_{nrm}} = \begin{cases} \frac{p_{nrm}}{1 - p_{nrm} \cdot \left(r \bmod \frac{1}{p_{nrm}}\right)} & \text{if } s_{nrm} \in G' \\ 0 & \text{Otherwise} \end{cases} \tag{34}$$

$$T_{s_{adv}} = \begin{cases} \frac{p_{adv}}{1 - p_{adv} \cdot \left(r \bmod \frac{1}{p_{adv}}\right)} & \text{if } s_{adv} \in G'' \\ 0 & \text{Otherwise} \end{cases} \tag{35}$$

where, the set of normal and advanced nodes are denoted by G' and G'', that have not become CHs within last $\frac{1}{p_{nrm}}$ and $\frac{1}{p_{adv}}$ rounds (r), respectively.

7.1.2 Cluster Head Selection Method for 3 Level Heterogeneity of LEACH Protocol

The papers [9–17] has introduced a 3-level heterogeneity, by defining 3 kinds of sensors: super, advance, and normal nodes. A supernode has more than an advanced node, which has additional energy than a normal node. The total network energy for the 3-level heterogeneity, denoted by E_{total}, is given by

$$E_{total} = N * E_0 * (1 + m * (\alpha + m_0 * \beta)) \tag{36}$$

where E_0 is the preliminary battery power of a normal node, m is the fraction of N as advanced nodes and m_0 is the fraction of the advanced nodes as supernodes.

The energies of a super and an advanced node are $E_0 * (1 + \beta)$ and $E_0 * (1 + \alpha)$, respectively, where α & β are constants. It is to note that the network total energy given

by (36) is not correctly simplified. The correct formula for the entire battery of the network is as below:

$$E_{total} = N * E_0 * (1 + m * (\alpha * (1 - m_0) + m_0 * \beta)) \tag{37}$$

Using the 3-level heterogeneity, the total network energy increases by a factor of $(1 + m * (\alpha * (1 - m_0) + m_0 * \beta))$. The weighted probabilities of the normal, advanced, and supernodes, signified by p_{nrm}, p_{adv}, and p_{sup}, respectively, are given by

$$p_{nrm} = \frac{p_{opt}}{(1 + m * (\alpha * (1 - m_0) + m_0 * \beta))} \tag{38}$$

$$p_{adv} = \frac{p_{opt} * (1 + \alpha)}{(1 + m * (\alpha * (1 - m_0) + m_0 * \beta))} \tag{39}$$

$$p_{sup} = \frac{p_{opt} * (1 + \beta)}{(1 + m * (\alpha * (1 - m_0) + m_0 * \beta))} \tag{40}$$

The thresholds for normal, advanced, and supernodes, for becoming CHs, signified by $T_{s_{nrm}}$, $T_{s_{adv}}$ and $T_{s_{sup}}$, respectively, are given by

$$T_{s_{nrm}} = \begin{cases} \frac{p_{nrm}}{1 - p_{nrm} \cdot \left(r \bmod \frac{1}{p_{nrm}}\right)} & \text{if } s_{nrm} \in G' \\ 0 & \text{Otherwise} \end{cases} \tag{41}$$

$$T_{s_{adv}} = \begin{cases} \frac{p_{adv}}{1 - p_{adv} \cdot \left(r \bmod \frac{1}{p_{adv}}\right)} & \text{if } s_{adv} \in G'' \\ 0 & \text{Otherwise} \end{cases} \tag{42}$$

$$T_{s_{sup}} = \begin{cases} \frac{p_{sup}}{1 - p_{sup} \cdot \left(r \bmod \frac{1}{p_{sup}}\right)} & \text{if } s_{sup} \in G'' \\ 0 & \text{Otherwise} \end{cases} \tag{43}$$

where the set of normal, advanced, and super nodes are denoted as G', G'' and G''' that have not become CHs within last $1/p_{nrm}$, $1/p_{adv}$, and $1/p_{sup}$ rounds, respectively.

7.2 SEP: Stable Election Protocol

The hetSEP is the implementation of the SEP protocol by considering the heterogeneous network model. The hetSEP-1, hetSEP-2 and hetSEP-3 refer to SEP implementation for 1-level, 2-level [6–8] and 3-level heterogeneity [9–17], correspondingly. We discuss the CH election process in hetSEP-3 which requires that the defined

network comprising of three kinds of nodes, i.e., normal, advanced, and super nodes. The total initial energy of the heterogeneous network is (refer 44)

$$N * \left(\theta * E_0 + \theta^2 * E_1 + \left(1 - \theta - \theta^2\right) * E_2\right)$$

It can be written as

$$E_0 * N * \left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right) \tag{44}$$

If there were only one type nodes, the network energy would have been as $(E_0 * N)$. Thus, in this heterogeneous network model, the network energy increases by a factor of $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)$. In other worlds, there have been increase of $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)$ times more normal nodes. In LEACH protocol [24], all homogeneous nodes become CH precisely once in every $1/p_{opt}$ rounds, where p_{opt} is node optimal probability to convert a node into CH. The average number of CHs per round is equal to $N * p_{opt}$ which sustains the lowest energy consumption in each round. The heterogeneous network has $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)$ fold more energy, thus a node become CH exactly once in every $1/p_{opt} * \left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)$ rounds. It also helps in optimizes the stable region of the deployed network. Thus, the ordinary quantity of Cluster Heads per round is equal to $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right) * N * p_{nrm}$ because every sensor has preliminary energy equivalent to the normal node in this scenario. For all type of sensors different threshold values are set which are based on the initial energies of the different types of sensors calculated after $N * p_{opt}$.

Thus, each normal sensors becomes a CH once in every $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)/p_{opt}$ rounds, each advanced sensors turn into a CH $(1 + \alpha)$ times more than that of the normal sensors in every $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)/p_{opt}$ rounds, and each super sensor turn into a CH $(1 + \beta)$ times more than that of the normal sensors in every $\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)/p_{opt}$ rounds by incorporating heterogeneity in the defined networks. Thus, the constraint of $N * p_{opt}$ CHs per round is violated. This weight must be equal to the ratio of the initial energy of a designated sensor as CHs and the factor of the entire enlarged batter power in heterogeneous network. The initial energy of normal, advanced, and super nodes are $E_0, E_1,$ and E_2, respectively, and the factor of the entire enlarged batter power is $\theta * E_0 + \theta^2 * E_1 + \left(1 - \theta - \theta^2\right) * E_2$.

Thus, the weight of a node is given by $E_0/\theta * E_0 + \theta^2 * E_1 + \left(1 - \theta - \theta^2\right) * E_2$. The weighted probabilities of the normal, advanced, and super nodes in hetSEP-3, signified by p_{nrm}, p_{adv}, and p_{sup}, respectively, are given by

$$p_{nrm} = \frac{p_{opt} * E_0}{\left(\theta * E_0 + \theta^2 * E_1 + \left(1 - \theta - \theta^2\right) * E_2\right)} \tag{45}$$

$$p_{adv} = \frac{p_{opt} * E_0}{\left(\theta * E_0 + \theta^2 * E_1 + \left(1 - \theta - \theta^2\right) * E_2\right)} \tag{46}$$

$$p_{sup} = \frac{p_{opt} * E_0}{\left(\theta * E_0 + \theta^2 * E_1 + \left(1 - \theta - \theta^2\right) * E_2\right)} \tag{47}$$

They can be written as

$$p_{nrm} = \frac{p_{opt}}{\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)} \tag{48}$$

$$p_{adv} = \frac{p_{opt} * (1 + \alpha)}{\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)} \tag{49}$$

$$p_{sup} = \frac{p_{opt} * (1 + \beta)}{\left(\theta + \theta^2 * \frac{E_1}{E_0} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{E_0}\right)} \tag{50}$$

In this work, the same approach as discussed in LEACH protocol is measured for CH selection, the probability is computed as follows.

$$T(s) = \begin{cases} \frac{p_{opt}}{1 - p_{opt} \cdot \left(r \bmod \frac{1}{p_{opt}}\right)} & \text{if } s \in G \\ 0 & \text{Otherwise} \end{cases} \tag{51}$$

where p_{opt} is an initial % of CHs, and G is set of sensors that have not been CHs in last $1/p_{opt}$ rounds. Generally, the value of p_{opt} is put in (51) by the weighted probabilities p_{nrm}, p_{adv}, and p_{sup} to obtain the threshold for different type of nodes, correspondingly in directive to designate the CH in each round. We describe threshold $T_{s_{nrm}}$ for a normal node as given by

$$T_{s_{nrm}} = \begin{cases} \frac{p_{nrm}}{1 - p_{nrm} \cdot \left(r \bmod \frac{1}{p_{nrm}}\right)} & \text{if } s_{nrm} \in G' \\ 0 & \text{Otherwise} \end{cases} \tag{52}$$

where G' is set of normal nodes that have not become CHs within last $\frac{1}{p_{nrm}}$ rounds and $T_{s_{nrm}}$ is threshold applied to $(\theta * N)$ normal nodes.

This guarantees that individually normal node will turn into CH exactly once in every $\left(\theta+\theta^2*\frac{E_1}{E_0}+\left(1-\theta-\theta^2\right)*\frac{E_2}{E_0}\right)/p_{nrm}$ rounds and the average number of CHs which are normal nodes per round is identical to $(\theta*N)*p_{nrm}$. Correspondingly, the thresholds for advanced and super nodes are given by

$$T_{s_{adv}}=\begin{cases}\frac{p_{adv}}{1-p_{adv}.\left(r \bmod \frac{1}{p_{adv}}\right)} & \text{if } s_{adv}\in G'' \\ 0 & \text{Otherwise}\end{cases} \tag{53}$$

$$T_{s_{sup}}=\begin{cases}\frac{p_{sup}}{1-p_{sup}.\left(r \bmod \frac{1}{p_{sup}}\right)} & \text{if } s_{sup}\in G'' \\ 0 & \text{Otherwise}\end{cases} \tag{54}$$

So, probabilities and thresholds in CH selection are help in prolonging the lifespan of the proposed networks as defined in the above method.

7.3 DEEC Protocol: Distributed Energy-Efficient Clustering Protocol

The DEEC protocol is one of the significant protocol by considering the 3-level heterogeneous network model [9–17]. Now, the execution of the DEEC protocol is deliberated and the naming convention is concerned, we use the same as the SEP protocol used. The CH selection process for hetDEEC-3 is similar as the LEACH protocol [23, 24] by deliberates the average number of CHs as $N*p_{opt}$ in every round and each sensor becomes a CH once in every $r_i=\frac{1}{p_{opt}}$. rounds, and r_i is round in which i^{th} sensor is CH. The network average energy denoted as $\bar{E}(r)$ at round r is given as follows:

$$\bar{E}(r)=\frac{1}{N}\sum_{i=1}^{N}E_i(r) \tag{55}$$

where, $E_i(r)$ is remaining energy of i^{th} node in round r.

The i^{th} sensor average probability to become a CH during r^{th} round is given as follows

$$p_i=p_{opt}\left[1-\frac{\bar{E}(r)-E_i(r)}{\bar{E}(r)}\right]=p_{opt}*\frac{E_i(r)}{\bar{E}(r)} \tag{56}$$

The total number of CHs per round is given by

$$\sum_{i=1}^{N}p_i=\sum_{i=1}^{N}p_{opt}*\frac{E_i(r)}{\bar{E}(r)}=p_{opt}\sum_{i=1}^{N}\frac{E_i(r)}{\bar{E}(r)}=N*p_{opt} \tag{57}$$

The i^{th} node in r_i^{th} round is the CH defined as follows (using Eq. (56))

$$r_i = \frac{1}{p_i} = \frac{\bar{E}(r)}{p_{opt} * E_i(r)} = r_{opt} * \frac{\bar{E}(r)}{E_i(r)} \tag{58}$$

If there were only one type nodes, the network energy would have been as $(E_0 * N)$. Thus, in this heterogeneous network model, the network energy increases by a factor of $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)$. In other worlds, there have been increase of $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)$ times more normal nodes. In LEACH protocol [24], all homogeneous nodes become CH precisely once in every $1/p_{opt}$ rounds, where p_{opt} is node optimal probability to convert a node into CH. The average number of CHs per round is equal to $N * p_{opt}$ which sustains the lowest energy depletion in every round. The heterogeneous network has $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)$ fold more energy, thus a node become CH exactly once in every $1/p_{opt} * \left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)$ rounds. It also helps in optimizes the stable region of the deployed network. Thus, the average number of CHs per round is equal to $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right) * N * p_{nrm}$ because each node has initial energy equal to the normal node in this scenario. For all type of sensors different threshold values are set which are based on the initial energies of the different types of sensors calculated after $N * p_{opt}$. Thus, each normal node becomes a CH once in every $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)/p_{opt}$ rounds, each advanced node becomes a CH $(1 + \alpha)$ times more than that of the normal nodes in every $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)/p_{opt}$ rounds, and each supernode becomes a CH $(1 + \beta)$ times more than that of the normal sensors in every $\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right)/p_{opt}$ rounds by incorporating heterogeneity in the defined networks. Thus, the restriction of $N * p_{opt}$ CHs per round is despoiled. This weight must be equal to the ratio of the initial energy of a designated sensor as CHs and the factor of the entire distended energy in heterogeneous network. The initial energy of normal, advanced, and super nodes are E_0, E_1, and E_2, respectively, and the element of the total increased energy is $\theta * E_0 + \theta^2 * E_1 + (1 - \theta - \theta^2) * E_2$.

This method allocates weights to get optimum probability for each type of sensor. In the proposed heterogeneous model, we divide p_i as given in (56) by the factor of the total increased energy in proposed model for clustering. The weighted probabilities of the normal, advanced and super nodes for hetDEEC-3, denoted by p_{nrm}, p_{adv}, and p_{sup}, respectively, are given by

$$p_{nrm} = \frac{p_{opt} * E_i(r)}{\left(\theta + \theta^2 * \frac{E_1}{E_0} + (1 - \theta - \theta^2) * \frac{E_2}{E_0}\right) * \bar{E}(r)} \tag{59}$$

$$p_{adv} = \frac{\mathrm{p_{opt}}(1+\alpha) * \mathrm{E_i(r)}}{\left(\theta + \theta^2 * \frac{E_1}{\mathrm{E_0}} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{\mathrm{E_0}}\right) * \bar{\mathrm{E}}(\mathrm{r})} \tag{60}$$

$$p_{sup} = \frac{\mathrm{p_{opt}}(1+\beta) * \mathrm{E_i(r)}}{\left(\theta + \theta^2 * \frac{E_1}{\mathrm{E_0}} + \left(1 - \theta - \theta^2\right) * \frac{E_2}{\mathrm{E_0}}\right) * \overline{\mathrm{E}}(\mathrm{r})} \tag{61}$$

We substitute $\mathrm{p_{opt}}$ in (51) by the weighted election probabilities $\mathrm{p_{nrm}}$, p_{adv}, and p_{sup} to obtain the thresholds for different kinds of sensors, in order to designate the CHs in each round. The thresholds $\mathrm{T}(s_i)$ for different kinds of sensors are given by

$$\mathrm{T}(s_i) = \begin{cases} \frac{p_{nrm}}{1 - p_{nrm} * \left(\mathrm{r} \bmod \frac{1}{p_{nrm}}\right)} & \text{if } p_{nrm} \in \mathrm{G}' \\ \frac{p_{adv}}{1 - p_{adv} * \left(\mathrm{r} \bmod \frac{1}{p_{adv}}\right)} & \text{if } p_{adv} \in \mathrm{G}'' \\ \frac{p_{sup}}{1 - p_{sup} * \left(\mathrm{r} \bmod \frac{1}{p_{sup}}\right)} & \text{if } p_{sup} \in \mathrm{G}''' \\ 0 & \text{Otherwise} \end{cases} \tag{62}$$

where $\mathrm{G}', \mathrm{G}''$ and G''' are set of different kinds of sensors that have not become CHs within last $1/p_{nrm}$, $1/p_{adv}$, and $1/p_{sup}$ rounds, respectively. So, probabilities and thresholds in CH selection are help in prolonging the lifespan of the proposed networks as defined for hetDEEC-3.

7.4 HEED Protocol: Hybrid Energy Efficient Distributed Protocol

The HEED is very basic protocol which is initially deliberated for homogeneous networks. The implementation of HEED protocol is discussed by considering different kind of nodes for heterogeneous network model. Firstly, the CH determination process of the HEED protocol is discussed by opting two parameters namely residual energy as primary and intra-cluster communication as secondary parameters [35]. The primary parameter opts an initial set of CHs probabilistically and use the secondary parameter to discontinuity the tie between them. A tie takes place when a node reduction within the range of more than one head of the cluster. The range of the cluster is determined by the power level used during clustering for inter-cluster communication.

The % of CHs in HEED is initially predetermined which is defined as the probability of the CHs C_{prob} is only used to limit the initial CH. It sets the probability that a node will be produced as a CH which is given by the HEED protocol [35].

$$CH_{prob} = C_{prob} * \frac{E_{residual}}{E_{max}} \tag{63}$$

where E_{max} and $E_{residual}$ are maximum energies of the apprehensive node and residual, correspondingly.

The assessment of CH_{prob} is subordinate limited by the threshold p_{min}. In HEED, CHs not covered nodes double their likelihood of becoming a CHs. All the sensors to gathered data and send their respective CHs. The heads of the cluster send the data received to the BS. Multi-hop communication with data accumulation is used to gather data. $E_{residual}$ of the HEED protocol is replaced by the total preliminary battery of the 2-level and 3-level heterogeneous network is (refer 44) as $N^* E_0 * (1 + \alpha * m)$ and $N^*(\theta * E_0 + \theta^2 * E_1 + (1 - \theta - \theta^2) * E_2)$, respectively as discussed in Subsects. 7.1.1 and 7.1.2.

7.5 PEGASIS Protocol: Power Efficient Gathering in Sensor Information Systems

It was modified in the power-efficient collection of sensor information systems (PEGASIS) protocol, where only one sensor is elected as the head node that sends the fused data or information to the BS [36]. Each node communicates in this protocol only with a closest neighbor who communicates with his closest neighbor. This process goes on to the head node and finally to the BS. Thus, because of less transmission distance, it reduces the amount of energy spent. However, the energy level for CH selection is not considered and is not appropriate for outsized networks. Since there is only one head node, network causing delay may be bottleneck. The LEACH protocol CH selection method is similar to that discussed in Sects. 7.1.1 and 7.1.2, respectively, for 2 and 3 level heterogeneity.

8 Performance Analysis of Communication Protocols Using Different Heterogeneity Models

In this segment, the performance investigation of the various communication procedures such as LEACH [24], SEP [6], DEEC [3, 21], HEED [35], PEGASIS [36] by considering both network homogeneity and heterogeneity are discussed. All the variants of the communication protocols are simulated by deliberating three levels of heterogeneity that are 1-level heterogeneity in which all the sensors have same amount of battery, 2-level heterogeneity in which networks comprise of 2-type of sensors namely advanced & normal sensors, and 3-level heterogeneity in which networks consist of three type of sensors namely super, advanced & normal sensors. The performance of 1-level, 2-level, and 3-level heterogeneity are analyzed on the basis of network lifespan, per round alive nodes, data packet delivery, energy consumption, and residual energy. All the networks are simulated in MATLAB environment to estimate the enactment of the communication procedures and their variants. The 100 number of sensors are disseminated in the $100 \times 100\,m^2$ monitoring area with 0.5 J initial energy and BS is fixed in the middle of the deployed area. In two-level of heterogeneity, we considered 70 nodes as the normal and 30 nodes as the advanced nodes with their initial energies 0.414 J and 0.7 J, respectively. In three-level of heterogeneity, we considered 50 sensors as the normal sensors, 30 sensors as the advanced sensors and 20 sensors as the super sensors with their initial energies 0.40 J, 0.50 J, and 0.75 J, respectively.

The energy depletion to execute transmitter or receiver circuit ($\in_{elec}$), by amplifier to transmit signal at shorter distance ($\in_{fs}$), and by amplifier to transmit at longer distance ($\in_{mp}$) are 50 nJ/bit, 10 pJ/bit/m^2, and 0.0013 pJ/bit/m^4, respectively. The message size (L), threshold distance (d_0), and cluster radius (R) are 4000 bits, 75 m, and 25 m, respectively. For each experiment, we have taken 25 simulation using randomly sensor deployment and finally, average of that 25 simulations are considered as the outcome of the results. Figure 1 shows an instance of the deployment of sensor nodes and sink (in middle), cluster heads and their respective cluster members in different colors for 3-level of heterogeneity. The figure also indicates the normal nodes by circular (○) mark, advanced nodes by star (∗) mark, and super nodes by plus (+) mark. The BS is marked as (X) in the middle of the monitoring area. The clusters and their corresponding cluster members are indicating by the same color as shown in Fig. 1. In the next subsection, we will deliberate the reproduction results and their comparative performance investigation for various communication protocol namely LEACH, SEP, DEEC, HEED, and PEGASIS.

8.1 Performance Investigation for Homogeneous and Heterogeneous LEACH Protocol Variants

In this segment, the comparative analysis of homogeneous and heterogeneous LEACH protocol variants results is discussed.

Figure 2 illustrations the number of alive nodes in respect of number of rounds for MLLEACH-1, MLLEACH-2, and MLLEACH-3. The MLLEACH-1 is containing single type of nodes also called homogenous network and MLLEACH-2 & MLLEACH-3 is consisting of 2 & 3 types of nodes, respectively, also called as the

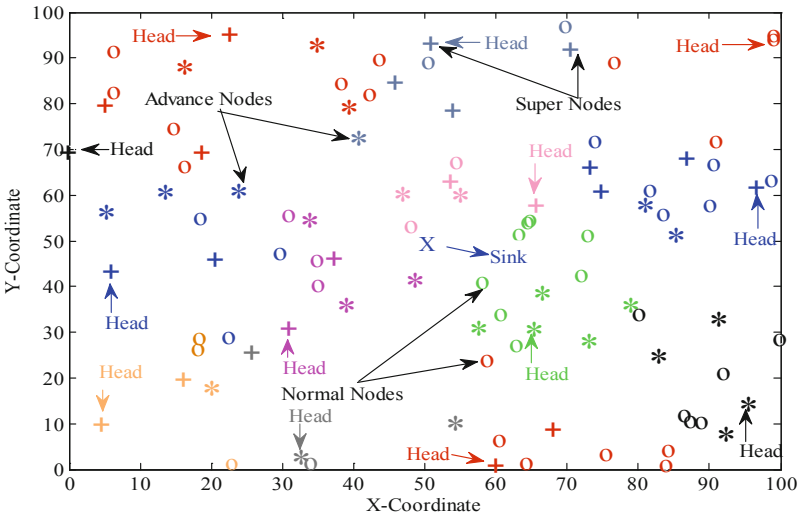


Fig. 1. Deployment of sensors and sink (or BS), cluster heads (CHs) and their respective cluster members in different colors

heterogeneous networks in nature. It is observed that MLLEACH-3 covers 2142 number of rounds whereas MLLEACH-2 and MLLEACH-1 cover 1597 and 1407 number of rounds, correspondingly, already depletes comprehensive energy of all the sensors. Thus, MLLEACH-2 and MLLEACH-3 increase 13.50%, and 52.24% in the network lifetime in respect of MLLEACH-1, respectively.

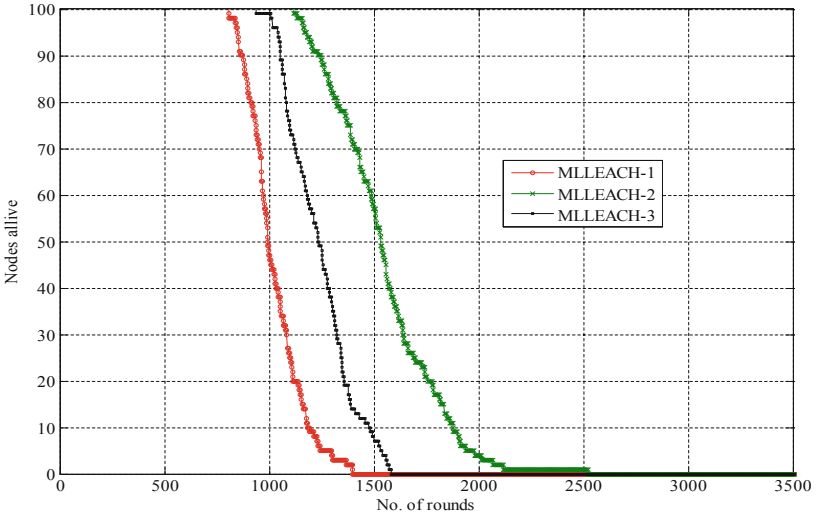


Fig. 2. Number of alive nodes with respect to round numbers for LEACH variants

The MLLEACH-3 helps in increment in the network lifetime because advanced energy sensors get additional chance to become a CH in each round. It is also reducing the dead rate of the nodes and helps in prolonging the lifespan of the network. The sustainable period of the network for MLLEACH-1, MLLEACH-2, and MLLEACH-3 are 807, 947, 1122 number of rounds, respectively. It is also manifest from the Fig. 2 the sustainable period of the MLLEACH-2 and MLLEACH-3 for first node dead significantly exceeds by 17.35%, and 39.03%, as comparison with the MLLEACH-1, respectively.

Figure 3 signifies the entire battery consumption in consecutive rounds for MLLEACH-1, MLLEACH-2, and MLLEACH-3. Initial total energy network is considered as 50 J. The battery consumption in MLLEACH-3 is very less for consecutive rounds as compare to the MLLEACH-1 and MLLEACH-2 because it selects higher energy nodes as a cluster head instead of random selection for all the rounds. It allocates the load uniformly amongst the sensors and CH. The results show the higher energy consumption in MLLEACH-1 because distribution of energy is same for all the nodes. Thus, it diminishes the computational battery cost of the head sensors in the networks as the level of heterogeneity prolongs in the networks.

The number of packets received by the BS in respect of the number of rounds till the networks alive for MLLEACH-1, MLLEACH-2, and MLLEACH-3 is shown the

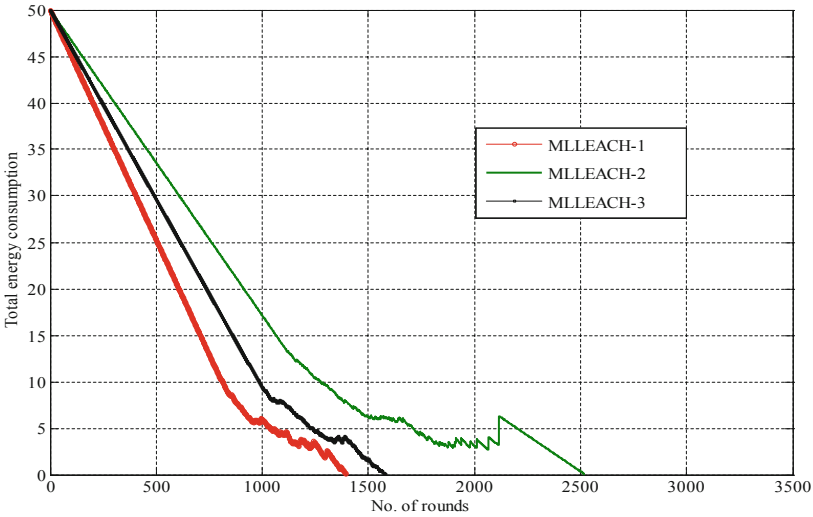


Fig. 3. Total energy consumption in the networks with respect to round numbers for LEACH variants

Fig. 4. A great number of packets are provided to the BS with the fact that as extensive as the network live. Thus, the number of packets directed by the MLLEACH-3, MLLEACH-2, and MLLEACH-1 to the BS are 1.71×10^{-4}, 1.31×10^{-4}, and 1.10×10^{-4}, in the consecutive rounds, respectively. It is observed that the MLLEACH-3 sent data packets at the higher rate to the base station as associated to

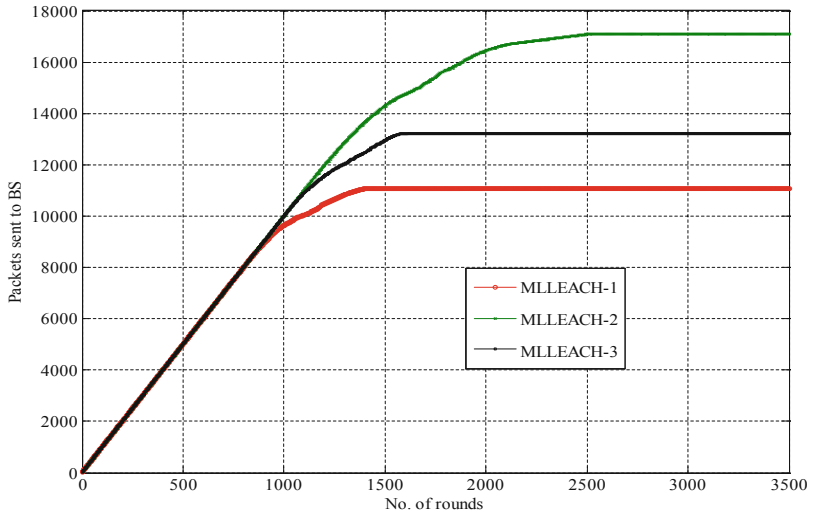


Fig. 4. Total number of packets sent to BS by the networks with respect to round numbers for LEACH variants

MLLEACH-1 and MLLEACH-2. However, the MLLEACH-3 produces highest number of packets because the nodes in MLLEACH-3 remain alive more in terms of number of rounds.

8.2 Performance Investigation for Homogeneous and Heterogeneous SEP Protocol Variants

In this segment, comparative analysis of simulation results for homogeneous and heterogeneous SEP protocol variants are shown in the Fig. 5. It is depicted the number of alive nodes in respect of number of rounds for MLSEP-1, MLSEP-2, and MLSEP-3. The MLSEP-1 is containing single type of nodes also called homogenous network and MLSEP-2 & MLSEP-3 is consisting of 2 & 3 types of nodes, respectively, also called as the heterogeneous networks in nature. It is evident that MLSEP-3 covers 2659 number of rounds whereas MLSEP-2 and MLSEP-1 cover 2157 and 1517 number of rounds, correspondingly, before exhausts comprehensive battery of all the nodes. Thus, MLSEP-2 and MLSEP-3 increase 42.19%, and 75.28% in the network lifetime in respect of MLSEP-1, respectively. The MLSEP-3 supports in increment in the network lifetime because advanced energy sensor get additional chance to become a CH in each round. It is also reducing the dead rate of the sensors and helps in prolonging the lifespan network. The sustainable period of the network for MLSEP-1, MLSEP-2, and MLSEP-3 are 752, 1001, 1333 number of rounds, respectively. It is manifest from the Fig. 5 the sustainable period of the MLSEP-2 and MLSEP-3 for first node dead significantly exceeds by 33.11%, and 77.26%, as comparison with the MLSEP-1, respectively.

Figure 6 signifies the total energy consumption in consecutive rounds for MLSEP-1, MLSEP-2, and MLSEP-3. Initial network battery is considered as 50 J. The energy

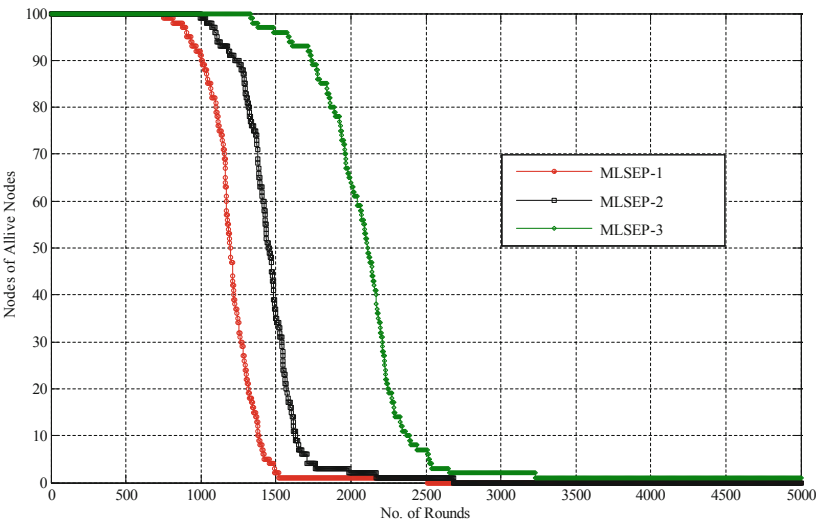


Fig. 5. Number of alive nodes with respect to round numbers for SEP variants

consumption in MLSEP-3 is very less for consecutive rounds as compare to the MLSEP-1 and MLSEP-2 because it elects higher energy nodes as a cluster head instead of arbitrary selection for all the rounds. It allocates the load consistently between the sensors and cluster heads. The results demonstrate the higher energy consumption in MLSEP-1 because distribution of energy is same for all the nodes. Thus, it decreases the computational energy cost of the head nodes in the networks as the level of heterogeneity growths in the networks.

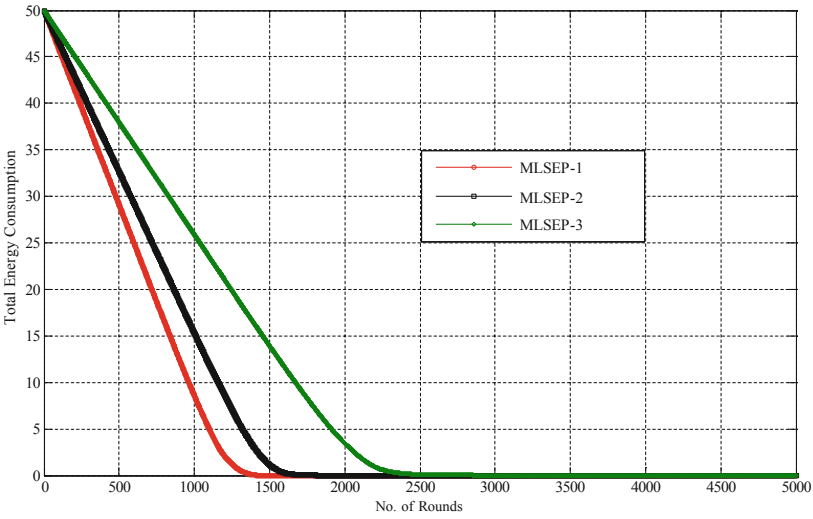


Fig. 6. Total energy consumption in the networks with respect to round numbers for SEP variants

The number of data packets received by the BS in respect of the number of rounds till the networks alive for MLSEP-1, MLSEP-2, and MLSEP-3 is shown the Fig. 7. A huge number of data or information packets are conveyed to the BS with the circumstance that as extensive as the network live. Thus, the number of data or information packets directed by the MLSEP-3, MLSEP-2, and MLSEP-1 to the BS are 2.29×10^{-4}, 1.60×10^{-4}, and 1.33×10^{-4}, in the consecutive rounds, respectively. It is depicted that the MLSEP-3 sent data packets at the higher rate to the base station as associated to MLSEP-1 and MLSEP-2. However, the MLSEP-3 produces highest number of packets because the nodes in MLSEP-3 remain alive more in terms of number of rounds.

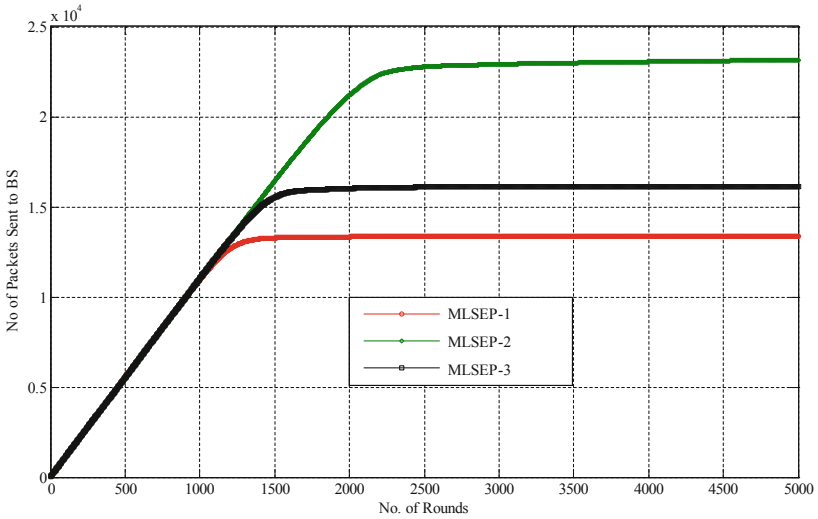


Fig. 7. Total number of packets sent to BS by the networks with respect to round numbers for SEP variants

8.3 Performance Investigation for Homogeneous and Heterogeneous DEEC Protocol Variants

In this section, comparative analysis of the simulation results for homogeneous and heterogeneous DEEC protocol variants are discussed. Figure 8 demonstrates the number of alive nodes in respect of number of rounds for MLDEEC-1, MLDEEC-2, and MLDEEC-3. The MLDEEC-1 is comprising single type of nodes also called homogenous network and MLDEEC-2 & MLDEEC-3 is consisting of 2 & 3 types of nodes, respectively, also called as the heterogeneous networks in nature. It is experientially observed that MLDEEC-3 covers 3446 number of rounds whereas MLDEEC-2 and MLDEEC-1 cover 2412 and 1787 number of rounds, correspondingly, before exhausts whole battery of entire sensors. Thus, MLDEEC-2 and MLDEEC-3 increase 34.97%, and 92.84% in the network lifetime in respect of MLDEEC-1, respectively. The MLDEEC-3 supports in increment in the network lifetime because advanced energy sensors get additional chance to become a CH in each round. It is reducing the dead rate of the sensors and benefits in prolonging the network lifespan. The sustainable period of the network for MLDEEC-1, MLDEEC-2, and MLDEEC-3 are 1350, 1633, 2014 number of rounds, respectively. It is manifest from the Fig. 8 the sustainable period of the MLDEEC-2 and MLDEEC-3 for first node dead significantly exceeds by 20.96%, and 49.19%, as comparison with the MLDEEC-1, correspondingly.

Figure 9 signifies the total energy consumption in consecutive rounds for MLDEEC-1, MLDEEC-2, and MLDEEC-3. Initial total network energy is considered as 50 J. The energy consumption in MLDEEC-3 is very less for consecutive rounds as compare to the MLDEEC-1 and MLDEEC-2 because it elects higher energy nodes as a

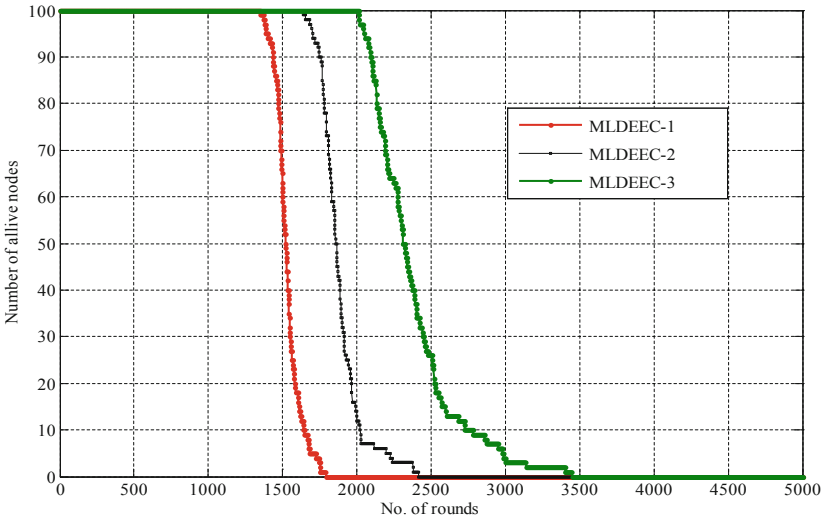


Fig. 8. Number of alive nodes with respect to round numbers for DEEC variants

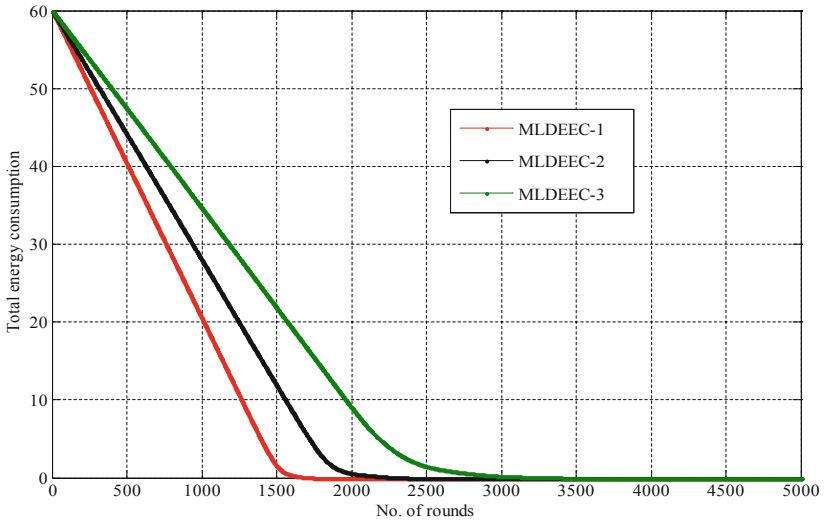


Fig. 9. Total energy consumption in the networks with respect to round numbers for DEEC variants

cluster head instead of random selection for all the rounds. It allocates the load consistently between the sensors and cluster heads. The results illustrate the higher energy consumption in MLDEEC-1 because distribution of energy is same for all the nodes. Thus, it diminishes the computational energy cost of the head nodes in the networks as the level of heterogeneity intensifications in the networks.

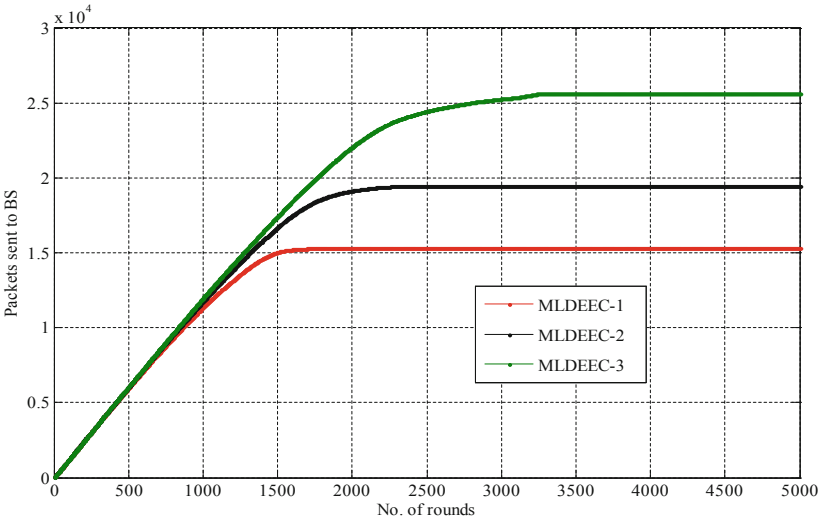


Fig. 10. Total number of packets sent to BS by the networks with respect to round numbers for SEP variants

The number of data or information packets received by the BS in respect of the round numbers till the networks alive for MLDEEC-1, MLDEEC-2, and MLDEEC-3 is shown the Fig. 10. A large number of packets are conveyed to the BS with the fact that as extensive as the network live. Thus, the number of packets sent by the MLDEEC-3, MLDEEC-2, and MLDEEC-1 to the BS are 2.56×10^{-4}, 1.94×10^{-4}, and 1.52×10^{-4}, in the consecutive rounds, respectively. It is observed that the MLDEEC-3 sent data packets at the higher rate to the base station as associated to MLDEEC-1 and MLDEEC-2. However, the MLDEEC-3 produces highest number of packets because the nodes in MLDEEC-3 remain alive more in terms of number of rounds.

8.4 Performance Investigation for Homogeneous and Heterogeneous HEED Protocol Variants

In this segment, comparative analysis of simulation results for homogeneous and heterogeneous HEED protocol variants are discussed. The number of advanced & normal nodes are 39 & 61 and their respective energies are 0.6 J and 0.5 J in case of 2-level heterogeneity. In case of 3-level heterogeneity, the number of super, advanced, & normal nodes are 23, 26, & 51 and their respective energies are 2.0 J, 0.6 J, and 0.5 J. Figure 11 illustrations the number of alive nodes in respect of round numbers for MLHEED-1, MLHEED-2, and MLHEED-3. The MLHEED-1 is containing single type of nodes also called homogenous network and MLHEED-2 & MLHEED-3 is consisting of 2 & 3 types of nodes, respectively, also called as the heterogeneous networks in nature. It is observed that MLHEED-3 covers 5574 number of rounds whereas MLHEED-2 and MLHEED-1 cover 1814 and 1459 number of rounds,

correspondingly, before exhausts comprehensive battery of all the nodes. Thus, MLHEED-2 and MLHEED-3 increase 24.33%, and 282.04% in the network lifetime in respect of MLHEED-1, respectively. The MLHEED-3 helps in increment in the network lifetime because advanced energy sensors get additional chance to become a CH in each round. It is also reducing the dead rate of the sensors and benefits in prolonging lifespan of the network. The sustainable period of the network for MLHEED-1, MLHEED-2, and MLHEED-3 are 341, 364, 364 number of rounds, respectively. It is also manifest from the Fig. 11 the sustainable period of the MLHEED-2 and MLHEED-3 for first node dead significantly exceeds by 6.74%, and 6.74%, as comparison with the MLHEED-1, respectively.

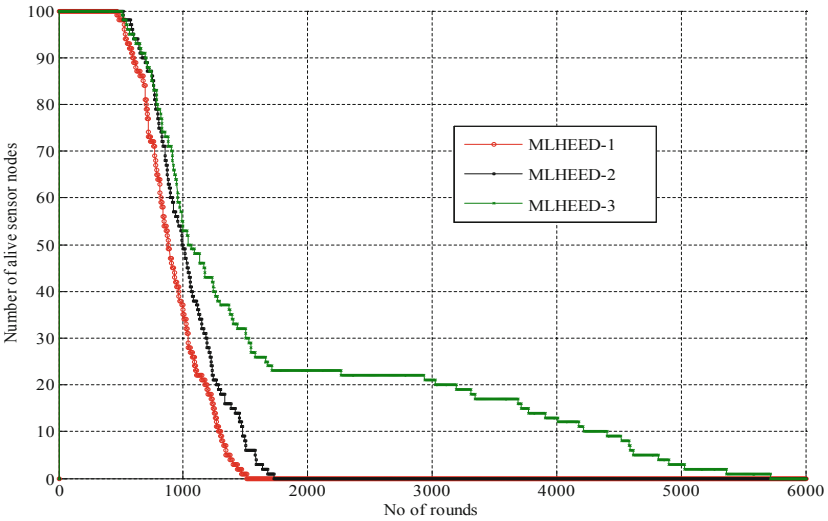


Fig. 11. Number of alive nodes with respect to round numbers for HEED variants

Figure 12 represents the total battery depletion in successive rounds for MLHEED-1, MLHEED-2, and MLHEED-3. Initial energy of the network is considered as 50 J. The energy consumption in MLHEED-3 is very less for consecutive rounds as compare to the MLHEED-1 and MLHEED-2 because it selects higher energy nodes as a cluster head instead of random selection for all the rounds. It allocates the load consistently between the sensors and cluster heads. The results show the higher energy consumption in MLHEED-1 because distribution of energy is same for all the nodes. Thus, it diminishes the computational energy cost of the head nodes in the networks as the level of heterogeneity prolongs in the networks.

The number of data or information packets received by the BS in respect of the number of rounds till the networks alive for MLHEED-1, MLHEED-2, and MLHEED-3 is shown the Fig. 13. A large number of data packets are conveyed to the BS with the circumstance that as extensive as the network live. Thus, the number of packets delivered by the MLHEED-3, MLHEED-2, and MLHEED-1 to the BS are

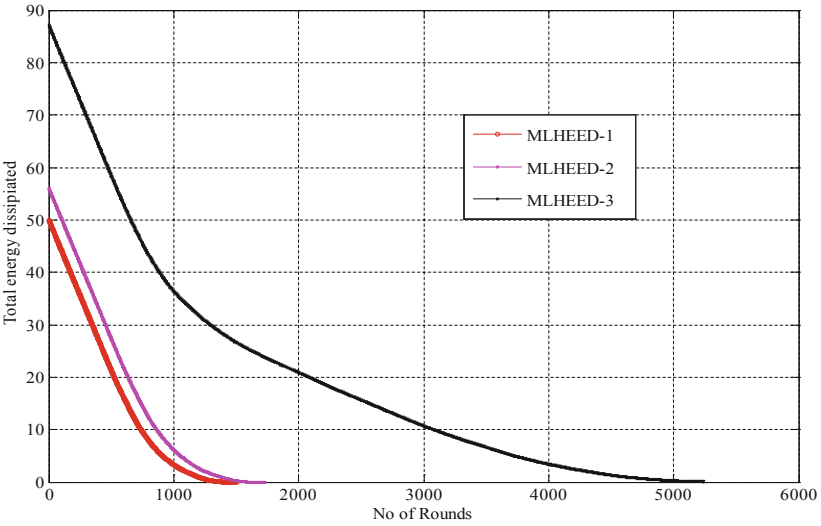


Fig. 12. Total energy consumption in the networks vs round numbers for HEED variants

4.60×10^{-4}, 1.41×10^{-4}, and 1.20×10^{-4}, in the consecutive rounds, respectively. It is observed that the MLHEED-3 sent data packets at the higher rate to the sink as associated to MLHEED-1 and MLHEED-2. However, the MLHEED-3 produces highest number of packets because the nodes in MLHEED-3 remain alive more in terms of number of rounds.

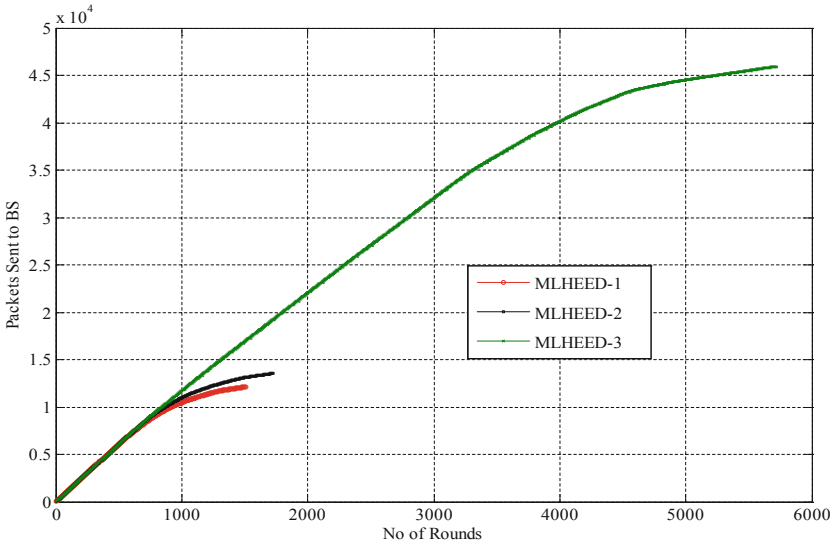


Fig. 13. Total number of packets sent to BS vs round numbers for HEED variants

8.5 Performance Investigation for Homogeneous and Heterogeneous PEGASIS Protocol Variants

In this segment, the comparative analysis of the results for homogeneous and heterogeneous PEGASIS protocol variants are discussed. Figure 14 shows the number of alive sensors in respect of round numbers for MLPEGASIS-1, MLPEGASIS-2, and MLPEGASIS-3. The MLPEGASIS-1 is comprising single type of nodes also called homogenous network and MLPEGASIS-2 & MLPEGASIS-3 is consisting of 2 & 3 types of nodes, respectively, also called as the heterogeneous networks in nature. It is observed that MLPEGASIS-3 covers 3366 number of rounds whereas MLPEGASIS-2 and MLPEGASIS-1 cover 2830 and 2232 number of rounds, correspondingly, before diminishes comprehensive battery of entire the sensors. Thus, MLPEGASIS-2 and MLPEGASIS-3 increase 26.79%, and 50.81% in the network lifetime in respect of MLPEGASIS-1, respectively. The MLPEGASIS-3 supports in increment in the network lifetime because advanced energy sensors get additional chance to become a CH in each round. It is also reducing the dead rate of the sensors and benefits in prolonging the network lifespan. The sustainable period of the network for MLPEGASIS-1, MLPEGASIS-2, and MLPEGASIS-3 are 805, 958, 1063 number of rounds, respectively. It is manifest from the Fig. 14 the sustainable period of the MLPEGASIS-2 and MLPEGASIS-3 for first node dead significantly exceeds by 19.01%, and 32.05%, as comparison with the MLPEGASIS-1, correspondingly.

Figure 15 signifies the total energy depletion in successive rounds for MLPEGASIS-1, MLPEGASIS-2, and MLPEGASIS-3. Initial network energy is considered as 50 J. The energy consumption in MLPEGASIS-3 is very less for consecutive rounds as compare to the MLPEGASIS-1 and MLPEGASIS-2 because it selects higher energy nodes as a cluster head instead of random selection for all the rounds. It

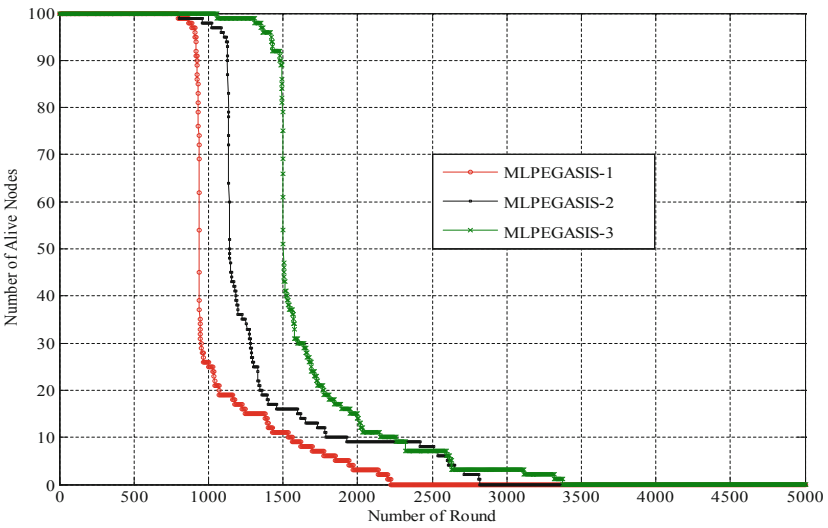


Fig. 14. Number of alive nodes with respect to round numbers for PEGASIS variants

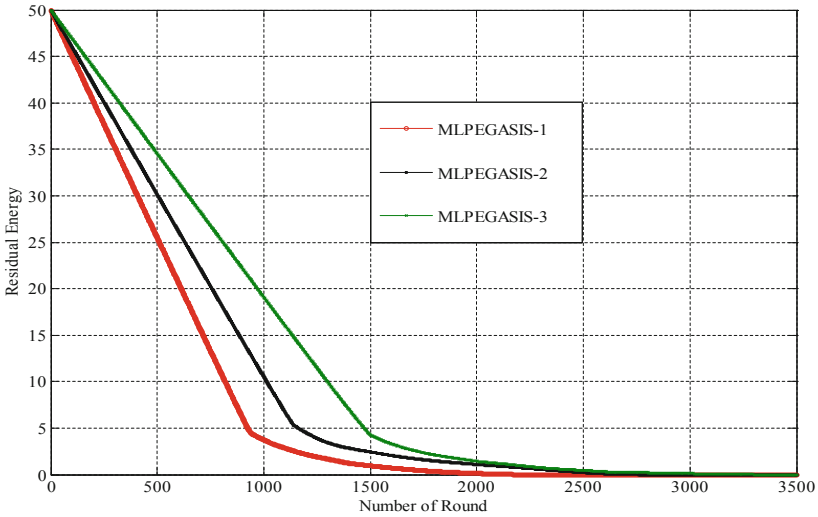


Fig. 15. Total energy consumption in the networks with respect to round numbers for PEGASIS variants

allocates the load consistently between the sensors and CHs. The results show the higher energy consumption in MLPEGASIS-1 because distribution of energy is same for all the nodes. Thus, it diminishes the computational energy cost of the head nodes in the networks as the level of heterogeneity prolongs in the networks.

The number of packets received by the BS in respect of the number of rounds till the networks alive for MLPEGASIS-1, MLPEGASIS-2, and MLPEGASIS-3 is shown the Fig. 16. A large number of information or data packets are conveyed to the base station with the circumstance that as extended as the network live. Thus, the number of packets sent by the MLPEGASIS-3, MLPEGASIS-2, and MLPEGASIS-1 to the base station are 1.73×10^{-4}, 1.33×10^{-4}, and 1.11×10^{-4}, in the consecutive rounds, respectively. It is observed that the MLPEGASIS-3 sent data packets at the higher rate to the base station as associated to MLPEGASIS-1 and MLPEGASIS-2. However, the MLPEGASIS-3 produces highest number of packets because the nodes in MLPEGASIS-3 remain alive more in terms of number of rounds.

8.6 Comparative Analysis of Different Protocols

The comparative analysis of the LEACH, SEP, DEEC, HEED, PEGASIS variants protocols are shown the Table 1 in term of network lifetime, percentage increment in network lifespan, and number of packets directed to BS. The 3-level heterogeneity has an important enhancement in the lifespan of the network and the information packet sent to the BS among all procedures due to the subsequent explanations. First, network consist of 3 types of sensor nodes. Thus, advanced remaining battery sensors are selected as the CHs instead of arbitrary nodes. Secondly, the sophisticated energy sensors are used to balancing the nodes among the other nodes. Similarly, in 3-level

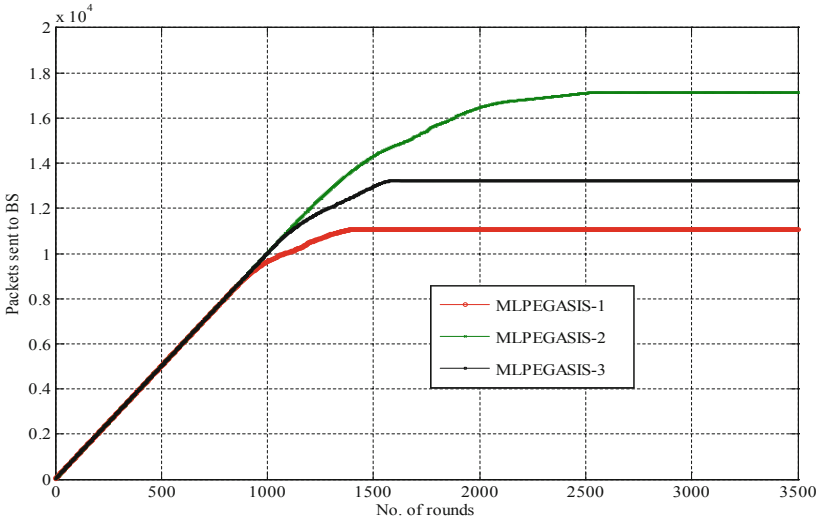


Fig. 16. Total number of information packets sent to BS by the networks with respect to round numbers for PEGASIS variants

heterogeneity, a huge number of information packet are conveyed to the BS. It is also obvious that the networks have long lifetime when it is transmitting huge number of information packets to the BS.

Table 1. Specifies the network lifetime and number of packets sent to BS for different variants of communication protocols

Protocols	Variants	Network lifetime	% Increment in network lifetime	Number of pkts sent to BS
LEACH	MLLEACH-1	1407	–	1.10×10^{-4}
	MLLEACH-2	1597	13.50%	1.31×10^{-4}
	MLLEACH-3	2142	52.24%	1.71×10^{-4}
SEP	MLSEP-1	1517	–	1.33×10^{-4}
	MLSEP-2	2157	42.19%	1.60×10^{-4}
	MLSEP-3	2659	75.28%	2.29×10^{-4}
DEEC	MLDEEC-1	1787	–	1.52×10^{-4}
	MLDEEC-2	2412	34.97%	1.94×10^{-4}
	MLDEEC-3	3446	92.84%	2.56×10^{-4}
HEED	MLHEED-1	1459	–	1.20×10^{-4}
	MLHEED-2	1814	24.33%	1.41×10^{-4}
	MLHEED-3	5574	282.04%	4.60×10^{-4}
PEGASIS	MLPEGASIS-1	2232	–	1.11×10^{-4}
	MLPEGASIS-2	2830	26.79%	1.33×10^{-4}
	MLPEGASIS-3	3366	50.81%	1.73×10^{-4}

Table 2 shows the comparative analysis for LEACH, SEP, DEEC, HEED, PEGASIS protocols variants in terms of constancy period and percentage increment in the constancy of the network. Stability period of a network is the time when the first node (FND) of the network dead. In all the variants, type 3 networks have more stable as compare to the type 2 and type 1 networks. The stable period of the LEACH, SEP, DEEC, HEED, PEGASIS protocols in case of type 3 and type 2 of heterogeneity are 39.03%, 77.26%, 49.19%, 6.74%, & 32.05% and 17.35%, 33.11%, 20.96%, 6.74%, & 19.01% as compare to homogeneity, respectively.

Table 2. Indicates the Stability period for different variants of communication protocols

Protocols	Variants	Stability period	% Increment in stability period
LEACH	MLLEACH-1	807	–
	MLLEACH-2	947	17.35%
	MLLEACH-3	1122	39.03%
SEP	MLSEP-1	752	–
	MLSEP-2	1001	33.11%
	MLSEP-3	1333	77.26%
DEEC	MLDEEC-1	1350	–
	MLDEEC-2	1633	20.96%
	MLDEEC-3	2014	49.19%
HEED	MLHEED-1	341	–
	MLHEED-2	364	6.74%
	MLHEED-3	364	6.74%
PEGASIS	MLPEGASIS-1	805	–
	MLPEGASIS-2	958	19.01%
	MLPEGASIS-3	1063	32.05%

9 Advantages of Heterogeneous Networks over Homogeneous Networks

There are lot of advantages of heterogeneous WSNs over the homogeneous wireless sensor networks as discussed as follows.

- ***Load balancing in energy consumption:*** The energies of the sensors are different in heterogeneous networks at the time of their deployment. The nodes have more energy helps in increasing the lifespan for data transmission and processing information. Thus, it balancing the load among the sensor nodes.
- ***Sensing and communication range coordination:*** The heterogeneous WSNs have uneven sensing and communication ranges. Some of the sensor nodes have r_1 sensing/communication range and others are having r_2 sensing/communication range. It helps in such environment where sensing areas are unfavorable because of the existing obstacles.

- ***Computation and storage effectiveness:*** Sensors have very inadequate memory and computational power. In some sceneries, sensors node performs more computation and also require more memory for the storage opinion. Thus, it is necessary to deploy sensor nodes in the with different capabilities for the effectiveness of a networks.
- ***Prolong network lifespan:*** Deployment of few heterogeneous nodes in the networks always helps in increasing the lifespan of the overall networks. It may also increase the existing energy of the networks. Sometimes, it may increase the cost but proportionally increase the lifespan of the deployed networks.

10 Summary

For the last couple of years, there have been a good amount of research works on WSNs that include several protocols like LEACH, SEP, DEEC, HEED, PEGASIS and their variants protocols, etc. All the protocols are aimed for increasing the network lifetime by efficiently utilizing network energy. This is all the more important because the sensor nodes are having limited battery power, which cannot be recharged or replaced. Another way of enhancing the network lifetime is to prolong the network energy and energy efficient clustering. The network energy can be increased through energy heterogeneity. In this chapter, we have discussed LEACH, SEP, DEEC, HEED, PEGASIS and their variants protocols by incorporating the 2-level and 3-level heterogeneity. The summary of the LEACH, SEP, DEEC, HEED, PEGASIS and their variants protocols are given as follows after comparative performance investigation.

The network lifetime increases by 13.50% and 52.24% in MLLEACH-2 and MLLEACH-3 without any increment in the network energies with respect of MLLEACH-1. The throughput of the MLLEACH-3, MLLEACH-2, and MLLEACH-1 is to successful transmitted 1.71×10^{-4}, 1.31×10^{-4}, and 1.10×10^{-4} number of information packets to the BS in the consecutive rounds, respectively.

The lifespan of the network increases by 42.19% and 75.28% in MLSEP-2 and MLSEP-3 without any increment in the network energies with respect of MLSEP-1. The throughput of the MLSEP-3, MLSEP-2, and MLSEP-1 is to successful transmitted 2.29×10^{-4}, 1.60×10^{-4}, and 1.33×10^{-4} number of information packets to the BS in the consecutive rounds, respectively.

The lifespan of the network increases by 34.97% and 92.84% in MLDEEC-2 and MLDEEC-3 without any increment in the network energies with respect of MLDEEC-1. The throughput of the MLDEEC-3, MLDEEC-2, and MLDEEC-1 is to successful transmitted 2.56×10^{-4}, 1.94×10^{-4}, and 1.52×10^{-4} number of information packets to the BS in the consecutive rounds, respectively.

The lifespan of the network prolongs by 24.33% and 282.04% in MLHEED-2 and MLHEED-3 for increasing 7.8% and 74.2% in the network energies, respectively, with respect of MLHEED-1. The throughput of the MLHEED-3, MLHEED-2, and MLHEED-1 is to successful transmitted 4.60×10^{-4}, 1.41×10^{-4}, and 1.20×10^{-4} number of information packets to the BS in the consecutive rounds, respectively.

The lifespan of the network increases by 26.79% and 50.81% in MLPEGASIS-2 and MLPEGASIS-3 without any increment in the network energies with respect of MLPEGASIS-1. The throughput of the MLPEGASIS-3, MLPEGASIS-2, and MLPEGASIS-1 is to successful transmitted 1.73×10^{-4}, 1.33×10^{-4}, and 1.11×10^{-4} number of information packets to the BS in the consecutive rounds, respectively.

Overall, the lifespan of the network prolongs as the level of heterogeneity extends and if networks work for a longer duration then networks transmitted a huge number of packets to the BS. Thus, throughput of the networks enhances significantly.

11 Future Scope

There are lots of future scope in this area of research as given as follows. Firstly, these works can be extended for the real time scenarios such as precision agriculture, traffic monitoring, structure health monitoring, military applications etc. Secondly, this work can be integrated with different Internet of Things (IoT) applications such as smart city, smart grids, smart home, wearable devices that make our life easy, smart farming, smart retail etc. Thirdly, these works can be extended to increasing the capabilities of secure data transmission. Fourthly, the fault tolerance system can be developed in the extension of the work. Last but not the least, these works can be extended to the implement IoT enabled software defined networks.

Moreover, we have considered the nodes as static in our network models. These works can be extended by considering nodes mobility in the networks. We have also considered a single base station, which is static. These works can be extended for multiple base stations and their mobility may also be incorporated. Further, the hierarchical clustering can also be considered. This works has been discussed in 2-D environment; they can be explored in higher dimension environment. We also deliberated grid placement of the sensors. More types of deployments can be explored and accordingly these algorithms can be extended.

References

1. Singh, S., Chand, S., Kumar, B.: Performance investigation of heterogeneous algorithms in WSNs. In: 3rd IEEE International Advance Computing Conference (IACC), pp. 1051–1054 (2013)
2. Singh, Y., Singh, S., Kumar, R.: A distributed energy-efficient target tracking protocol for three level heterogeneous sensor networks. Int. J. Comput. Appl. **51**, 31–36 (2012)
3. Qing, L., Zhu, Q., Wang, M.: Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Comput. Commun. **29**, 2230–2237 (2016)
4. Chand, S., Singh, S., Kumar, B.: 3-level heterogeneity model for wireless sensor networks. Int. J. Comput. Netw. Inf. Secur. **5**, 40–47 (2013)
5. Singh, S.: Heterogeneous protocols for increasing lifetime of wireless sensor networks. J. Global Res. Comput. Sci. **2**, 172–176 (2011)
6. Smaragdakis, G., Matta, I., Bestavros, A.: SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. Technical report BUCS-TR-2004-022, Boston University, Computer Science Department, pp. 1–11 (2004)

7. Singh, S., Sharma, A.K.: Energy-efficient data gathering algorithms for improving lifetime of WSNs with heterogeneity and adjustable sensing range. Int. J. Comput. Appl. **4**, 17–21 (2010)
8. Singh, S., Chand, S., Kumar, B., Kumar, R.: A heterogeneous network model for prolonging lifetime in 3-D WSNs. In: The Next Generation Information Technology Summit (4th International Conference), pp. 257–262 (2013)
9. Mao, Y., Liu, Z., Zhang, L., Li, X.: An effective data gathering scheme in heterogeneous energy wireless sensor networks. In: International Conference on Computational Science and Engineering, pp. 338–343 (2009)
10. Kumar, D., Aseri, T.C., Patel, R.B.: EEHC: energy efficient heterogeneous clustered scheme for wireless sensor networks. Comput. Commun. **32**, 662–667 (2009)
11. Singh, S., Malik, A.: hetSEP: heterogeneous SEP protocol for increasing lifetime in WSNs. J. Inf. Optim. Sci. **38**, 721–743 (2017)
12. Chand, S., Singh, S., Kumar, B.: Heterogeneous HEED protocol for wireless sensor networks. Wirel. Pers. Commun. **77**, 2117–2139 (2014)
13. Singh, S., Malik, A., Kumar, R.: Energy efficient heterogeneous DEEC protocol for enhancing lifetime in WSNs. Eng. Sci. Technol. Int. J. **20**, 345–353 (2017)
14. Chand, S., Singh, S., Kumar, B.: hetADEEPS: ADEEPS for heterogeneous wireless sensor networks. Int. J. Future Gen. Commun. Netw. **6**, 21–32 (2013)
15. Singh, S., Chand, S., Kumar, B.: 3-tier heterogeneous network model for increasing lifetime in three dimensional WSNs. In: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, pp. 238–247 (2013)
16. Singh, S., Malik, A.: hetDEEC: heterogeneous DEEC protocol for prolonging lifetime in wireless sensor networks. J. Inf. Optim. Sci. **38**, 699–720 (2017)
17. Singh, S., Sharma, A.K.: Distributed energy-efficient algorithm for wireless sensor networks. Int. J. Adv. Res. Comput. Sci. **2**, 548–550 (2011)
18. Qureshi, T.N., Javaid, N., Khan, A.H., Iqbal, A., Akhtar, E., Ishfaqc, M.: BEENISH: balanced energy efficient network integrated super heterogeneous protocol for wireless sensor networks. Procedia Comput. Sci. **19**, 920–925 (2013)
19. Singh, S., Chand, S., Kumar, B.: A stage-4 heterogeneous network model in WSNs. In: International Conference on Advances in Computing, Communications and Informatics, pp. 2191–2195 (2014)
20. Singh, S., Chand, S., Kumar, B.: Energy efficient clustering protocol using fuzzy logic for heterogeneous WSNs. Wirel. Pers. Commun. **86**, 451–475 (2016)
21. Qing, L., Zhu, Q., Wang, M.: Design of a distributed energy efficient clustering (DEEC) algorithm for heterogeneous wireless sensor networks. Comput. Commun. **29**, 2230–2237 (2006)
22. Singh, S., Chand, S., Kumar, B.: Multilevel heterogeneous network model for wireless sensor networks. Telecommun. Syst. **64**, 259–277 (2017)
23. Singh, S.: Energy efficient multilevel network model for heterogeneous WSNs. Eng. Sci. Technol. Int. J. **20**, 105–115 (2017)
24. Heinzelman, W.R., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**, 660–670 (2002)
25. Singh, S., Chand, S., Kumar, B.: Distributed algorithms for maximizing the lifetime of WSNs with heterogeneity for adjustable sensing ranges. Electr. Eng. Res. **1**, 10–17 (2013)
26. Singh, S., Malik, A.: Heterogeneous energy efficient protocol for enhancing the lifetime in WSNs. Int. J. Inf. Technol. Comput. Sci. **9**, 62–72 (2016)
27. Singh, S., Malik, A.: Energy efficient scheduling protocols for heterogeneous WSNs. Int. J. Forensic Comput. Sci. **11**, 8–29 (2016)

28. Singh, S., Kumar, P.: Performance investigation of energy efficient HetSEP for prolonging lifetime in WSNs. In: International Conference on Futuristic Trends in Network and Communication Technologies, pp. 496–509 (2018)
29. Singh, S., Chand, S., Kumar, B.: An energy efficient clustering protocol with fuzzy logic for WSNs. In: 5th International Conference-Confluence the Next Generation Information Technology Summit, pp. 427–431 (2014)
30. Singh, S., Sharma, A.K.: Distributed algorithms for maximizing lifetime of WSNs with heterogeneity and adjustable sensing range for different deployment strategies. Int. J. Inf. Technol. Comput. Sci. **5**, 101–108 (2013)
31. Singh, S.: Energy-efficient target monitoring algorithm for wireless sensor networks. J. Global Res. Comput. Sci. **2**, 186–189 (2011)
32. Singh, S., Sharma, A.K.: A heterogeneous power efficient load balancing target-monitoring protocol for sensor networks. In: International Conference on Parallel, Distributed and Grid Computing, pp. 152–157 (2010)
33. Singh, S., Chand, S., Kumar, R., Malik, A., Kumar, B.: NEECP: novel energy-efficient clustering protocol for prolonging lifetime of WSNs. IET Wirel. Sens. Syst. **6**, 151–157 (2016)
34. Singh, S., Chand, S., Kumar, B.: Performance evaluation of distributed protocols using different levels of heterogeneity models in wireless sensor networks. Int. J. Comput. Netw. Inf. Secur. **7**, 38–45 (2015)
35. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks. IEEE Trans. Mob. Comput. **3**, 366–379 (2004)
36. Lindsey, S., Raghavendra, C.S., Sivalingam, K.M.: Data gathering algorithms in sensor networks using energy metrics. IEEE Trans. Parallel Distrib. Syst. **13**, 924–935 (2002)

A Firefly Optimization Algorithm for Maximizing the Connectivity in Mobile Wireless Sensor Network

Mamatha K M[1(✉)] and Kiran M[2]

[1] Visvesvaraya Technological University, Belgaum, India
mamatha.km33@gmail.com
[2] National Institute of Technology Karnataka, Surathkal, Mangalore, India
kiranmanjappa@nitk.edu.in

Abstract. For the effective functioning of a Mobile Wireless Sensor Networks (MWSN), the connectivity maintenance of the sensor nodes is of significant concern. Otherwise, it may result in an independent node or nodes wholly get detached from the network. Though such detached sensor nodes are functioning correctly and have good energy backup, its service cannot be utilized for the purpose it is intended for as it is isolated from the core network. These sensor nodes are sophisticated tiny devices and costlier depending on the application; therefore, proper care should be taken to keep them connected to the network. Hence, a firefly based algorithm, a Swarm Intelligence technique, referred to as *Firefly Algorithm for Connectivity in Mobile WSN (FACM)* has been proposed in this article in order to establish proper connectivity among the sensor nodes in MWSN. FACM is based on the insect fireflies, which have a unique feature of producing light, a result of chemical reaction, at different intervals to escape from the predators and most of the time to attract prey. The inevitable feature of insect firefly, attracting the prey, is exploited in the proposed FACM where a brighter sensor node (in terms of energy and distance) will attract the less bright neighboring sensor nodes. Thus, the less bright sensor node can depend on the brighter sensor node for the data transfer, thereby saving its energy. A fitness function has been designed based on the combination of two parameters *energy* and the *distance*, which decides the brightness of the sensor node. The effectiveness of the proposed FACM has been theoretically analyzed and verified by simulation through MATLAB. The results obtained are compared with classical FA and are found to be inspiring.

Keywords: Mobile Wireless Sensor Network (MWSN) · Firefly Algorithm (FA) · Swarm Intelligence (SI) · Connectivity · Self organization

1 Introduction

Wireless Sensor Networks (WSNs) are gaining importance in smart technologies of wireless communication [1]. A typical WSN involves a large number of sophisticated tiny devices with intelligent sensors that have the capability of sensing the data, collecting the data, compute the data and establish communication with neighboring

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 195–217, 2020.
https://doi.org/10.1007/978-3-030-40305-8_10

sensor nodes within the network. Evolving generations are highly dependent on the Internet of Things (IoT) and are widely used in *physical systems, industrial environment monitoring systems, information technology, wearable medical care systems, military, and other applications*. On the other side, these WSNs, which are in extensive use in recent technologies, have some limitations which affect their performance. The sensor nodes are usually prone to failures because of hardware degradation, node displacement, environmental causes, and for other reasons [2].

WSNs are categorized into Stationary WSNs (SWSNs) and MWSNs. In SWSNs sensor nodes are static i.e. once the sensor nodes are deployed they do not change their position and have the advantage of easy deployment and easy connectivity establishment within the network. The MWSN have the same property as that of SWSNs but the sensor nodes here are deployed randomly and are able to change their position depending on the application and scenario. In SWSNs, when a sensor node fails, that particular area may be left uncovered or in worst case it may result in partitioning of the whole network which in turn may affect the performance of the network. Where as in MWSNs such situations will be handled by its self- organization property which make sure that all the sensor nodes are well connected and thereby providing the good network efficiency.

Self organization property aims to establish an optimized connectivity within the sensor network field and is an essential feature of MWSNs which has resulted in global level response. In self organization, the network system interacts among sensor nodes without a central authority, dynamically and autonomously to maintain the connectivity with all sensor nodes.

2 Issues and Challenges in MWSNs

Introduction of mobility in SWSNs brings a great challenge in WSNs. In this section, recent issues and challenges of MWSNs are discussed. Recent smart technologies of MWSNs are widely used in monitoring *Nuclear Power Plant, Life Habitat, Earthquake,* and in many more applications. Achieving the *reliability, security* and *robustness* with respect to these applications remains a great challenge. Issues with the mobility of sensor nodes in MWSNs results in variation with the network topology, packet loss rate, time delay, and other parameters. Maintaining stability in the network sensors Localization [3], establishing Connectivity and Coverage [4] in MWSNs plays an important role.

Recent trends find MWSNs in different applications including Underwater MWSNs, Terrestrial MWSNs and Aerial MWSNs [5]. Underwater MWSNs can be linked with Autonomous Underwater Vehicles (AUV) which can be used for monitoring-marine life, water quality and others. Terrestrial MWSNs and Aerial MWSNs can be linked with Unnamed Aerial Vehicles (UAVs) and are used for wildlife monitoring, surveillance, object tracking and multimedia data gathering. Main challenges faced with MWSNs are with hardware and environment. Hardware constraint is mainly because of limited battery power and thus energy has to be utilized efficiently for maintaining long time connectivity within the sensor field.

Optimized connectivity is a basic problem in MWSNs which reflects performance of sensor network. In recent research development, natured inspired Swarm Intelligence (SI) [6] techniques have been adopted in solving the connectivity and coverage issues in MWSNs. SI is concerned with study of combined behavior of individuals within the environment. Many SI techniques such as *ant colony optimization, particle swarm optimization, bird flocking algorithm, honey bee optimization, school of fish algorithm* and *FA* have inspired researchers to optimize issues like self-organization and decentralized coordination. These algorithms are based on nature inspired intelligence and are highly robust, adaptive and scalable [7]. One of the unique feature of SI techniques is self-organization; thus this property of SI can be exploited for self organization in MWSNs [2].

Hence in this article, an optimized SI based connectivity maintenance algorithm has been defined in order to achieve efficient connectivity among the sensor nodes with low power utilization and with less complexity to improve the performance of the sensor network. The proposed algorithm the classical FA, one of the exciting SI techniques, for connectivity maintenance as this technique has been proven very promising [8–11].

The unique feature of fireflies, flashing of light at different intervals due to chemical reaction, has been exploited in the proposed algorithm for better connectivity of the sensor nodes. Fireflies use flashing light for two reasons, *to escape from the predators* and *to attract the prey*. As the light produced by the fireflies will be brighter, the other insects will get attracted by this and becomes easy prey for the fireflies. This feature of fireflies, producing brighter light and attracting prey, has been exploited in the proposed algorithm for maintaining optimized connectivity in MWSNs. Based on the two important features, namely *remaining energy* and *the distance from the neighbor node*, the brightness of the sensor nodes will be decided. The brighter sensor nodes attract less bright sensor nodes. The less brighter sensor nodes (low energy nodes) moves towards and tries to establish connectivity with a much brighter sensor node (high energy nodes); once the connection is established, the less bright sensor node relies on brighter sensor node for the data transfer. Thus less bright sensor node saves its energy and improving the network lifetime. In order to decide the brightness of a sensor node, a fitness function is derived considering the remaining energy and distance parameter of the sensor node. Thus an effort has been made in this article to give the best solution for the hard objective problem of MWSNs, which is optimized connectivity.

The rest of the article is organized as follows. Section 3 gives the related work and Sect. 4 gives the network model for our proposed algorithm. In Sect. 5, the proposed fire fly algorithm has been discussed in detail and in Sect. 6 the results and analysis has been given. In Sect. 7, a future thought of the authors has been given and finally the article is concluded in Sect. 8.

3 Related Work

This section highlights the latest and well known articles surveyed for the given problem statement. The survey focus on Non-SI techniques and SI techniques applied for connectivity and coverage problem in WSNs. Accordingly, this section is divided in to Non-SI based algorithms and SI based algorithms.

3.1 Non-SI Based Algorithms

Self organization of sensor network has been widely investigated by Mills for WSNs in [12] where features like *resource sharing, processing and communication capacity, forming and maintaining structures, conserving power, synchronizing time, adapting behavior associated with routing* have been exploited. Furthermore, author has introduced scientific understandings of self-organizing systems and then have identified the main models investigated by computer scientists which can be applied for self-organization in WSNs. Author also adds that, wireless networks become adept at self organization allowing device to reconnect with surrounding nodes and cooperate to form topologies. Author considers self organization from two views: *natural phenomenon* and *design strategy*. Self organization as a natural phenomenon describes the emergent behavior of an individual which arise naturally through a process of self organization in an natural systems such as biological organisms, ecosystem and geological system. Design strategy includes applying self organization behavior in wireless networks by allowing the adoptability to changing user density and traffic patterns. Authors have even said that self organization could help reconfigure topologies as nodes move in and out of range in mobile ad hoc networks. Nodes in a wireless network share resources such as electromagnetic spectrum, transmission bandwidth and processing capacity. Authors also adds that self organization could be used to discover participants and demands, to determine how best to allocate resources, to monitor changes, and to reallocate resources as and when needed. Further, author has discussed the structure formation and maintenance of networks, simultaneously minimizing power consumption and meeting performance objectives. Finally, the author has concluded the article saying that dynamic nature of sensor networks prevents a prior design of optimal behaviors to implement such functions. For this reason, researchers investigate self organizing techniques that could enable a network to shape its own behaviors based on environment and need.

Wang et al. [13] presents fundamental studies on the sensing coverage and the network connectivity from *mathematical modeling, theoretical analysis and performance evaluation* perspectives. For the experiment both pattern-based deployment strategy and a random deployment strategy are considered for the study. The study aims to deliver a systematic review on the fundamental problems in WSNs and provide guidelines in selecting critical network parameters for WSN design and implementation in practice. Authors have concluded that to communicate successfully, a WSN must provide satisfactory network connectivity eliminating the isolation of sensors and enable each sensor to report its sensed data to its fusion center.

Fei et al. [14] have studied applications of WSNs, especially in the context of monitoring and surveillance, with respect to Multi-Objective Optimization (MOO) considering the challenging factors such as *energy dissipation, packet-loss rate, coverage* and *network lifetime.* The article provides a detailed tutorial and survey of recent research and development efforts in MOO. First, authors provide an overview of the main optimization objectives used in WSNs such as the *maximal energy efficiency, the shortest delay, the longest network lifetime* and *the highest reliability* or the trade-offs among the above objectives. Then, they elaborate on various approaches considered for MOO, such as mathematical programming based scalarization methods,

heuristics or metaheuristics based optimization algorithms and many advanced optimization techniques.

Authors define that the network connectivity in WSNs is dependent on the selected communication protocol. Connectivity requires only the location of any active node that should lie within the communication range of one or more active nodes, hence all active nodes can form a connected communication network. Maintaining the network's connectivity is essential for ensuring that the messages are indeed propagated to the appropriate sink node or base station, and the loss of connectivity is often treated as the end of the network's lifetime. Authors have mentioned that the network connectivity is closely related to the coverage and energy efficiency of WSNs. Authors have also described coverage in the context of the sensing range and connectivity corresponding to the communication range. The article provides useful guidelines for researchers to understand the referenced literature on MOO. Finally, authors have discussed types of open problems to be tackled by future researchers.

3.2 SI Based Algorithms

Mohajerani et al. [15] presents a new Ant Colony Optimization (ACO) based routing algorithm, referred to as *Life Time Aware routing algorithm for Wireless Sensor Networks (LTAWSN)*, which uses special parameters in its competency function, namely *energy* and *distance*, for reducing energy consumption of network nodes. In LTAWSN, a new pheromone update operator was designed to integrate energy consumption and hops into routing choice. Multiple simulation results of LTAWSN in comparison with the previous ant colony based routing algorithms such as *energy aware ant colony routing algorithms* [16], *ant colony optimization-based location-aware routing algorithm* [17] *and traditional ant colony algorithm* [18] shows increase in the efficiency of the system, gain in balanced transmission among the nodes, reduction in the energy consumption of the routing and extends the network lifetime.

In [19] Hashim et al. proposes an enhanced deployment algorithm based on Artificial Bee Colony (ABC) which guarantees to extend the network lifetime by optimizing the network parameters and constraining the total number of deployed relays. Authors claims that the proposed ABC based node deployment algorithm, *Improved Lifetime Deployment subject to Cost Constraint (ILDCC)* enhances the network lifetime. ILDCC uses two-phase relay node deployment strategy where in the first phase the backbone of the network is connected using minimum number of relay nodes for cost efficiency; and in the second phase, a novel heuristic approach is introduced for searching the global optima. The network parameters are optimized in such a way that the minimum objective function is guaranteed and the desired network connectivity is maintained. The proposed technique shows its effectiveness in solving the placement problems associated with WSNs, and the solution can be adopted in wide range applications such as: WSN for Volcanic Monitoring, relay node deployment in forests to detect fires and report wild life activities. Simulations show the effectiveness of the proposed algorithm in comparison with different cases of problem complexity. Results validate that the proposed method improves the network lifetime considerably when compared to solutions reported in the literature such as *Shortest Path 3-D grid Deployment (SP3D) algorithm* [20].

Kumar and Kumar in [21] have given an energy efficient clustering mechanism for WSNs based on ABC algorithm and factional calculus method to maximize the life time of nodes by optimally selecting Cluster Head (CH). The proposed hybrid optimization algorithm referred to as *multi objective fractional artificial bee colony* controls the convergence rate of ABC and derives a new fitness function for finding the CH by having three objectives such as *energy consumption, distance travelled* and *delays.* The proposed algorithm is validated by simulating WSN and performance of algorithms is extensively analyzed with three different perspectives namely *alive node, energy* and *CH*. The simulation results are compared with *LEACH* [22], *PSO* [23] and *ABC* [24] based routing and the results found to be encouraging.

Wang et al. [25] have considered the problem of fixed sink node which often suffer from hot spots problem; sensor nodes which are close to the fixed sink node experience a huge traffic burden during data transmission process. Thus the overall network lifetime is reduced due to the fact that the nodes near the static sink node deplete their energy much faster compared to the rest of the nodes. As a solution, authors have proposed Particle Swarm Optimization (PSO) based clustering technique referred to as *Energy efficient PSO based routing algorithm with Mobile Sink (EPMS)* which uses mobile sink in order to enhance energy efficiency, network lifetime, and latency. EPMS uses virtual clustering technique combined with PSO algorithm to improve the network performance. While selecting the CH, the residual energy and position of the nodes are primary considered to select CH and a control strategy is adopted for receiving the data at mobile sink node from CH. Simulation results show that the energy consumption is much reduced, the network lifetime is prolonged, and the transmission delay is reduced in proposed routing algorithm than *LEACH* [26] and *TTDD* [27] algorithms.

Wang et al. [28] have studied hot-spot problem (WSNs with one static sink node) where the sensor nodes near the static sink bear more traffic load than outlying nodes. Traditionally, adopting sink mobility has been considered as a good strategy to overcome the hot spot problem [29]. Mobile sink nodes move physically within the network field and establish communication with selected nodes to perform direct data collection through short range communications; such short range communications do not require routing. For proper data collection and to achieve higher energy efficiency, the mobile sink node should have optimal mobility trajectory. Authors have found that the traditional ACO algorithm is a good solution for finding an optimal mobility trajectory for the mobile sink. Since ACO suffers from delay; an *Improved ACO algorithm* has been proposed in this article which uses distance of CH for optimal connectivity and for finding the optimal sink node mobility trajectory. The proposed algorithm divides the network in to clusters and each cluster will have one CH. CHs are selected based on the residual energy of each node in the cluster and unlike traditional CH rotation scheme, in the proposed work the CH rotation is done only when the residual energy of the current CH is less than a given energy threshold. Simulation results show that the proposed algorithm can significantly improve WSNs performance compared to other routing algorithm *ACO-M* [30].

In order to improve network lifetime, Madhukar et al. [31] have investigated the Mobile Sensor Deployment (MSD) problem which comprises of network connectivity and target coverage and the authors have resolved the same using *Euclidean Spanning Tree Model (ECST)* and *ECST Adaptive VABC (ECST-AVABC)* method respectively.

AVABC optimization algorithm is proposed considering minimum movement of mobile sensors over the network. With the extensive simulation experiments, authors have offered the optimal promising solutions of network connectivity to the MSD problem with minimum movement and providing the extended lifetime of WSN The experimental results states that the movement distance shown by the proposed ECST-AVABC become 20% lesser than the standard ECST-VABC method [32].

In [33], Ray et al. have studied *coverage* and *energy conservation*, the two prime issues of WSNs, extensively. Sensor movement is required to achieve high coverage; but on the other hand sensor movement consumes most of the sensor node's energy. Thus, coverage and consumption of energy are correlated issues and are difficult to achieve their efficiency at the same time. In this article, authors have studied these conflicting issues, using one of the latest bio-inspired algorithms, known as *Glowworm Swarm Optimization algorithm*. The proposed algorithm referred to as *Energy Efficient Multi-Parameter Reverse Glowworm Swarm Optimization (EEMRGSO)* algorithm achieves the connectivity of sensor nodes in an energy efficient manner. Due to random sensor deployment, two sensor nodes can fall in the same coverage area and it results in the redundancy of network coverage. EEMRGSO reduces redundant coverage area by moving the sensors from densely deployed areas to some predefined grid points. Energy consumption is reduced by decreasing the number of moving sensors as well as the total distance traversed. Simulation results show that, the proposed EEMRGSO algorithm is efficient than the existing Glowworm Swarm Optimization algorithm [34] as it reduces total energy consumption at most by 60%. Proposed algorithm also reduces the number of overlapping sensors significantly and achieves an effective coverage of 80–89% approximately.

Eldrandaly et al. in [35] have focused on optimization and design of MWSNs assuring the spatial coverage of given network area. Authors aim to improve discoverability of mobile sensor nodes using the geographical locations and propose an improved bio- inspired firefly algorithm called *Firefly Algorithm with Crossover and Detection Algorithm (CDFA)* for enhancing the network connectivity and coverage in MWSNs. Proposed CDFA algorithm performs firefly encoding using Grid quorum-based locomotion strategy to establish connectivity and coverage of sensor node with respect to the interest area specified. Also, authors propose three lemma's to optimize maximize coverage area percentage of MWSNs. Authors have tested the proposed CDFA algorithm against different data sets with different criteria comparing to other algorithms such as *whale optimization algorithm* [36], *particle swarm optimization* [37] and *flower pollination algorithm* [38]. The experiments results prove the efficiency of the proposed algorithm with respect to connectivity and coverage rate.

Lu et al. [39] have proposed an coverage optimization techniques for MWSNs using improved FA algorithm. Focusing on the optimization of sensor node distribution, especially in low convergence area, authors have defined a improved firefly algorithm called *Directed Randomly selected Firefly Algorithm (DRSFA)* based on *Randomly Selected Firefly Algorithm (RSFA)* defined in [40]. The DRSFA algorithm updates the position of only two sensor nodes and enable them to move instead of enabling the movement of all the nodes at a time. The sensor nodes are ranked based on their order of connectivity and the sensor nodes with larger connectivity are selected. Author aims to reduce the density of node distribution rapidly and maximize the

coverage rate in short time. And finally show that the simulation results of DRSF algorithm achieve better network coverage comparing to RSFA algorithm.

The exhaustive literature study infer that, the WSNs are distance and energy constrained, as sensor nodes have low power and low computational capabilities. There are only few articles which utilize these constraints and establish an effective communication in the network field. The recent literature study reveals that SI techniques aims to provide an optimized connectivity among sensor nodes in WSNs, allowing the sensor nodes to reconnect with their surroundings, cooperate to form topologies, monitor and adapt to environmental changes, all without human intervention. With reference to article [35] and [39] FA algorithm has proved its efficiency in MWSNs in recent research. And also, comparing to other SI techniques FA is more suited for MWSNs to enhance the connectivity and network life time. Hence, this article focus on providing an SI based solution to connectivity and energy optimization for MWSNs using FA algorithm, with a new fitness function derived using distance and energy parameter.

4 Network Model

In this chapter, connectivity maximization algorithm is proposed with the following properties. Considering the sensor network field where the homogenous mobile sensor nodes are randomly deployed within the network. After the initial deployment nodes change their location for self organization in order to establish stronger connectivity with other sensor nodes in the network. During self organization phase, one of the major problem sensor nodes face is *where to move?*. There is always a threat that, a sensor node can move in the opposite direction of the network and can become isolated. Thus, the algorithm which guides the movement of sensor nodes is very important and this part will be very crucial for the better functioning of the WSNs. Hence in this article, well known SI technique FA algorithm has been used for guiding the sensor node movements in the network field. Like a fire fly attracts other fire flies and insects by flashing of brighter light, sensor node with high energy attracts sensor nodes with low energy in the proposed model; the lesser energy sensor nodes thereafter can depend on the high energy sensor nodes for data transfer. Thus to save the critical sensor nodes and to improve the network life time fitness function is designed using distance and energy as its parameter.

Accordingly, the network model is composed of randomly deployed sensors nodes in the MWSN and each of them has same sensing range R_s with in which nodes try to establish communication with the other nodes. Quality of the coverage inside the circle with radius R_s is constant. Also, in order to simplify, the following assumption has been made for the proposed model:

- Sensor nodes are randomly deployed in MWSN and position of each node is known through GPS.
- Each sensor node is enabled with processor, battery, memory and transceiver.
- After the deployment of the sensor nodes, they transmit their energy and location information to the neighboring nodes. Based on the information received, sensor

nodes selects best neighbor node for communication by performing the fitness function for each nodes.

- Sensor nodes are mobile, they move within the field to establish connectivity among the nodes.

Area that needs to be connected, i.e. sensing field was recognized as *m*n* grid where each grid has size 1 m and *N* represents the total number of the sensors in the network. The Probability of coverage with Grid points *G(x, y)* covered by sensor nodes s_i ($i = 1, 2, \ldots, N$), if their distance is less than or equal to sensing radius R_s is given by Eq. (1) [41]:

$$P(x, y, si) = \begin{cases} 1, & if\ d(G(x, y), si) \leq R_s \\ 0, & otherwise \end{cases} \tag{1}$$

where d($G(x, y)$, s_i) is Euclidean distance between grid point (x, y) and location (xi, yi) of the sensor s_i. Euclidean distance, which gives the distance between the two nodes *node1 (with coordinates x1, y1)* and *node2 (with coordinates x2, y2)* is given in Eq. (2) [42]:

$$d(x, y) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{2}$$

With the gathered information about the distance and energy of each node, the proposed model decides the brightness of the node using two steps. In the first step the higher energy sensor node will be a preferred for next node connectivity; the second objective is to find sensor node with minimum distance (nearest node). The reason behind finding the nearest node is that, the sensor node will expense less amount of energy for its movement towards the nearest neighbor. The overall objective here is to find the *nearest higher energy* node. Finally, using fitness function, the fitness value of the sensor nodes will be decided based on first and second steps.

In order to chose the sensor node with higher energy Eq. (3) will be used where Ex_i($i = 1 \ldots N$) is the energy of the sensor node x_i.

$$F_{energy} = \forall_{i=1}^{n} max\ Ex_i \tag{3}$$

Next, to find the minimum distance between node x_i and next hop x_{i+1}, Eq. (4) will be used where $d(x_i, x_{i+1})$ is the Euclidean distance between two nodes:

$$F_{Distance} = \frac{1}{\forall_{i=1}^{n} d(x_i, x_{i+1})}, \quad where\ d < Rs \tag{4}$$

Considering Eqs. (3) and (4), a fitness function $f(x)$ has been defined in Eq. (5) which gives the fitness value of x^{th} sensor node.

$$f(x) = p\left(F_{energy}\right) + p\left(F_{Distance}\right) \tag{5}$$

Here p is a random value which is assigned to each sub functions whose values lie within [0–1]. With this fitness function *f(x)*, the sensor node establishes the connectivity to the nearest higher energy sensor node in the sensor network field by relocating itself by using the fire fly algorithm explained in the next section.

5 Firefly Algorithm for Connectivity in Mobile WSN(FACM)

Firefly Algorithm (FA) [7], a nature inspired algorithm and a SI technique, mimic the behavior of insect fire flies. In the last few years, FA is successfully applied for different hard optimization problems in WSNs such as *continuous connectivity optimizations* [43], *clustering* [44], *mobile coverage* [45], *and self-organization* [46–48]. In the FA algorithm, firefly's brightness is calculated using a fitness function and the goal is to minimize value of fitness function. Intensity of the light emitted is directly proportional to the brightness of the sensor node. The brightness is directly proportional to intensity of light *I(x)* [7], hence brightness of a sensor node at location x based on its attractiveness are defined using Eqs. (6) and (7).

$$I(x) = \begin{cases} \frac{1}{f(x)}, & if\ f(x) > 0, \\ 1 + |f(x)|, & otherwise \end{cases} \tag{6}$$

where x is *d-dimensional point* in *d-dimensional space* and *f(x)* is the fitness function defined in Eq. (5). The attractiveness β of a sensor node is defined in Eq. (7) where β_0 is the attractiveness at radius $R_s = 0$ and γ is a constant whose value varies between 0.01 and 1 [7].

$$\beta(x) = \frac{\beta_0}{1 + \gamma Rs^2}, \tag{7}$$

Attractiveness β, of a sensor node depends on the distance between two sensor nodes and it is directly proportional to their brightness $I(x)$. As sensor node moves, its value for γ varies between 0.01 and 1. The attractiveness of a sensor node varies with the distance Rs and can be given in Eq. (8) and the movement of a firefly x_i toward more attractive i.e. brighter, firefly x_j is determined by the following Eq. (9).

$$\gamma = e^{\gamma Rs_{ij}^2} \tag{8}$$

$$x_i = x_i + \beta_0 e^{\gamma Rs_{ij}^2}\left(x_j - x_i\right) + \alpha\, \epsilon_i \tag{9}$$

where α is constant and represents randomization parameter, ϵ_i is a vector of random numbers from a Gaussian or uniform distribution, and R_{sij} is the distance between fireflies i and j. In this paper two dimensional sensing field is considered, for determining the coordinates of N sensors, position of each sensor node point will be with respect to x and y coordinates in two dimensional space. Basic steps of the Proposed FACM are presented in Algorithm 1.

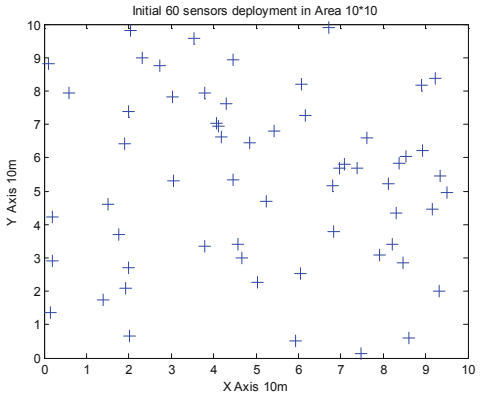
```
Procedure of FACM
    SN - Sensor Node
    f(x) - Fitness function of x^th SN
    Li - Light Intensity of i^th SN
    γ - Light absorption coefficient
    Rs - Sensing Radius of each sensor node
    t - Total Number of Iterations.
    I(x) - Brightness of a x^th SN

Generate initial population of SN (i=1,2,....n) in the network
Calculate the distance d from each SN to its neighbor nodes
Calculate the f(x) using Eqn. (5) for each SN
Calculate brightness of x^th SN using Eqn. (6)

While t becomes zero do
for each x_i do
   for each neighbor SN x_j of x_i do
    if Ii < Ij
        if d< Rs then
                Move SN x_i towards SN x_j in d-dimensional space using Eqn.(9)
                Vary attractiveness with distance Rs using Eqn.(8)
                Update light intensity of SN x_i using Eqn. (5)
            end if
          endif
       end for
     end for
end FACM
```

6 Simulation

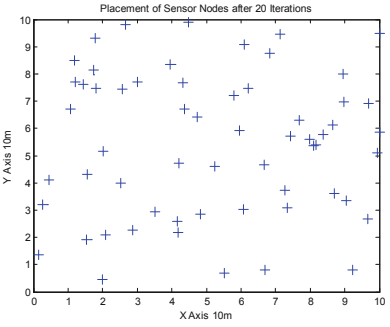
In order to perform the quantitative and qualitative analysis, proposed FACM algorithm and existing FA [35] are simulated using MATLAB R2016a. For simulation, the sensor nodes are randomly deployed within the sensor field and the efficiency of the proposed algorithm is compared with FA with *distance* and *energy* as the comparison parameter. Each sensor node is simulated with the sensing range of $R_s = 2$ m. In order to have the better clarity, the simulation study is done in two folds; Experiment 1, where the self organization of the sensor nodes in the sensor field (movement of sensor nodes) is shown by keeping the node density constant and varying the number of algorithm iterations. Experiment 2, where the self organization of the algorithm is shown by varying the node density and keeping the number of algorithm iterations as constant. Also, the comparison of the FACM and FA is done against the network life time parameter for deep understanding of the proposed algorithm. The two experiments along with the explanations are as follows.

6.1 Experiment 1

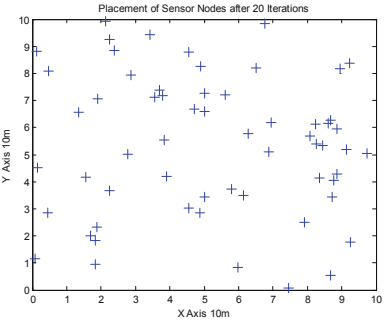
In this experiment, the node density is kept constant i.e. 60 and the behavior of the FACM is observed for 20, 40, 80 and 100 iterations for the 10 m × 10 m is considered



(a) Initial deployment of 60 sensor nodes

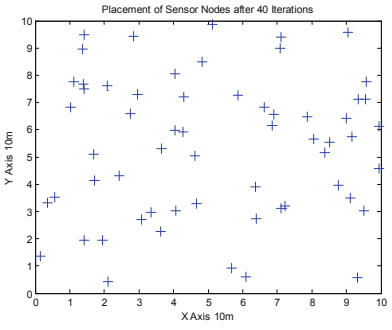


Classical FA

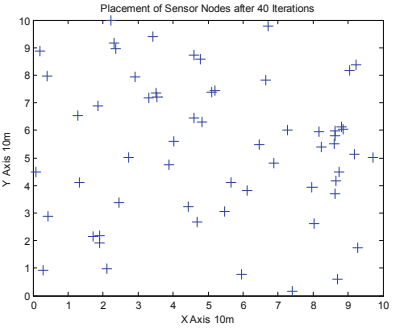


Proposed Algorithm FACM

(b) Displacement of 60 sensor nodes for 20 Iterations



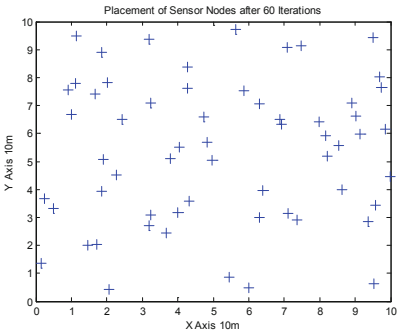
Classical FA

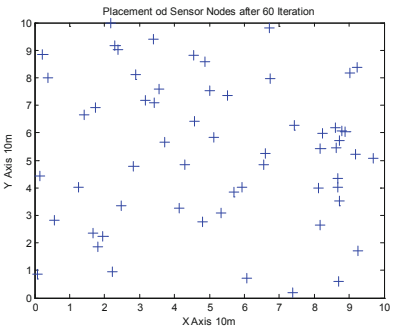


Proposed Algorithm FACM

(c) Displacement of 60 sensor nodes for 40 Iterations

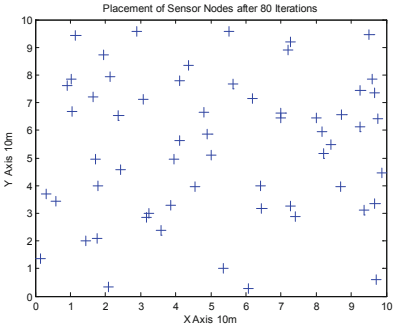
Fig. 1. Node Displacement comparison between FA and FACM for 10 m × 10 m network area

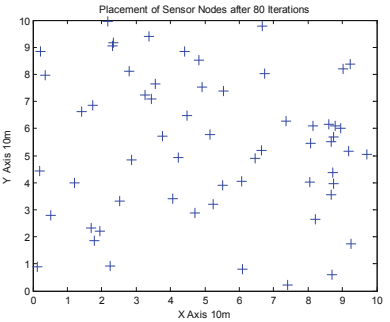




Classical FA Proposed Algorithm FACM

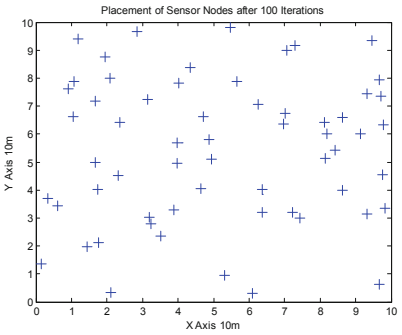
(d) Displacement of 60 sensor nodes for 60 Iterations

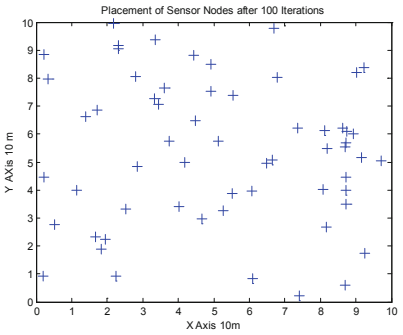




Classical FA Proposed Algorithm FACM

(e) Displacement of 60 sensor nodes for 80 Iterations





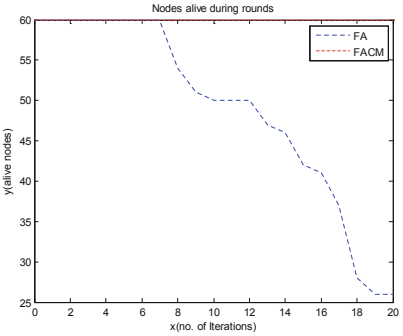
Classical FA Proposed Algorithm FACM

(f) Displacement of 60 sensor nodes for 100 Iterations

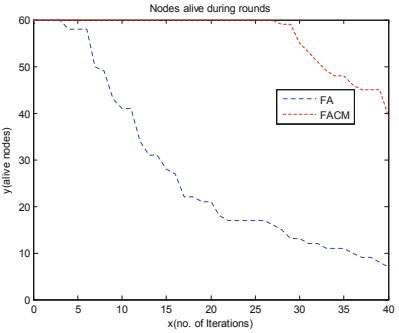
Fig. 1. (*continued*)

to study the behavior of the algorithm when the network is dense and the network is relatively spread out.

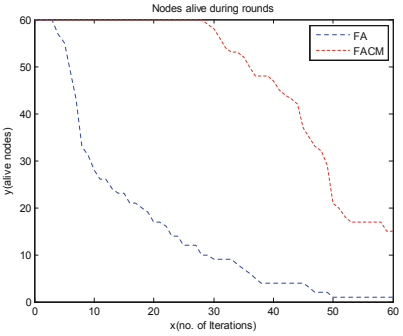
Figure 1(a) shows the initial deployment of 60 sensor nodes in the network area of 10 m × 10 m and Figs. 1(b), (c), (d), (e) and (f) shows the displacement of sensor nodes for 20, 40, 60, 80 and 100 iterations for classical FA and proposed FACM algorithms respectively. The study reveals that the self organization in FACM is better



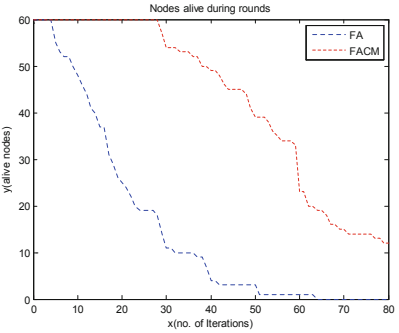
(a) Comparison for 20 Iterations



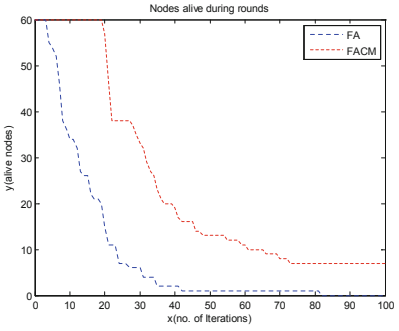
(b) Comparison for 40 Iterations



(c) Comparison for 60 Iterations



(d) Comparison for 80 Iterations



(e) Comparison for 100 Iterations

Fig. 2. Network life time comparison between FA and FACM

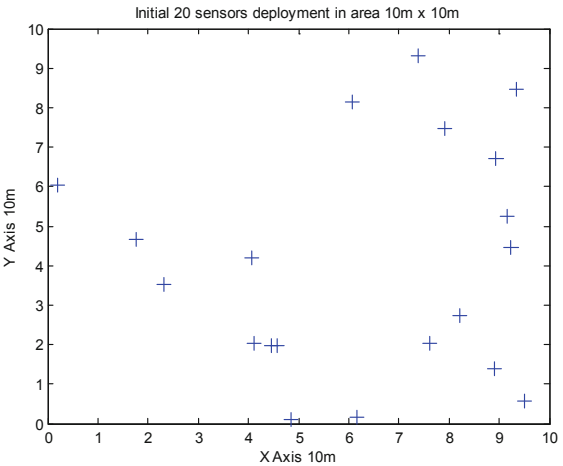
than the classical FA because in FA though the neighbor node distance is considered for self organization it will not consider the minimum distance (nearest neighbor) of selecting the neighbor nodes. Whereas in FACM algorithm, during self organization phase, the sensor nodes uses nearest neighbor node for connectivity and hence improved performance can be observed in FACM algorithm. In FACM algorithm each node according to the fitness value decides towards which nearest neighbor node it should move and each iteration of the algorithm improves the position of the sensor nodes in the network. From the resultant graph it can be clearly observed that after 60 iterations over fitting for the fitness function in the algorithm occurs and sensor nodes starts grouping together in the network.

Figures 2(a), (b), (c), (d) and (e) gives the comparative study of network life time between FACM and FA algorithms for 20, 40, 60, 80 and 100 iterations. After initial deployment, sensor node senses the environment to which it is intended for and self organize to have maximum connectivity. During self organization phase, the fitness value for the neighbor nodes is defined based on the nearest higher energy sensor node. Since higher energy sensor nodes are considered as an attractive factor, all low energy sensor nodes moves towards the higher energy neighbor sensor nodes and depends on them for data dissemination. Since low energy sensor nodes takes help of higher energy sensor nodes, they save much of their energy and will be alive for a longer period of time; thus increases the network lifetime. This can be clearly observed in the graphs shown in Fig. 2. One can clearly observe in Fig. 2(a) that even after 20 iterations all the sensor nodes in the network for FACM algorithm will be still alive where as in FA algorithm the network life starts depleting by 13 iterations only. This is mainly because the energy factor is not considered in the FA algorithm

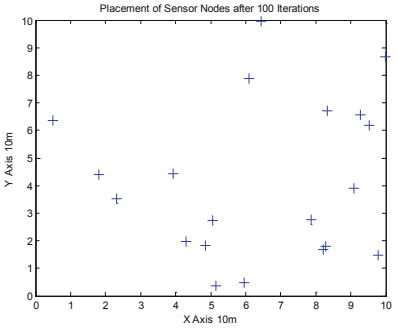
6.2 Experiment 2

Following with Experiment 1, Experiment 2 shows the scalability study of FACM algorithm. In this experiment, the proposed FACM's behavior is observed by keeping the constant number of iterations (i.e. 100) in the network area of range roughly 10 m $\times$ 10 m and varying the node density by 20, 40, 60, 80 and 100 sensor nodes. Each sensor node is simulated with the sensing range of R_s = 2 m. For node density 60, the results are already discussed in Fig. 1(f) of Experiment 1 and hence it is omitted in this section considering redundancy factor.

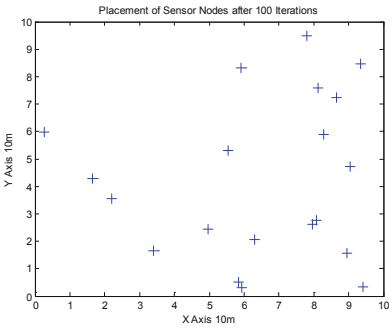
Figure 3(a) shows the initial deployment of 20 sensor nodes in the network area of 10 m $\times$ 10 m and Figs. 3(b) and (c) shows the displacement of 20 sensor nodes for 100 algorithm iterations.



(a) Initial deployment of 20 sensor nodes



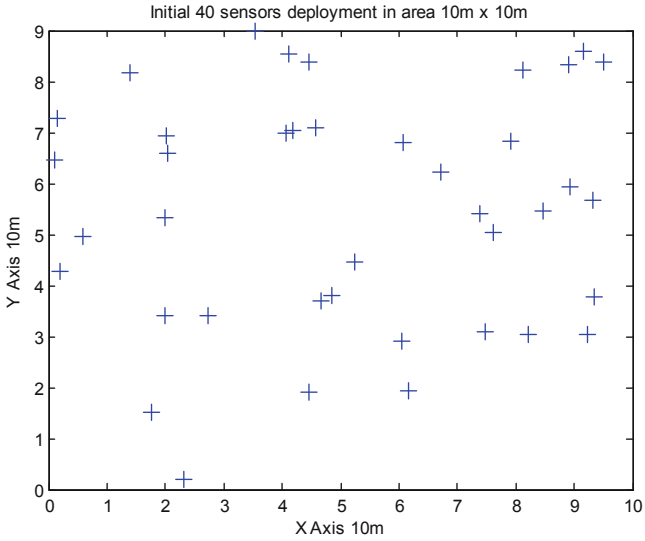
(b) Classical FA



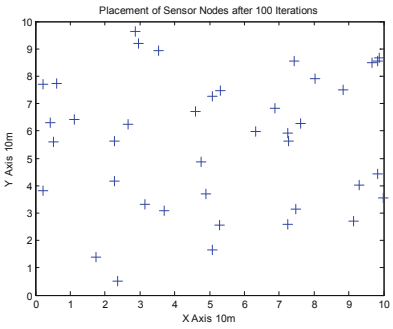
(c) Proposed Algorithm FACM

Fig. 3. 20 Sensor Node Displacement comparison between FA and FACM for 10 m × 10 m network area

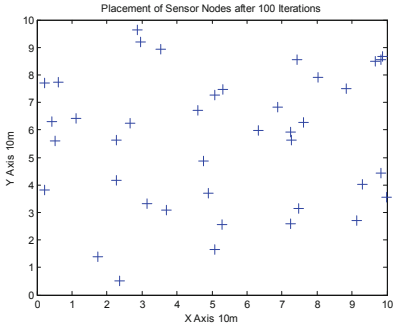
Figure 4(a) shows the initial deployment of 40 sensor nodes in the network area of 10 m × 10 m and Figs. 4(b) and (c) shows the displacement of 40 sensor nodes for 100 algorithm iterations.



(a) Initial deployment of 40 sensor nodes



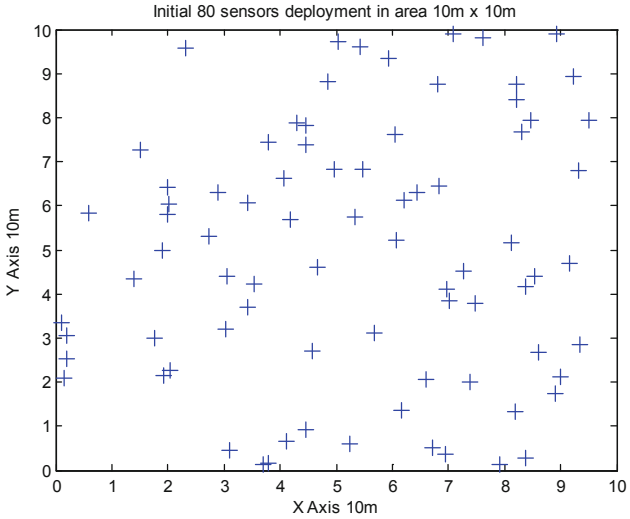
(b) Classical FA



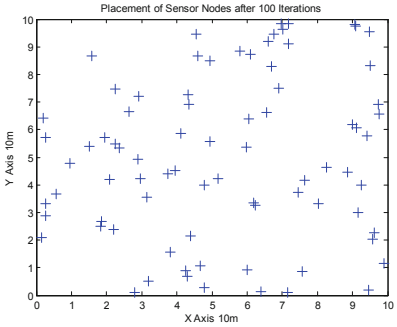
(c) Proposed Algorithm FACM

Fig. 4. 40 Sensor Node Displacement comparison between FA and FACM for 10 m × 10 m network area

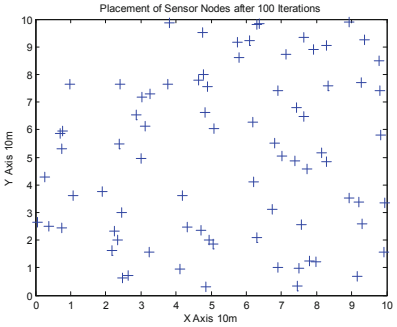
Figure 5(a) shows the initial deployment of 80 sensor nodes in the network area of 10 m × 10 m and Figs. 5(b) and (c) shows the displacement of 80 sensor nodes for 100 iterations.



(a) Initial deployment of 80 sensor nodes



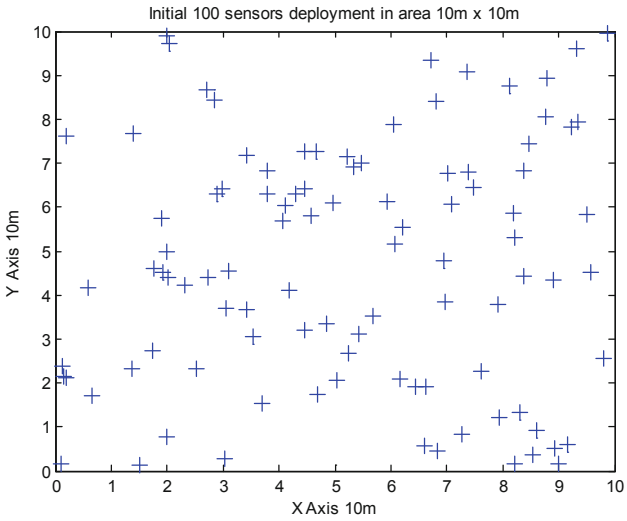
(b) Classical FA



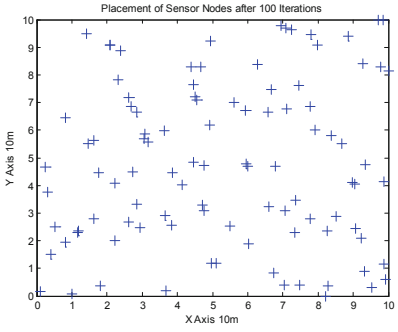
(c) Proposed Algorithm FACM

Fig. 5. 80 Sensor Node Displacement comparison between FA and FACM for 10 m × 10 m network area

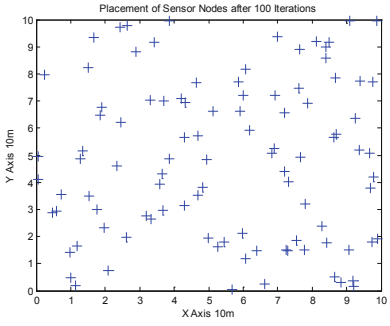
Figure 6(a) shows the initial deployment of 100 sensor nodes in the network area of 10 m × 10 m and Figs. 6(b) and (c) shows the displacement of 100 sensor nodes for 100 algorithm iteration.



(a) Initial deployment of 100 sensor nodes



(b) Classical FA

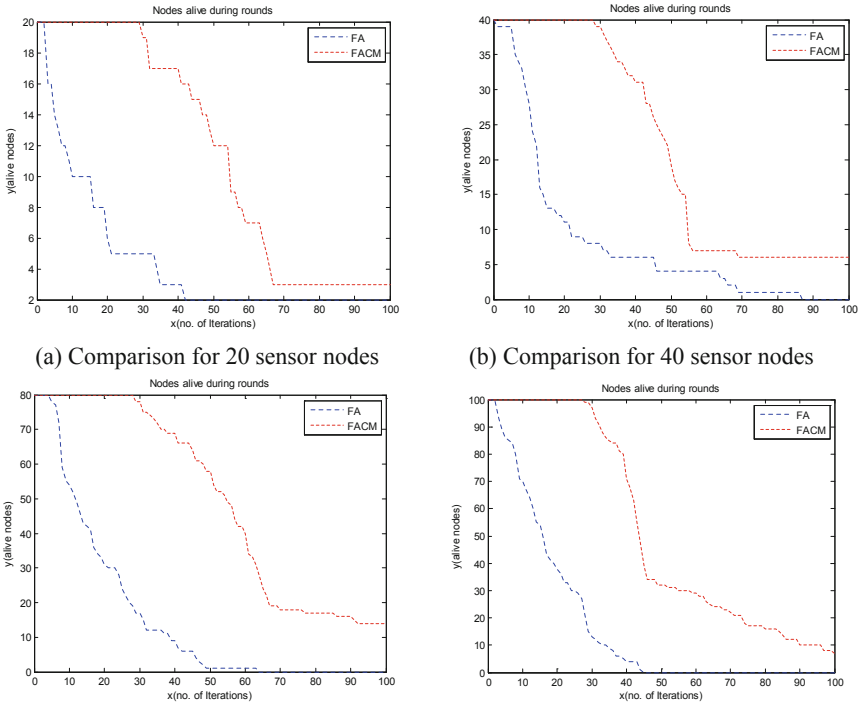


(c) Proposed Algorithm FACM

Fig. 6. 100 Sensor Node Displacement comparison between FA and FACM for 10 m × 10 m network area

The study reveals that the FACM algorithm shows better performance than classical FA varying node density case. For the comparison graph of 60 sensor nodes against 100 iterations according to their network lifetime is shown in Fig. 2(e). Figure 7 gives the number of nodes alive for both FA and FACM for constant 100 iterations with varying node density in 10 m × 10 m network area. Figures 7(a), (b), (c) and (d) gives the sensor node's life time comparison for node density 20, 40, 80 and 100 sensor nodes respectively.

The simulation results of *Experiment 1* and *Experiment 2* shows the efficiency in node displacement and network life time of proposed FACM algorithm as compared to classical FA while achieving the maximum connectivity within the network.



(a) Comparison for 20 sensor nodes

(b) Comparison for 40 sensor nodes

(c) Comparison for 80 sensor nodes

(d) Comparison for 100 sensor nodes

Fig. 7. Network life time comparisons for varying node density and for constant iteration

7 Future Thoughts

In near future, authors are planning to improve the connectivity management part of FACM algorithm. The proposed FACM algorithm checks for the higher energy neighbor node to establish connectivity and can be enhanced for maximizing the coverage part in the network field. However, in most complex environments, consumption of sensor node's energy is more important to keep the information for longer duration. Thus, defining a comprehensive method for energy consumption for critical environment is essential.

8 Conclusion

In this paper, maximum connectivity in WSN with minimal displacement was studied and accordingly a novel FACM algorithm has been developed for MWSNs. The proposed FACM algorithm explores and exploits the light flashing feature of insect firefly where a fitness function has been defined for deciding the brightness of the neighbor node considering two parameters namely *nearest neighbor in terms of distance* and *highest energy*; accordingly a fitness value will be defined for each neighbor

node. The sensor nodes gets attracted by other sensor nodes according to the fitness value defined for it. The proposed algorithm is implemented in MATLAB and a rigorous evaluation has been done. The results shows that the FACM algorithm performance better than classical FA algorithm.

References

1. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies, FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
2. Yick, J., Mukerjee, B., Goshal, D.: Wireless sensor network survey. Comput. Netw. **52**, 2292–2330 (2008)
3. Tuna, G., Gungor, V.C., Gulez, K.: An autonomous wireless sensor network deployment system using mobile robots for human existence detection in case of disasters. Ad Hoc Netw. **13**, 54–68 (2014)
4. Ghosh, A., Das, S.K.: Coverage and connectivity issue in wireless sensor network. In: Mobile Wireless and Sensor Network. Wiley (2006)
5. Obaida, M.S., Mishra, S.: Principles of Wireless Sensor Networks. Cambridge University Press, Cambridge (2014)
6. Hong, J., Cao, J.: Towards bio-inspired self-organization in sensor network: applying the ant colony algorithm. In: International Conference on advanced Information Networking and Application. IEEE (2008)
7. Yang, X.-S.: Nature Inspired Metaheuristic Algorithms. Luniver Press, Beckington (2010)
8. Manshahia, M.S.: A firefly based energy efficient routing in wireless sensor networks. Afr. J. Comput. ICT **8**, 27–32 (2015)
9. Sarkar, A., Senthil Murugan, T.: Cluster head selection for energy efficient and delay-less routing in wireless sensor network. J. Mob. Commun. Comput. Inf. **25**, 303–320 (2017)
10. Yadav, P., McCann, J.A., Pereira, T.: Self-synchronization in duty-cycled Internet of Things (IoT) applications. IEEE Internet Things J. **6**, 2068–2069 (2017)
11. Zahedi, Z.M., Akbari, R., Shokouhifar, M., Safaei, F., Jalali, A.: Swarm intelligence based fuzzy routing protocol for clustered wireless sensor networks. Expert Syst. Appl. **55**, 313–328 (2016)
12. Mills, K.L.: A brief survey of self-organization in wireless sensor networks. Wirel. Commun. Mob. Comput. **7**, 823–834 (2007)
13. Wang, Y., Zhang, Y., Liu, J., Bhandari, R.: Coverage, connectivity, and deployment in wireless sensor networks. In: Patnaik, S., Li, X., Yang, Y.M. (eds.) Recent Development in Wireless Sensor and Ad-hoc Networks. Signals and Communication Technology. Springer, New Delhi (2015)
14. Fei, Z., Li, B., Yang, S., Xing, C., Chen, H., Hanzo, L.: A survey of multi-objective optimization in wireless sensor networks: metrics, algorithms, and open problems. IEEE Commun. Surv. Tutor. **19**, 550–586 (2016)
15. Mohajerani, A., Gharavian, D.: An ant colony optimization based routing algorithm for extending network lifetime in wireless sensor networks. Wirel. Netw. **22**, 2637–2647 (2017)
16. Cheng, D., Xun, Y., Zhou, T., Li, W.: An energy aware ant colony algorithm for the routing of wireless sensor networks. In: Chen, R. (ed.) Intelligent Computing and Information Science, ICICIS 2011. Communications in Computer and Information Science, vol. 134, pp. 395–401. Springer, Heidelberg (2011)

17. Wang, X., Li, Q., Xiong, N., Pan, Y.: Ant colony optimization-based location-aware routing for wireless sensor networks. In: Li, Y., Huynh, D.T., Das, S.K., Du, D.Z. (eds.) Wireless Algorithms, Systems, and Applications, WASA 2008. Lecture Notes in Computer Science, vol. 5258, pp. 109–120. Springer, Heidelberg (2008)
18. Domínguez-Medina, C., Cruz-Cortés, N.: Routing algorithms for wireless sensor networks using ant colony optimization. In: Sidorov, G., Hernández, A.A., Reyes García, C.A. (eds.) Advances in Soft Computing, MICAI 2010. Lecture Notes in Computer Science, vol. 6438, pp. 337–348. Springer, Heidelberg (2010)
19. Hashim, H.A., Ayinde, B.O., Abido, M.A.: Optimal placement of relay nodes in wireless sensor network using artificial bee colony algorithm. J. Netw. Comput. Appl. **64**, 239–248 (2016)
20. Al-Turjman, F., Hassanein, H., Ibnkahla, A.: Efficient deployment of wireless sensor networks targeting environment monitoring applications. J. Comput. Commun. **36**(2), 135–148 (2013)
21. Kumar, R., Kumar, D.: Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network. Wirel. Netw. **22**, 1461–1474 (2015)
22. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd International Conference on System Science, HICSS 2000, Hawaii, USA, pp. 1–10 (2000)
23. Singh, B., Lobiyal, D.K.: A novel energy-aware cluster head selection based on particle swarm optimization for wireless sensor networks. Hum.-Centric Comput. Inf. Sci. (2012). https://doi.org/10.1186/2192-1962-2-13
24. Karaboga, D., Okdem, S., Ozturk, C.: Cluster based wireless sensor network routing using artificial bee colony algorithm. Wirel. Netw. **18**, 847–860 (2012)
25. Wang, J., Cao, Y., Li, B., Kim, H., Lee, S.: Particle swarm optimization based clustering algorithm with mobile sink for WSNs. J. Future Gen. Comput. Syst. **76**, 452–457 (2017)
26. Mot, S., Zahabi, M.: Optimizing LEACH clustering algorithm with mobile sink and rendezvous nodes. AEU - Int. J. Electron. Commun. (2014). https://doi.org/10.1016/j.aeue.2014.10.021
27. Luo, H., Ye, F., Cheng, J., Lu, S., Zhang, L.: TTDD: two-tier data dissemination in large-scale wireless sensor networks. Wirel. Netw. **11**(1–2), 161–175 (2005)
28. Wang, J., Cao, J., Sherratt, R.S., Park, J.H.: An improved ant colony optimization based approach with mobile sink for wireless sensor networks. J. Supercomput. **74**(12), 6633–6645 (2018)
29. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless micro sensor networks. In: Proceedings of the 33rd IEEE Hawaii Conference on System Sciences, pp. 1–10 (2000)
30. Wang, J., Cao, J., Li, B., Lee, S., Sherratt, R.S.: Bio-inspired ant colony optimization based clustering algorithm with mobile sinks for applications in consumer home automation networks. IEEE Trans. Consum. Electron. **61**(4), 438–444 (2015). https://doi.org/10.1109/tce.2015.7389797
31. Jagtap, A.M., Gomathi, N.: Minimizing movement for network connectivity in mobile sensor networks: an adaptive approach. J. Netw. Softw. Tools Appl. Cloud Comput. **22**, 1373–1383 (2018)
32. Jagtap, A.M., Gomathi, N.: A hybrid approach using Voronoi partition and swarm intelligence. Bull. Polish Acad. Sci. Tech. Sci. **65**(2), 263–272 (2017). https://doi.org/10.1515/bpasts-2017-0030
33. Ray, A., De, D.: An energy efficient sensor movement approach using multi-parameter reverse glowworm swarm optimization algorithm in mobile wireless sensor network. Simul. Model. Pract. Theory **62**, 117–136 (2016)

34. He, L., Tong, X., Huang, S.: A glowworm swarm optimization algorithm with improved movement rule. In: Proceedings of the 5th International Conference on Intelligent Networks and Intelligent Systems, ICINIS 2012 (2012)
35. Eldrandaly, K., Abdel-Basset, M., Abdel-Fatah, L.: Grid quorum-based spatial coverage in mobile wireless sensor networks using nature-inspired firefly algorithm. Expert Syst. e12421 (2019). https://doi.org/10.1111/exsy.12421
36. Mirjalili, S., Lewis, A.: The whale optimization algorithm. Adv. Eng. Softw. **95**, 51–67 (2016). https://doi.org/10.1016/j.advengsoft.2016.01.008
37. Ismail, W.W., Manaf, S.A.: Study on coverage in wireless sensor network using grid based strategy and particle swarm optimization. In: 2010 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), pp. 1175–1178. IEEE, December 2010. https://doi.org/10.1109/apccas.2010.5775080
38. Yang, X.S.: Flower pollination algorithm for global optimization. In: Durand-Lose, J., Jonoska, N. (eds.) Unconventional Computation and Natural Computation, UCNC 2012. Lecture Notes in Computer Science, vol. 7445, pp. 240–249. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32894-7_27
39. Lu, X., Cheng, W., He, Q., Yang, J.: Coverage optimization based on improved firefly algorithm for mobile wireless sensor networks. In: IEEE 4th International Conference on Computer and Communications (2018)
40. RSFA. https://github.com/ShangruZhong/Firefly_Algorithm_WSN
41. Tuba, E., Tuba, M., Beko, M.: Mobile wireless sensor networks coverage maximization by firefly algorithm. In: IEEE Conference Radioelektronika (2017)
42. Alfakih, A.Y.: Euclidean Distance Matrices and Their Applications in Rigidity Theory. Springer, Cham (2018)
43. Lalwani, P., Ganguli, I., Banka, H.: FARW: firefly algorithm for routing in wireless sensor networks. In: International Conferences on Recent Advances in Information Technology. IEEE (2016)
44. Matsumoto, Y., Fujiwara, A.: A firefly optimization for a connected dominating set in a sensor network. In: IEEE Symposium on Computing and Networking, pp. 594–596 (2017)
45. Tuba, E., Tuba, M., Simian, D.: Wireless sensor networks coverage problem using modified by fireworks algorithm. IEEE (2016)
46. Hong, J., Cao, J.: Towards bio-inspired self-organization in sensor networks: applying the ant colony algorithm. In: IEEE Advanced Information Networking and Application, pp. 1054–1061 (2008)
47. Łukasik, S., Żak, S.: Firefly algorithm for continuous constrained optimization tasks. In: Nguyen, N.T., Kowalczyk, R., Chen, S.M. (eds.) Computational Collective Intelligence. Semantic Web, Social Networks and Multiagent Systems, ICCCI 2009. Lecture Notes in Computer Science, vol. 5796, pp. 97–106. Springer, Heidelberg (2009)
48. Zhang, Z., Long, K., Wang, J., Dressler, F.: On swarm intelligence inspired self-organized networking. IEEE Commun. Surv. Tutor. **16**, 513–537 (2013)

Energy Conscious Packet Transmission in Wireless Networks Using Trust Based Mechanism: A Cognitive Approach

Anshu Bhasin(✉), Sandeep Singh, and Anshul Kalia

IKG Punjab Technical University, Kapurthala, India
Dr.anshubhasin@ptu.ac.in, Sandeep_madda@yahoo.co.in,
Anshul172l5@ctuniversity.in

Abstract. The self-motivated nature of wireless ad-hoc networks deters the possibility of a centralized solution. Also, no specific node can act as a centralized point due to energy and processing constraints. Constraint of non-centralization demands efficient and effective transmission of data between nodes by sharing information whenever needed without any disruption. This co-operation is a prodigious challenge due to the presence of covetous and malicious nodes in the network. Hence, an asserted need of some lightweight trust based mechanism in differentiating among reliable and unreliable nodes arises. This mechanism enhances security and improve co-operation in nodes. Energy efficiency remains central to the above segregation. Many trust-based methods are proposed which use packet delivered ratio as the major parameter for direct trust calculation. This work presents investigation of other related parameters like routing overhead, energy level etc. which can increase the effectiveness of trust based mechanisms for early detection of malicious nodes along with packet delivered ratio. Furthermore, an ameliorated energy optimization model is proposed for wireless network.

Keywords: Wireless ad-hoc networks · Routing · Attacks · Energy · MANET

1 Introduction

Wireless systems are extensively in use for communication nowadays. Wireless systems have various characteristics like scalability, dynamic topology, low cost, easy setup, mobility, high user density, multi hop wireless transmission and convenience [1]. In ad hoc setup, nodes can move in or move out from the network at any time, causing the topology to change quickly and unpredictably. Each node in the ad hoc setup has to work as a transmitter and a receiver. All nodes are in authority to create, operate and maintain the ad hoc network. Wireless systems can be categorized into two types - the infrastructure based wireless networks and the infrastructure-less wireless networks (ad hoc networks).

MANET is an interconnected system of wireless networks that can be designed quickly and dynamically without requiring any additional external router or access point [2]. MANET is also sometimes referred as Self-Organizing Networks (SONs) [3].

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 218–238, 2020.
https://doi.org/10.1007/978-3-030-40305-8_11

The nodes themselves behave like a router. Its dynamic and ad-hoc nature deters the possibility of a centralized solution. In addition, no specific node can act as a centralized point due to energy and processing constraints [1].

MANET is mobile in the sense that all the nodes keep on moving and thus the network topology is highly dynamic in nature [4]. So, the protocols must be adjusted as a node enters or leaves the network. It is Ad-hoc in the sense that the network works in accordance with the demand and current scenario with all the paths being made spontaneously.

The communication between two nodes is feasible only when the nodes are within the range of each other; else communication is possible with inclusion of intermediate nodes. It uses multi hop wireless transmission that requires two or more hops to transfer the information from the source to the destination [5]. In a multi-hop network, every node has to take part in routing process and each node can act as an intermediate node.

In recent years, wireless networks have gained in popularity due to their interesting applications in military and civilian, emergency rescue, ecological observing, and commercial innovations [17]. Energy consumption and security are actively researched areas in ad- hoc networks due to their special features like autonomous, dynamic topology, multi hop wireless transmission [6].

2 Routing

The ad hoc network routing protocols aims at finding the shortest and most reliable paths in a network. The prime goal of routing protocol is the establishment of a precise and efficient route in the network, so that sender can send packets to the destination in the shortest and most secure manner [7]. Routing should involve minimum resources, such as overhead and bandwidth consumption. The additional challenges combined with routing protocols to setup a path among the nodes makes it the most actively researched area [18]. The routing protocols in ad-hoc systems can be categorized into network organization, protocol operation and route discovery. The network organization includes flat based, hierarchical based and location based protocols. The hierarchical based includes multipath, query, QoS and coherent based routing protocols. The route discovery protocols can be classified according to their routing operation i.e. reactive, proactive, and hybrid routing. Classification of routing protocols is shown in Fig. 1.

Reactive routing algorithms have less computational overheads as nodes are not required to maintain a path from them to all other nodes, but are meant to generate the best route when required.

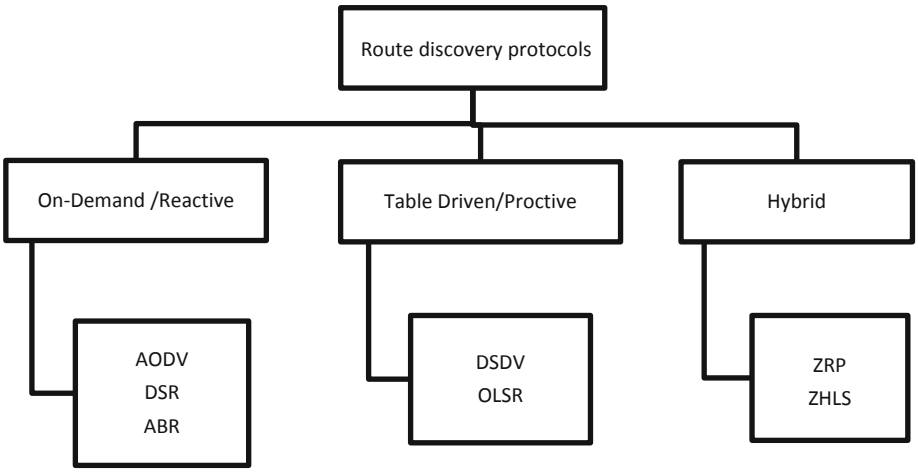


Fig. 1. Various types of routing

2.1 Reactive Routing

Reactive routing is also recognised as the on-demand routing protocol. Reactive routing algorithms have less computational overheads because they do not maintain the routing information in advance for all the nodes. They only update the routing information when one or more nodes are interested in communication, in such a case the protocol finds the route to a particular node. This indicates that the reactive routing protocol works on demand basis. Reactive routing finds the path information through distance vector routing algorithm.

Reactive protocols are appropriate for networks where the nodes have higher node mobility and transmit data infrequently. Reactive routing protocol out performs proactive routing protocol in terms of network throughput and routing overhead [8]. Ad-hoc on-demand distance vector (AODV) and dynamic source routing (DSR) are two well-known reactive routing protocols. The main shortcomings of reactive routing protocol are:

- High latency time in route finding.
- Excessive flooding leading to network clogging.

2.2 Ad-hoc On-demand Distance Vector (AODV)

AODV protocol was basically proposed as a protocol to be adapted by the nodes in ad-hoc networks [9]. It is one of the important routing protocols in ad-hoc networks. It has many features like easy installation, non-existence central authority, no fixed

infrastructure and many more. AODV is low-memory and processing load-consuming algorithm for providing routes between nodes. It can determine the best path from the source to destination in an ad-hoc network. In AODV a routing table is available with every node. The table has the route from the source to destination. When two or more nodes are interested in data transmission, the AODV protocol explores and setup route between nodes. AODV is a distance vector routing protocol. It uses the concept of destination sequence number and hop counts in order to devise a feasible route. The nodes which are not selected for the path, they do not keep up the routing table and therefore AODV is categorized as a pure on-demand routing protocol. The AODV routing protocol shows an excellent packet arrival rate, however it suffers from various types of security problems.

The destination sequence number is produced by the target node when a path is requested. Sequence number is the measure of freshness. The higher the destination number, the fresher is the route [4]. While hop count suggests the number of intermediate nodes a message must encounter before reaching the destination from the source, it offers finest and safe communication to send the data from the source to destination.

AODV broadcasts four different types of packets namely path request (PREQ), path reply (PREP), HELLO and route error (RERR). PREQ is broadcasted when creating a new route among the source and target. When target node receives PREQ, it drives the PREP message to the source. The sender sends the HELLLO message to the destination to check the current route. When the recent path testing fails RERR message is sent [9].

2.3 Dynamic Source Routing Protocol (DSR)

DSR is another on demand routing protocol which is designed for multi-hop ad-hoc networks. DSR works in two phases known as “Route Discovery” and “Route Maintenance”. Route discovery phase finds the path from the source to the destination and accumulates the complete information about the route in its header. When a route is discovered, route reply is sent by the destination. If no path is found from the source to the destination then the error message is generated.

The dissimilarity between DSR and AODV is that DSR not only records next hop information, but also maintain the route cache in the routing table. AODV records next hop information only [10].

2.4 Proactive Routing

This protocol is also known as the table-driven routing protocol. It maintains current and uniform routing information proactively. In proactive routing a node is required to maintain its routing tables as topology changes [11]. The routing table of a node contains information such as adjacent nodes and reachable nodes. When a node leaves or joins the network, then the updated information is shared in the network. All nodes update their routing tables according to the shared information. Optimized Link State

Routing (OLSR) and Destination Sequence Distance Vector (DSDV) are two eminent proactive routing protocols.

The link state routing has the advantage of fast convergence over distance vector routing. However, it needs more control traffic. When the network scale increases, the routing overhead increases due to more routing information from mobile nodes. Proactive protocols are most suited for networks having lower movement or higher data transfer rate. The major shortcomings of these algorithms are:

- Relevant amount of data for maintenance.
- Slow response to restructuring and failures.
- Short Life span of a link.
- If the nodes transmit intermittently, most of the routing information is redundant.

2.5 Destination-Sequenced Distance-Vector Routing (DSDV)

DSDV is a proactive or table driven routing protocol. DSDV is the most effective protocol as compared to other protocols in the category of table driven routing protocols [8]. Bellman ford algorithm is used to find the shortest route from the existing set of routes. In this protocol; each node periodically shares its routing information with its neighbors. The Path sequence number is used to find the best route. The routing table is renewed when the source node has the greater sequence number than the existing path. The DSDV is limited by more bandwidth consumption and non-support for multiple routing [8].

2.6 Hybrid Routing

Hybrid routing protocols integrates the feature of reactive protocol and proactive protocol. The fundamental idea of hybrid technique is to use proactive routing in the particular portion of the network at particular times and reactive routing in the remaining network. The proactive actions are confined to a small area to lessen the control packet overheads and delays; on the other hand, the reactive protocols are utilized for discovering nodes outside this area, as it is more bandwidth efficient.

A hybrid protocol starts with proactive routing to find zone neighbours and reactive approach to find routes among zones. The neighbouring zone is updated frequently by sending ‘hello’ packets to the neighbours to check whether they are active or not. In hybrid protocols, paths to neighbour’s are immediately available when need [11]. Two well-known Hybrid routing protocols are zone routing protocol (ZRP) and zone based hierarchal link state (ZHLS) routing protocol. The main drawbacks of such algorithms are:

- Performance depends on the number of nodes activated.
- Response to traffic depends on traffic volume.

2.7 Zone Routing Protocol (ZRP)

ZRP is a hybrid protocol as it combines the features of proactive and reactive routing protocols [8]. Reactive protocol is an on-demand protocol which finds the route from the source to destination when there is a requirement. Proactive protocols store the information about each path in the form of tables.

3 Attacks

The network layer in ad-hoc network is susceptible to numerous kinds of security attacks. Standard routing algorithms are not planned to handle such kinds of attacks. Security is a challenging issue in wireless ad-hoc networks because intruders can easily disturb the routing protocols [12]. Any untrusted node can become the part of the network easily due to the absence of centralized control. Such nodes are known as malicious nodes. The malicious node(s) can attack the network using dissimilar techniques, for example, by sending bogus packets a number of times, false routing information, drop the packets, false advertising to disrupt routing processes. The main challenge in the ad-hoc networks is to decrease the attacks triggered by malicious nodes or to detect malicious nodes at an initial phase.

Researchers are using various techniques to prevent and secure the network from these attacks. Some of them are using destination sequence number, some others are using cryptography mechanism, some of them used trust-based mechanism, and some of them used IDS and many more.

3.1 Black Hole Attack

In a Black hole attack [13], a malicious node drives fake routing information in the network, claiming that it has the best route during the route request phase by sending a high sequence number. The sequence number is a metric to determine the newness of the route. A high sequence number denotes the freshness of the route. It also reduces the hop count to the lowest value to show that their route is the shortest route from the source to the destination. The sender believes the malicious node and then creates a route through that node. All the packets are then transferred through that node and the node has the power to do whatever it wants with the packets. In a black hole attack the malicious node mostly drops the packets sent through it [14]. Black hole is an active kind of attack that significantly reduces the data route security.

3.2 Co-operative Black Hole Attack

In Co-operative black hole attack [15], two or more malicious nodes work in group to violate the routing protocol, i.e. collaborate to abrupt packet relaying by forwarding them to each other and then dropping the data packets to disrupt routing. Co-operative black hole attack is shown pictorially in Fig. 2.

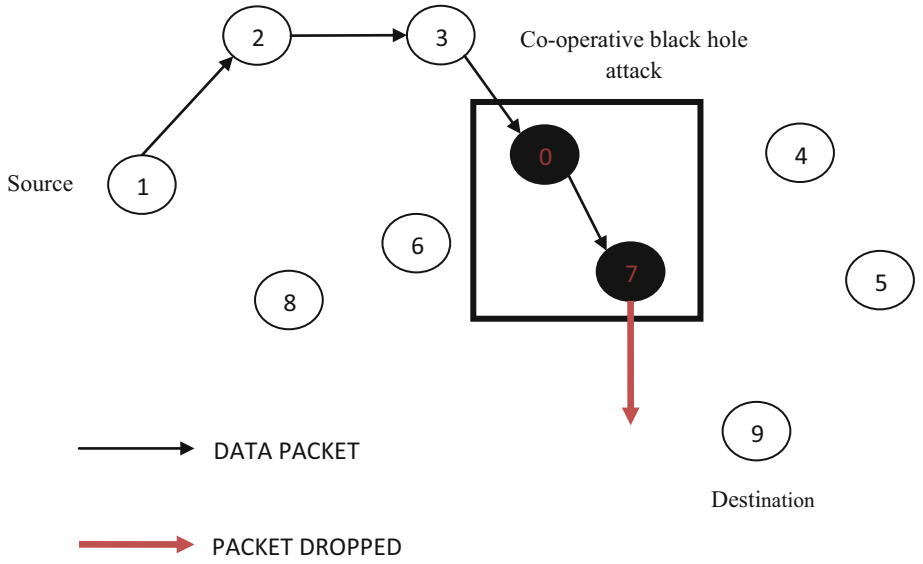


Fig. 2. Co-operative black hole attack

3.3 Flooding Attack

In flooding attack [16], an attacker can drain the network resources, such as bandwidth, computational and battery power. It may disturb the routing process to cause severe degradation in network performance.

3.4 Rushing Attack

In rushing attack [13], the attacker after receiving the RREQ packet from source or any intermediate node quickly floods the RREQ packets to its neighbor. As a result, the route from source to destination is bound to have the attacker node. This type of attack is common in reactive routing protocols where route discovery is done on demand.

3.5 Gray Hole Attack

In Gray Hole attack [13], the malicious node selectively drops the data packet sent to it by its previous hop. It is a very crucial attack as it cannot be easily detected through mechanisms like watchdog. The attacker drops only a certain number of data packets in such a manner that its counter of drop packets should not exceed or reach the threshold limit to declare it as a black hole by the watchdog mechanism.

3.6 Sybil Attack

In Sybil attack [16], an intruding node tries to forge the identity of another node and if it succeeds in doing so it will cause real damage to integrity, confidentiality and security of data. This attack is implemented by stealing important information that is vital in performing node(s) authentication.

3.7 Sleep Deprivation

In sleep deprivation attack [13], the resources like battery power, processor, etc., of a particular node or a cluster of nodes in the network are consumed by attacking nodes by keeping them busy in finding routes to unknown or non-existent destinations. In such a way they waste their neighbor's power by making them process and forward these packets that will ultimately lead to nothing.

3.8 Worm Hole Attack

A wormhole attack is one of the most refined and severe attacks in MANETs [16]. In this attack, a number of conspiring nodes record packets at one place and replay them at another place using a private high-speed network. The severity of this attack is that it can be introduced against all transmissions that have a provision for authenticity and confidentiality. Worm hole attack is shown pictorially in Fig. 3.

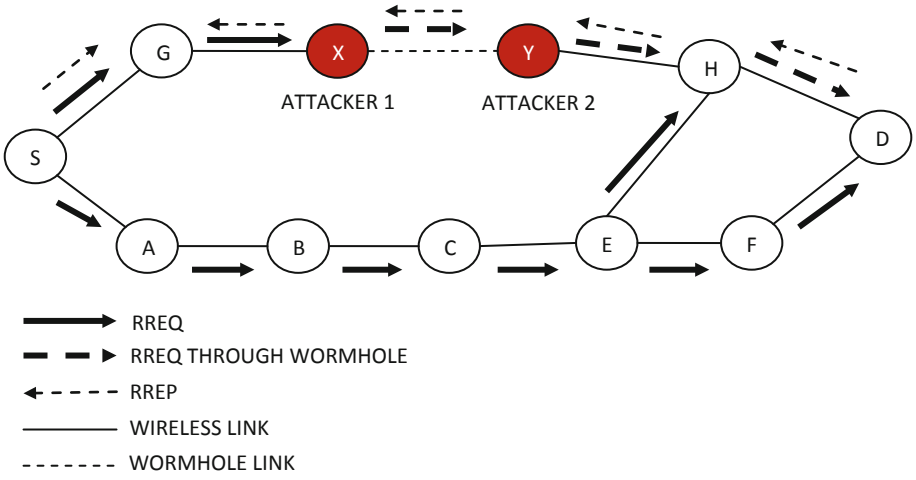


Fig. 3. Worm hole attack

Thus, we have learnt that ad-hoc networks are vulnerable to routing and data security attacks. Out of all these attacks, packet drop attacks are very severe, in the presence of which the ideal network is very difficult to attain.

4 Related Work

In [19] authors propose EATSRA, which has less energy consumption and provides enhanced security and improved packet delivery ratio. This mechanism used packet drop ratio, number of acknowledgements sent to neighbors, residuals energy along with temporal and spatial constraints for trust calculations. The distance between two nodes is compared with a defined threshold to establish a path between them. The detection of

malicious nodes is done by packet delivery ratio or when the trust drops below a certain well-defined threshold. Use of temporal and spatial constraints helps in better stability of links. Actual packet delivery ratio is not used for trust calculation. Acknowledgements are only used for trust calculation that can be dropped even for delivered packet.

This mechanism [20] is named as TSQRS in which authors propose a trust-based routing scheme by merging social and QoS parameters like residual energy, channel quality, link quality, etc. Hello Messages are modified for exchange of trust value. QOS based links are generated according to the need and required level of trust. Use of QOS parameters provides adaptability and effective use of resources with improved security and quality of service routing in terms of overhead, packet delivery ratio and energy consumption. Authors have also suggested the inclusion of software agents and intelligent agents for future research. This is a total prevention approach with no measures for detection of the malicious node.

In [21] this mechanism direct and indirect trust is considered along with energy saving issue to propose a trust-based mechanism. The routing table is optimized using a gravitational search approach. This routing method is called Energy-aware Trust-based Gravitational Search Approach (ETGSA). The node selected must satisfy the desire level of trust which is calculated using PDR. It selects the best route according to the trust, energy, Number of hops and traffic rate of routes. Due to the multipath nature of the scheme less route discovery is needed. The residual energy of the nodes increases significantly because of the less number of control packets sent and less route discovery process. The route established phase using trust value is more robust. It does not incorporate historic Trust. The node mobility does not affect the results. This method levies overhead to the network.

In [22] authors proposed an ESCT scheme that matches human cognitive process and depend on trust information to prevent attacks. In this scheme the nodes calculate the trust value on the basis of PFR and make judgment regarding the malicious node on the basis of their own cognitive judgment. The nodes can co-operate with each other to detect the most intelligent attack like grey hole by maintaining & exchanging sending history record (SHR), receiving history record (RHR), self-analysis record (SAR), neighbour judgment record (NJR), trust information record (TIR). Self-detection and cooperative detection schemes are used to improve the performance of the method. Furthermore, voting scheme in cooperative detection is used so that malicious nodes cannot increase their trust mutually. Co-operation detection provides better isolation of malicious nodes. Only PFR is used for trust calculation.

The mechanism [23] is named as TBRS. It calculates trust of a node on the basis of PDR and position of neighbor's. It uses the KNN approach to filters the paths. Direct trust is computed through the delivery ratio. It can fine-tune the weight coefficient of direct trust parameters. The cooperative computation model for trust calculation is used to filter untruthful recommendation trust values. If the trust value falls below the certain threshold the malicious node gets detected. The use of position of node provides better link stability. The use of GPS for finding the position of a node consumes more power.

This mechanism [24] used grey relational analysis theory and Fuzzy logic to calculate the nodes trust. The calculated trust is then used for decision making in routing. This mechanism is compared with different variants of AODV (Ad-hoc on-demand distance vector) on the basis of PDR (packet delivery ratio), Delay, and throughput.

This mechanism helps in establishing the most optimal path with little to no chance for attacking node. However, this protocol's implementation is dependent and cannot adapt to the dynamic needs of the network.

This mechanism [25] involves the cluster of different sizes in the network in which cluster heads maintain the trust value for other cluster heads and members of the cluster. On the basis of forwarding nature and recommendation from other cluster heads final trust is calculated. If the threshold falls below a threshold value the node is termed as malicious and marked as attacking node. For the secure and stable communication group key management process is used. To maintain the confidentiality, the group key management is used by all the intermediary heads. This mechanism provides authentication and confidentiality. However, the trust module is not robust as it can lead to the false positive or true negative. This mechanism is compared with their previous work on the basis of delay, packet drop ratio, and throughput.

This mechanism [26] is named as TRAB-IDS. It is a hybrid approach that uses Intrusion detection along with trust values and cryptography. It involves a Deep Packet Inspection Algorithm that differentiates a data payload from control traffic. Key generating and certificate authority is used along with trust values to provide authentication that too with reliability. Basically, processes like key generation and distribution, signature-based verification, key exchange verification and error reporting after attack detection techniques are involved to make the mechanism robust. The use of trust and cryptography makes the intrusion detection procedure more accurate and decreases the false positive. However, high computational overhead causes more energy dissipation and it is difficult to set up such architecture with high end nodes that can act as Certificate Authority.

This mechanism [27] is named as ReTEAODV. The Bayesian probability is used for refinement of trust calculation. Both direct and indirect trusts are used to get the final trust. Packet delivered ratio is used as the main parameter for direct trust. Energy and final trust are used to check the trustworthy of the route formed. The routing process includes both the route discovery phase and route maintenance phase. This mechanism is compared with their previous work on the basis of packet delivered ratio, Routing packet overhead, Energy consumption and average end to end latency. Energy consumption is more in this scheme.

This mechanism [28] is named as DATEA. In this method various types of trust are used like direct trust, communication trust, indirect trust, and historical trust. Communication trust is calculated using forwarding ratio. Final trust is calculated using direct trust and indirect trust. Recommendation trust is based on the reliability factor. The Adaptive weighting method is used to assign weights to all trust components. Indirect trust is calculated on the basis of trust propagation distance. This method uses also predication technique to predict trust. This method can effectively detect malicious nodes in the network. However, this algorithm puts more computation overhead to calculate trust.

This mechanism [29] is named as TeAOMDV. This method uses a decentralized trust reference model. The fuzzy AHP scheme is used to assign weights to different parameters in direct trust. It provides security with additional computation overhead. AOMDV (ad-hoc on demand multipath distance vector protocol) is used in this scheme. It uses only passive and local monitoring information to evaluate the behavior of interest nodes. It also uses indirect and historical trust. A matrix is defined at each

node helps in quick calculation for trust values. This mechanism used various parameters like packet delivered ratio, Routing overhead, average end to end latency, route discovery frequency and number of malicious nodes.

Based on above discussion of related work Table 1 shows the summary of trust based systems and Table 2 covers the contributions and gaps of these trust based systems.

Table 1. Summary of trust based mechanisms

Proposal method	Protocol	Indirect trust	Historical trust	Modification in protocol	Trust parameters	Simulator
EATSRA	LEACH	No	Yes	Yes	Packet drop Ratio, energy, number of acknowledgements	NS2
TSQRS	AODV	No	Yes	Yes	Residual energy	NS2
ETGSA	AODV	Yes	No	Yes	PDR	NS2
ESCT	DSR	Yes	No	Yes	PFR	NS2
TBRS	AODV	Yes	No	No	PDR	One simulator
F-AODV	AODV	Yes	Yes	Yes	PDR	NS2
IDSGKM	Wireless protocol	Yes	No	No	PDR	NS2
TRAB-IDS	–	Yes	No	No	PFR	NS2
RETE-AODV	AODV	Yes	No	No	PDR	QUALNET
DATEA	ZRP	Yes	No	No	Packet drop ratio, packet forwarding ratio, energy	MATLAB
TEAOMDV	MAODV	Yes	No	No	PFR	NS2

Table 2. Summary of contributions and gaps in trust based mechanisms

Proposal method	Contributions	Gaps
EATSRA	Temporal and spatial constraints helps in better stability of links	Actual packet delivery ratio is not used for trust calculation
TSQRS	Use of QOS parameters provide adaptively and effective use of resources	Totally prevention approach with no measures for detection of malicious node
ETGSA	The route established phase using trust value is more robust	It does not incorporate historic trust
ESCT	Co-operation detection provides better isolation of malicious nodes	Only PFR is used for trust calculation
TBRS	Use of position of node provide better link stability	Use of GPS for finding the position of a node consumes more power
Favorite-AODV	Helps in establishing the most optimal path	Non adaptive
IDSGKM	Provide authentication and confidentiality	False positive and true negative
TRAB-IDS	Use of IDS with cryptography helps in accurate detection	High computational overhead causes more energy dissipation
RETE-AODV	Energy consideration in path formation	Only PDR is used for trust calculation
DATEA	Strong mathematical model	Difficult to implement
TEAOMDV	Efficient trust estimation	True negative

5 Challenges

MANET has a dynamic infrastructure and due to the mobile nature of its nodes it lacks static logical topology. The open communication features and limited energy resources created many challenges in MANET. For transmissions in MANET; co-operation amongst nodes in the MANET is required. In MANET, nodes act as intermediate nodes for other nodes so that information can be communicated from the source node to destination node. For efficient and effective transmission of data between nodes, every node must co-operate with each other by sharing information whenever needed without any disruption. Also, as MANET is a wireless multi hop network, there is a need that all the nodes do not misuse the information that they are capturing, storing, and forwarding. The nodes must be reliable and co-operative.

However, this co-operation is not easy to achieve and if achieved is not easy to rely upon for safer communication if proper measures are not taken. This is due to the presence of some nodes in the network that may act selfishly or act maliciously to obtain information not intended for them or interrupt actions of other nodes for some selfish reasons.

However, this problem can be sorted out by using the mechanism of co-operation and isolating nodes that are dropping packets selfishly. Also, no node should send sensitive information through a multi hop network as such. So, there is a need to use some mechanism that will transform sensitive information into a form that is of no use for intermediaries. Apart from that, all these mechanisms should not produce overheads in networking and should not consume a better part of their resources.

So, there is a need of some energy conscious mechanism to be implemented in nodes of MANET that will help them in differentiating among reliable and unreliable states. They should take preventive as well as corrective actions to avoid unreliable state. For preventive measures, trust-based mechanism proves to be best in countering both active and passive attacks. For corrective actions, each node should implement some mechanism in which it distinguishes a reliable node from a selfish node. This helps in maintaining reliability and efficiency of MANET. Even after forming a sound mechanism, it is of no use if it consumes a lot of energy of nodes. So, the mechanism must be energy efficient in its implementation.

Hence, it can be stated that “Energy conscious packets transmission in wireless networks using trust based mechanism” can be one of the solutions for mitigation packet drop attacks in an effective manner.

6 Why Trust

Security can be enhanced effectively in ad-hoc networks by introducing the concept of trust. The word trust comes from the social sciences where it is used to represent relations among individuals, entities, objects or actions. Trust based methods are gaining more acceptances in securing wireless ad-hoc networks above other detection

systems (like firewalls, key management, cryptography, IDS based mechanism, watchdog, or routing based mechanism). Trust mechanism does not need any hard encryptions and hashing techniques as used in cryptography solutions. Trust mechanism provides security in a much better way because of its preventive nature, improved cooperation, accuracy and robustness, ease of implementation, integration, flexibility and scalability. The trust based approach provides a system where we can continuously observe the performance and behavioural patterns of neighbouring nodes in the network. To make it clearer, the authors of [30] have suggested some other profits of using Trust based mechanism, they are listed below.

- A Trust based mechanism provides various steps of access control on the basis QoS parameters delivered by the evaluated node.
- A Trust based mechanism supports in the detection and isolation of malicious nodes.
- The Trust based mechanisms also ensures that only trustworthy nodes contribute in the authentication and authorization process during communications.

The trust [31] of a node expresses the character of a node, which is based on experiences of a node's observed conduct over a period of time. Trust can be direct, indirect or historical. Direct trust is computed based on direct sincerity of a node with its direct neighbours. Indirect trust is gathered from the other nodes in the network. In trust based mechanisms, the neighbouring nodes are assessed on the foundation of their previous routing performance and behaviour. The nodes having higher trust values are selected to form routes because they have a better possibility of successful routing. The nodes having lesser trust values can be considered as malevolent or selfish nodes. The trust-based mechanisms are not limited in detection and isolation of malicious nodes in the network; it can be applied to other research areas such as routing, security against various network layer attacks, selection of designated nodes, QoS, data aggregation, authentication, and authorization.

Direct trust can be calculated using multiple parameters, instead of a single parameter. Direct trust can also include historical trust into calculation if there is no recent activity between the two nodes. If the calculated direct trust value falls below the predefined threshold value, then the node will be moved to the list of malicious nodes. Otherwise, we will get indirect trust based on the recommendations to get final trust. After obtaining final trust it is again compared with the predefined threshold value. If final trust is below the threshold, then the node will be moved to the list of malicious nodes. All other nodes having greater trust value can take part in the communication process. The flow chart of above discussion is shown in Fig. 4.

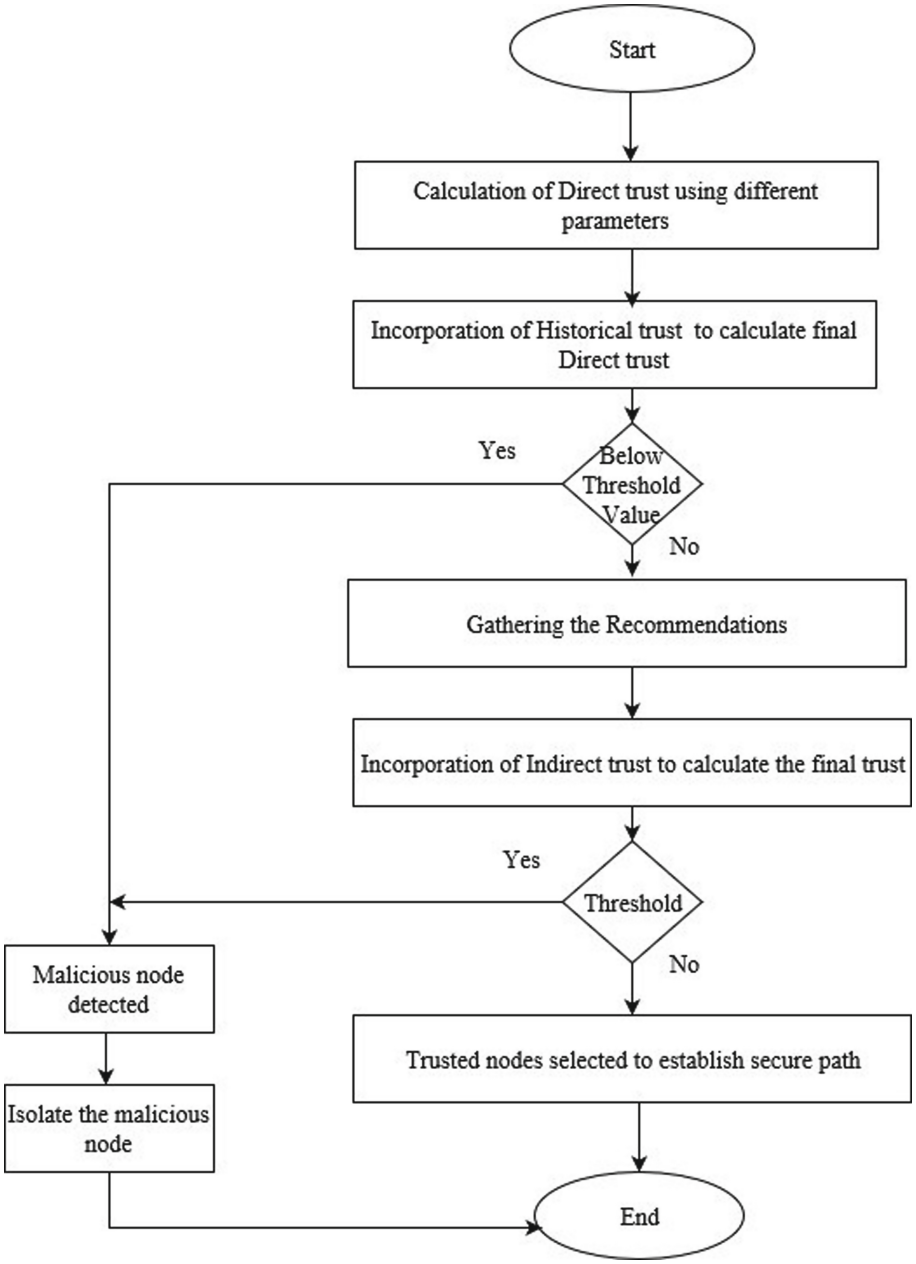


Fig. 4. Naïve trust calculation flow diagram

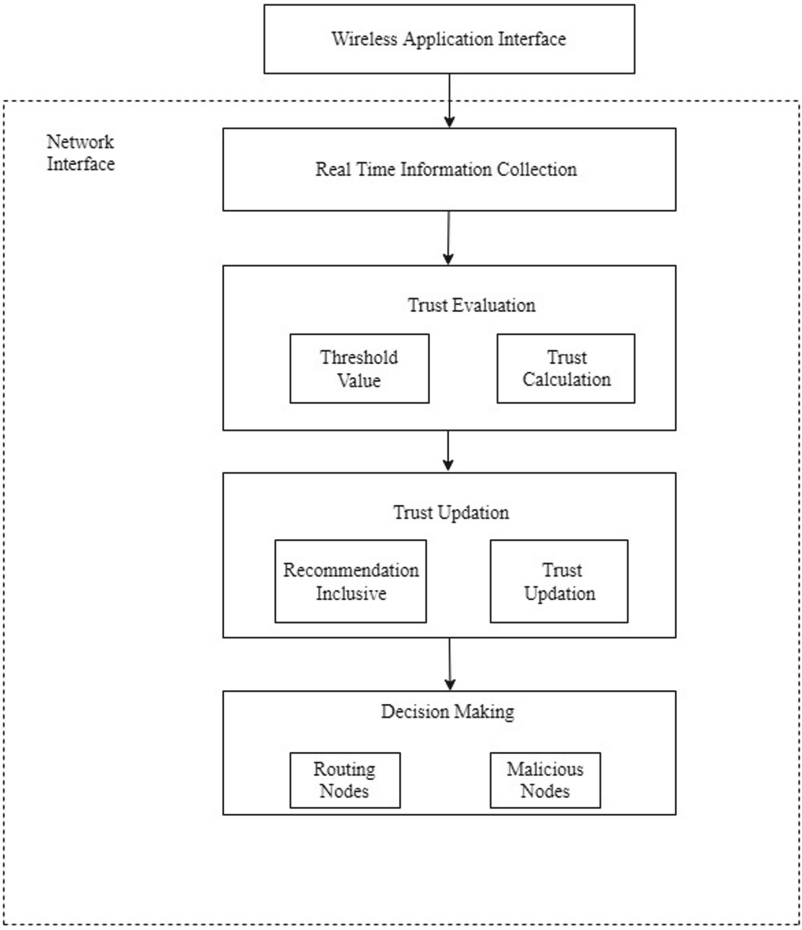


Fig. 5. Trust based framework for mitigation of malicious nodes.

Stimulating issues with the trust based approach (Fig. 5) *are as follows:*

- Most of the studies only use packet delivered ratio for trust calculation.
- Most of the Trust based mechanisms lack inappropriate weight harmonizing among different parameters for trust calculation and also in current and past trust values.
- Attaining a nodes trust is a challenging task, so energy exhaustion is more with trust based systems, which can affect the lifespan of the set-up.
- Some context-aware mechanism is required in which different trust attributes and their weights can be adjusted automatically.
- The secure routing is an important issue in the trust based systems, because trust based systems don't backup routing facts or routing movement in the network nodes if there is no communication.

- The future research can be focused to expand the present-day trust mechanisms. Mostly present solutions use single attribute trust and fixed weighted trust. So there is an option to work on multi trust metrics.

7 Different Parameters for Trust Calculation

7.1 Packet Delivery Ratio (PDR)

It is the main parameter in trust calculation methods and used by many researchers, because most of the attacks try to discard the packets. PDR is based on end to end transfer of the data packets and can be attained using acknowledgement based methods. The Formula to calculate the Packet delivery ratio is given below:

$$Packet\ delivery\ ratio = \frac{No : of\ Packets\ forwarded\ by\ a\ node}{No.\ of\ Packet\ Received\ by\ a\ node} \times 100$$

7.2 Packet Forwarding Ratio (PFR)

It deals with the forwarding of data packets to neighbouring nodes and not about real delivery of data packets to the target node. This means acknowledgements are not considered in this parameter [32]. The Formula to calculate the Packet forwarding ratio is given below:

$$Packet\ forwarding\ ratio = \frac{\text{No: of } Packets \text{ forwarded to a node}}{No.\ of\ Packet\ sent\ to\ a\ node} \times 100$$

7.3 Residual Energy

It is the main parameter in trust calculation and researchers used it very less as compared to Packet delivery ratio. When a node sent or receives the packets or when a node attends traffic of neighbouring nodes, energy of a node is used. The residual energy is the balance energy left with the node after performing a number of transactions in terms of packets sent or received. This parameter can be used to detect a malicious node because a malicious node can have lower residual energy due to its hyper activity.

$$\Delta E_i = E_{I_i} - E_{C_i}\ i = 1, 2, 3, \ldots, n$$

Where ΔE_i = Total Energy consumption by each packet,

E_{I_i} = Initial energy,

E_{C_i} = Current energy

7.4 Packet Integrity

It deals with the integrity of packets delivered, means the packets are not altered. The Formula to calculate the packet integrity is given below:

$$Packet\ integrity = \frac{\text{No: of } Packets \text{ forwarded unchanged}}{No.\ of\ Packet\ sent} \times 100$$

7.5 No of Control Packets Sent

There are three kinds of packets namely: data packets, network management packets and control packets. Control packets are primarily used to establish and tear down the session. Control packets consume bandwidth, so control packets can also be a parameter for trust calculation.

No. of control packets sent = PREQ + PREP + HELLO +RERR

Where PREQ (path request), PREP (path reply), and RERR (route error).

7.6 CPU Usage

The malicious node is always an active node, so it is using its resources more like CPU. The inclusion of this parameter in trust calculation can have a great impact in detection of the malicious node(s).

8 Energy

Energy is the most important component in Ad-hoc networks. Energy consumption should be as less as possible so that wireless nodes can work for more duration. It should be noted that, the communication mode in ad-hoc networks drains more energy than the computation and sensing modes. So there is a need to develop an efficient routing protocol for ad-hoc networks which consume less energy for transfer of packets. The following points are important to save energy.

- Energy required to transfer the packets among nodes can be decreased by increasing the number of nodes in the network, because transmission power requirement is very less for nearby nodes.
- Usually trust is updated at regular intervals by transfer of several packets which consumes more power. So Trust should not be updated regularly but on demand basis i.e. when there are some packets to send.
- We can adopt the cluster or zone based scheme to minimize the power consumption.

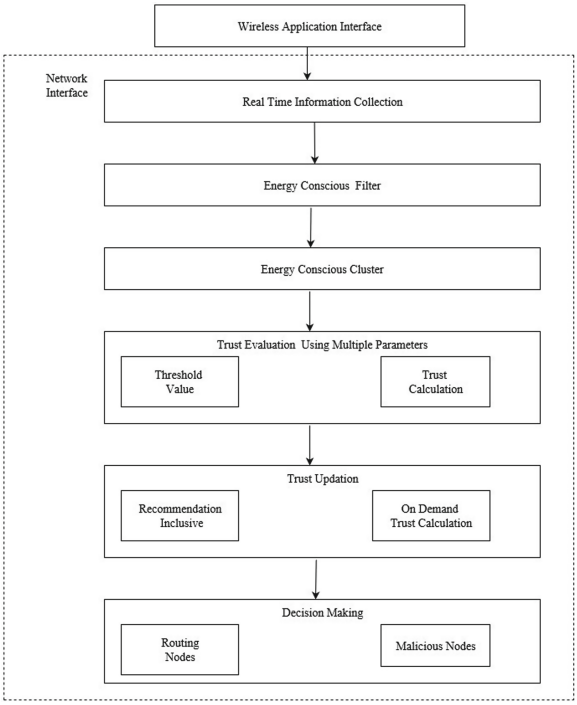


Fig. 6. Proposed model for energy conscious packet transmission using trust based mechanism.

Figure 6 shows the proposed model for energy conscious packet transmission using trust based mechanism. Real time information is collected in the proposed model to filter the nodes on energy basis. Afterword's, clusters are formed on the basis of above segregation of the nodes. Then trust based model is introduced to further classify the malicious nodes.

9 Open Issues

Trust based systems are complex, because they need to transfer various messages which consume more energy and bandwidth. A lot of work has been done on energy efficient and trust based mechanisms, but they are not integrated with each other. The critical issue is to decrease the energy consumption, bandwidth consumption and routing overheads without sacrificing the security of the network. Another issue is to use all kinds of trust (for example Direct trust, Indirect trust, Current trust and Historical trust) to calculate the Final trust. However when we use all kinds of trust, it will increase the Energy and Bandwidth consumption. So there is a need to develop the mechanisms which are energy efficient and uses all types of trust with multiple parameters for trust calculation. Co-operation between nodes is a prodigious challenge due to the presence of covetous and malicious nodes in the network. The trade-off

between various parameters is still an open issue for research. A hybrid technique is needed to solve the problem of true negatives, because in trust based system when the trust value of a node falls below the threshold value, it is marked as malicious but that node may be dropping packets due to some other reason. Another issue is to develop an adaptable mechanism which can handle the network changes like scalability, mobility, co-operation etc. A hybrid technique is needed to identify the malicious node right at the time of joining the network because trust based systems assumes all nodes are trusted by assigning them some initial trust value.

10 Conclusion

Wireless networks are being used extensively nowadays due to their numerous applications. They are susceptible to various kinds of attacks, because of their nature of operation, so there is a need of preventive, effective and energy efficient technique for packet transmission in ad-hoc networks. Trust based systems are one of the candidates for secure communication because of their effective and preventive nature. Trust can be calculated using various parameters. We have explored some parameters which can increase the effectiveness of trust based systems.

References

1. Merlin, R.T., Ravi, R.: Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET. Wirel. Pers. Commun. **104**, 1599–1636 (2019)
2. Mayti, M., Khatoun, R., Begriche, Y., Khoukhi, L., Gaiti, D.: A stochastic approach for packet dropping attacks detection in mobile ad hoc networks. Comput. Netw. **121**, 53–64 (2017)
3. Airehrour, D., Gutierrez, J.A., Ray, S.K.: SecTrust-RPL: a secure trust-aware RPL routing protocol for Internet of Things. Future Gener. Comput. Syst. (2018). https://doi.org/10.1016/j.future.2018.03.021
4. Khan, F.A., Imran, M., Abbas, H., Durad, M.H.: A detection and prevention system against collaborative attacks in mobile ad hoc networks. Future Gener. Comput. Syst. **68**, 416–427 (2017)
5. Wei, Z., Tang, H., Yu, F.R., Wang, M., Mason, P.: Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. IEEE Trans. Veh. Technol. **63**, 4647–4658 (2014)
6. Dorri, A., Vaseghi, S., Gharib, O.: DEBH: detecting and eliminating black holes in mobile ad-hoc network. Wirel. Netw. **24**, 2943–2955 (2017)
7. Badiwal, S., Kulshrestha, A., Garg, N.: Analysis of black hole attack in MANET using AODV routing protocol. Int. J. Comput. Appl. **168**(8), 27–33 (2017)
8. Paliwal, G., Taterh, S.: Impact of dense network in MANET routing protocols AODV and DSDV comparative analysis through NS3. Springer, Heidelberg (2018). Chap. 30
9. Li, X., Jia, Z., Zhang, P., Zhang, R., Wang, H.: Trust based on-demand multipath routing in mobile ad hoc networks. IET Inf. Secur. **4**, 212–232 (2010)
10. Tseng, F.H., Chiang, H.P., Chao, H.C.: Black hole along with other attacks in MANET: a survey. J. Inf. Process Syst. **14**, 56–78 (2018)

11. Yaseen, Q.M., Aldwairi, M.: An enhanced AODV protocol for avoiding black holes in MANET. Procedia Comput. Sci. **134**, 371–376 (2018)
12. Babu, M.R., Usha, G.: A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET. Wirel. Pers. Commun. **90**, 831–845 (2016)
13. Nadeem, A., Howarth, M.P.: A survey of manet intrusion detection & prevention approaches for network layer attacks. IEEE Commun. Surv. Tutor. **15**(4), 2027–2045 (2013)
14. Sood, M., Rani, P.: Removal of black hole attack using AODV protocol in MANET. Int. J. Eng. Manag. Res. (IJEMR) **7**(3), 72–75 (2017)
15. Khanna, N.: Mitigation of collaborative black hole attack using TRACEROUTE mechanism with enhancement in AODV routing protocol. IJFGCN **9**(1), 157–166 (2016)
16. Kaur, P., Kaur, D., Mahajan, R.: Simulation based comparative study of routing protocols under wormhole attack in MANET. Wirel. Pers. Commun. **96**(1), 47–63 (2017)
17. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y.(eds.): Futuristic trends in network and communication technologies, FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
18. Chander, D., Kumar, R.: Performance analysis of CBR and VBR applications on different multicast routing protocols over MANET. In: FTNCT 2018. Communications in Computer and Information Science, vol. 958, pp. 396–411. Springer, Singapore (2019)
19. Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., Kannan, A.: An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wirel. Pers. Commun. https://doi.org/10.1007/s11277-019-06155-x
20. Salman, M.S., Zhu, N., He, J., Zardari, Z.A., Memon, M.Q., Hussain, M.I.: An efficient trust-based scheme for secure and quality of service routing in MANETs. Future Internet **10**, 16 (2018). https://doi.org/10.3390/fi10020016
21. Zahedi, A., Parma, F.: An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks. Peer-to-Peer Netw. Appl. (2018). https://doi.org/10.1007/s12083-018-0654-0
22. Cai, R.J., Li, X.J., Chong, P.H.J.: An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE (2018). https://doi.org/10.1109/TMC.2018.2828814
23. Liang, W., Long, J., Weng, T.H., Chen, X., Li, K.C., Zomaya, A.Y.: TBRS: a trust based recommendation scheme for vehicular CPS network. Future Gener. Comput. Syst. (2018). https://doi.org/10.1016/j.future.2018.09.002
24. Beghriche, A., Bilami, A.: A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile ad hoc networks. Int. J. Intell. Comput. Cybern. (2018). https://doi.org/10.1108/IJICC-04-2017-0038
25. Shanthi, K., Murugan, D., Kumar, T.: Trust-based intrusion detection with secure key management integrated into MANET. Inf. Secur. J. Glob. Perspect. **27**(4), 183–191 (2018). https://doi.org/10.1080/19393555.2018.1505007
26. Anusha, K., Sathiyamoorthy, E.: A new trust-based mechanism for detecting intrusions in MANET. Inf. Secur. J. Glob. Perspect. **26**(4), 153–165 (2017). https://doi.org/10.1080/19393555.2017.1328544
27. Sethuraman, P., Kannan, N.: Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wirel. Netw. (2016). https://doi.org/10.1007/s11276-016-1284-1
28. Xia, H., Yu, J., Tian, C., Pan, Z., Sha, E.: Light-weight trust-enhanced on-demand multi-path routing in mobile Ad Hoc networks. J. Netw. Comput. Appl. (2015). https://doi.org/10.1016/j.jnca.2015.12.005

29. Zhao, D., Zhen, M., Zhang, D.: A distributed and adaptive trust evaluation algorithm for MANET. ACM (2016). http://dx.doi.org/10.1145/2988272.2990297
30. Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., Song, Y.-J.: Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **20**, 1698–1712 (2009)
31. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
32. Khanna, N., Sachdeva, M.: Study of trust based mechanism and its component model in MANET: current research state, issues, and future recommendation. Int. J. Commun. Syst. e4012 (2019). https://doi.org/10.1002/dac.4012

Energy Distance Neighborhood Based Weighted Hierarchical Clustering Algorithm

Rabindra Bista(✉) and Ajaya Thapa

Department of Computer Science and Engineering, Kathmandu University, Dhulikhel, Nepal
rbista@ku.edu.np, thapa.ajaythapa@gmail.com

Abstract. Wireless Sensor Network, a network of power-constrained sensing devices, is deployed in human unattainable areas easing daily life. Several clustering techniques allow WSN to be more energy efficient. LEACH, a principle clustering algorithm, and its descendant Q-LEACH uses a probabilistic model for cluster formation but do not consider any network parameters. RDBC, a randomized scoring algorithm, uses a distance model for improving the network's efficiency and reliability over LEACHes. However, it fails to evaluate network parameters such as node neighborhoods causing a lower stability period. We enhanced RDBC's scoring technique to create a new algorithm EDN that uses a weighted scoring model based on residual energy, distance from the BS and neighborhood to further improve network lifetime. We rigorously simulated different weights of the three parameters in Octave to model our algorithm and find out that it performed better than the aforementioned algorithms in terms of network stability and longevity.

Keywords: Wireless Sensor Networks · Clustering algorithm · Energy efficiency · Distance-based algorithm · Neighborhood count based algorithm · Network lifetime

1 Introduction

Numerous technologies have flourished in the world with the provision to make human life easier [1]. The technologies are built using algorithms that aim to conserve energy and make resource sustainable [2–4]. Wireless Sensor Network (WSN) is one of such technologies that is envisioned to integrate into the fabric of everyday life [5, 6]. The network itself is a combination of very small nodes of varying sensing capabilities that sense and collect data from the physical environment [7, 8]. These sensor nodes are resource-constrained devices equipped with one or more processors, a memory, a power supply, a transceiver and an optional actuator [9].

The combination of leaf and intermediate sensor nodes are deployed in human unattainable areas that include areas of military tracking and surveillance [10], healthcare [11], agriculture [12], natural disaster site [13], hazardous environment setting [14] and smart urban management [15]. In such areas, the primary source of

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 239–259, 2020.
https://doi.org/10.1007/978-3-030-40305-8_12

power supply to the nodes is merely button-sized batteries of low power capacity and once deployed, they should sustain for a larger period.

Algorithms are designed to allow sensor nodes to operate and transmit data to a powerful node called base station (BS). These algorithms should be energy efficient enough to extend the longevity of the network. One of the pioneer clustering algorithms LEACH [16] uses a probabilistic approach in achieving the longevity of the network but fails on assuring the reliability of cluster formation. Q-LEACH [17], like many other descendants of LEACH [18], improves energy efficiency but still uses the probabilistic approach like its ancestor in determining the CHs. Our work is based upon RDBC [19] which has significantly improved over both LEACH [16] and Q-LEACH [17]. It uses a randomized distance parameter to determine the CHs in the network. However, this algorithm uses a random number and do not consider other network parameters while electing CH which necessarily is not an ideal approach for real environment scenario. Our algorithm is better than these existing approaches regarding the stability, reliability, and efficiency of the network.

In hierarchical clustering, the method by which cluster header (CH) gets elected significantly determines how efficient the network is. Our algorithm uses the weighted sum model using three basic parameters of the sensor node to elect the CHs. The three parameters used are residual energy, distance from BS and neighborhood count (or EDN trio). A similar weighted model using different parameters was applied in ES-WCA [20] for the CH election but the primary focus is to detect misbehaving nodes in mobile WSN and assign weightage accordingly. Our focus is to analyze the relationship among the mentioned parameters to primarily focus on network stability and efficiency of the network.

We rigorously simulated with different weights of the EDN trio using the weighted model technique in a homogeneous network to finalize our model based on stability period and lifetime. The model was used to elect CHs based on the highest score value. Data transmission occurred in both single-hop and multi-hop fashion. The new algorithm meanwhile used the same TDMA scheme as that of LEACH to ensure that the nodes moved to sleep state while they are not transmitting data.

The paper is structured to discuss existing clustering algorithms related to the work in Sect. 2, propose the new algorithm in Sect. 3, compare the work with proven algorithms in Sect. 4 and finally conclude the work in Sect. 5.

2 Related Works

As briefly discussed in the previous chapter, LEACH [16] is observed as the pioneer of the hierarchical clustering algorithm which used probabilistic value for each node obtained from Eq. 1 to elect the CHs. The value of $T(n)$ for each node is compared to a random number between 0 and 1. If the value for any node, not elected as CH in the prior round, is less than the random number then that node is elected as the cluster

head. The nodes that receive broadcasting signals from CH of particular strength become the members of that cluster.

$$T(n) = \begin{cases} \frac{p}{1-p\left(r \bmod \frac{1}{p}\right)} & if\ n \in G \\ 0, \quad otherwise \end{cases} \tag{1}$$

The cluster formation and the data transmission processes occur in two phases. In the first phase (or the setup phase), the value of $T(n)$ is calculated for node n, p is the required number of cluster heads, r is the current round and G is the set of nodes not chosen as CHs in last 1/p rounds. In the second phase or the steady state phase, data transmission occurs from member nodes to CHs and all CHs aggregate and transmit the data to the base station directly in a single hop.

LEACH Centralized (LEACH-C) [21] uses BS during the setup phase to elect cluster heads where the node should have energy greater than the average energy of the overall network. BS identifies the location of the node and their residual energy and elects CH. Then it broadcasts the message containing cluster head ID information to all the nodes. The node that matches its ID against the CH's ID becomes the cluster head. All nodes except the CH determine their TDMA slots for data transmission and go to sleep until they have to transmit the data. This resembles the steady state phase of LEACH.

TL-LEACH transmits data to the BS by sending them over two different levels causing inter-cluster communication [22]. This leverages small transmission distance for cluster sensor nodes to the second level CHs rather than to the top-level CHs placed relatively to a farther distance. This extensively conserves the energy of sensor nodes during data transmission.

Q-LEACH (Quadrature LEACH) is a concept of applying LEACH separately to four different quadrants of an environment. This algorithm was an improvement to LEACH in terms of stability, throughput and network longevity [17]. The partition, however, introduced low data transmission and low data reliability as the number of rounds increased.

HEED [23], a hybrid energy-efficient algorithm, selects CH based upon residual energy and intra-cluster communication cost. The residual energy of each node identifies the initial set of CHs while intra-cluster communication cost determines the proximity to the neighbor for their membership to the cluster. It provides a uniform CH distribution across the network and better load balancing. However, the cost of intra-cluster communication requires information on the overall network by the algorithm.

MS-LEACH introduce by [24] resembles setup phase to LEACH, while in the steady state phase, requires calculating $Q_{critical}$ which is a critical cluster size and is compared to the average cluster size to either transmit data in multi-hop using Djikstra's algorithm or else in single-hop directly to the base station.

O-LEACH presented by [25], is an optimized technique to LEACH-C which elects cluster head based upon the residual energy being greater than 10% of the energy of other nodes. When the energy of nodes is less than 10% of the minimum residual energy, then the LEACH method is used instead.

Hybrid LEACH is a combination of LEACH and HEED protocols where CH is determined by using residual and maximum energy of the nodes [26]. CH is elected by selecting a random number after calculating the threshold value and average energy where the random number should be higher than the average energy.

RDBC, proposed by [19], is a randomized scoring technique where the approximate distance of the node from the base station, identified by using modified power distance formula in Eq. 2, is used to score each node. The distances, once calculated, are used for the remaining of the rounds as all the nodes are fixed.

$$P_r(dBm) = P_t(dBm) - 10 \times n \times \log(d) \tag{2}$$

Equation 3 gives the score that applies to the node in each round of the setup phase. The node with the highest score broadcast itself as the CH. The node with the highest score broadcast itself as the CH. All nodes receiving signal of a predetermined strength of X% of $P_{broadcast}$ becomes the cluster members of that node. The remaining nodes wait for their turn to become the CHs or the member nodes.

$$SCORE_i = Random\left(\frac{1}{d_{i\ to\ BS}\%}\right) \tag{3}$$

The steady state phase resembles that of LEACH where a predetermined TDMA time slot is fixed for each node. These nodes are expected to sense data at their time predetermined time slots. The algorithm is a significant improvement in increasing the life expectancy of the network, however, this is a random technique.

A table is presented (see Table 1) that compares and summarizes different criteria for all the existing algorithms briefly discussed above in the chapter. The criteria for comparison are listed and briefly described below.

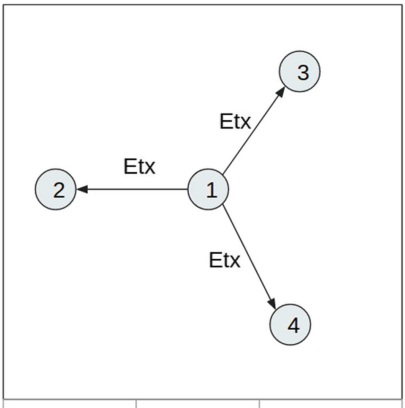
- Clustering: It defines whether the selection of cluster head is controlled by the central base station in which case it is centralized clustering or the selection of cluster head of a node is independent of any other nodes in which case it is distributed clustering.
- Location Required: It defines whether the location information of nodes is required for the election of cluster head or not.
- Hop Count: It defines how the sensed data from sensor nodes get transmitted to the base station either through direct transmission (or single hop) or through inter-cluster head communication (or multi-hop). If the data transmission from the sensor node to BS occurs via communication between two CHs, we define it as two hops communication.
- Scalability: It defines whether the algorithm can manage and function reliably with the increasing number of nodes and relatively high node density. The scalability can be low, moderate or high based on whether the increasing number of nodes affects the formation of the cluster and its longevity.
- Stability: It defines the duration or number of rounds until all nodes are alive and the entire network is capable of transmitting the data. The stability period can be low,

moderate or high based on whether the first node dies very early, in between or towards the end of the network lifetime.

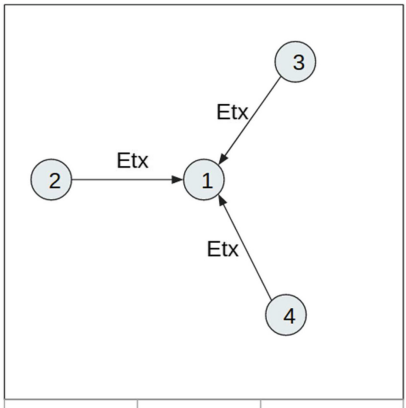
- Complexity: It defines the algorithm complexity in terms of cluster head election, cluster formation and data transmission which is based on the complexity of gathering parameters used for CH formation. The complexity of the algorithm can be low, moderate or high.
- CH Election: It provides brief information on how cluster head is formed and whether the formation approach is probabilistic or random or deterministic.

3 Energy Distance Neighborhood Based Hierarchical Clustering Algorithm

The proposed algorithm is a new technique to select cluster heads using weighted parameters SCORE of residual energy, the distance of the node from the base station and the neighborhood count. We extensively simulated 13 different combinations of weights of the three parameters Energy Distance Neighborhood (EDN trio) equaling to a sum of 1 and devised the mathematical model with optimal weight for each parameter based on the first node to death and the last node to survive in the network. EDN algorithm improves the stability of the network, the lifetime of the overall network and the total data transferred to BS when compared to existing algorithms.



Neighbor Table (NT)	NT(2)	1
	NT(3)	1
	NT(4)	1



Neighbor Table (NT)	NT(1)	2, 3, 4

Fig. 1. Neighbor Identification Algorithm Table for a node. The Neighbor Table (NT) for each node in the network to identify all its neighboring node

Table 1. Comparison of existing algorithms introduced in related works.

Algorithms	Criteria for comparison						
	Clustering	Location required	Hop count	Scalability	Stability	Complexity	CH election
LEACH	Distributed	No	Single-hop	Low	Low	Low	Random value of not getting elected in prior rounds
LEACH-C	Centralized	Yes	Single-hop	Low	Low	Low	BS elects cluster heads and forms cluster
TL-LEACH	Distributed	No	Two-hops	Low	Moderate	Low	Pre-determined. Two-levels with nodes having higher energy. Probabilistic and random
Q-LEACH	Distributed	Yes	Single-hop	High	Moderate	High	Probabilistic value of not getting elected in prior rounds in four quadrants. Probabilistic
HEED	Distributed	No	Multi-hop	Moderate	High	Moderate	Based on residual energy and communication cost. Probabilistic
MS-LEACH	Distributed	Yes	Multi-hop	Very High	Moderate	High	Random value of not getting elected in prior rounds. Probabilistic
O-LEACH	Distributed	Yes	Single-hop	High	Moderate	High	Energy of nodes to be higher than 10% of the average energy of the network. Probabilistic
H-LEACH	Distributed	No	Multi-hop	Moderate	High	Moderate	Residual and maximum energy of nodes. Probabilistic
RDBC	Distributed	Yes	Multi-hop	Moderate	Moderate	Moderate	Randomized Scoring using distance to BS. Probabilistic and random

The algorithm focuses on the three EDN trio as parameters as they significantly impact the energy efficiency of the network. The paper in [27] suggests that the data aggregating node with a high density of nodes as its members is an energy-efficient network. Greedy Cluster-based Routing, as per [28], uses maximum neighbor nodes and the minimum distance between source and BS for cluster election resulting in an

energy-efficient network. [19] has formally used the SCORE technique to elect the CH with the randomized value of node distance from BS as its technique for an energy-efficient network. Consideration of residual energy of a certain threshold has always been considered as the primary factor in the CH election in many descendants of LEACH. Hence, in the proposed algorithm, we feed in the simulated weights to the EDN trio parameters for each node during the setup phase to calculate the SCORE values and identify nodes that have the potential to become the CHs. We introduce this new scoring technique similar to that of [19] during the setup phase and then use LEACH steady phase technique to analyze the consumption of energy and the longevity of the network.

3.1 Experimental Setup

The algorithm has made the following assumptions before setting up the simulation:

- All the nodes are homogeneous, stationary and have constrained power.
- The nodes are randomly distributed in an N $\times$ N outdoor environment.
- The nodes will always sense some data in each round during their active state and transmit them to CH until their death.

The algorithm works in three phases namely the Initiation Phase, Setup Phase, and Steady State Phase. Initiation Phase occurs only once where the nodes get initialized with prerequisite parameters required for the algorithm's setup. Setup Phase and Steady State Phase occur simultaneously in a large number of rounds until all nodes die out. We do not need to consider other network forming problems such as routing, data aggregation and integrity in our experiment as those are resolved by other researches such as [8, 29] and are minimal to the requirements for the setup. In the setup phase, cluster heads are elected and clusters are formed while data transmission and aggregation occur to deduce the energy in the steady state phase. The energy of each node is deduced in each round by using the energy model explained in the Energy Model section. A detailed explanation of each of the phases is done in the next sections to follow. A detailed flowchart illustrating the simulation environment is shown in Fig. 2.

The flowchart in Fig. 2 illustrates that as long as all the nodes die out, cluster election, formation, and data transmission occur in the algorithm. The main objective of the algorithm is to make the nodes survive as many rounds as possible, which is achieved by the scoring method which detail is discussed in the next section. We rigorously simulated different weights of EDN trio understanding the relationship among the parameters and finalizing the SCORE formula based on stability and longevity factors of the network.

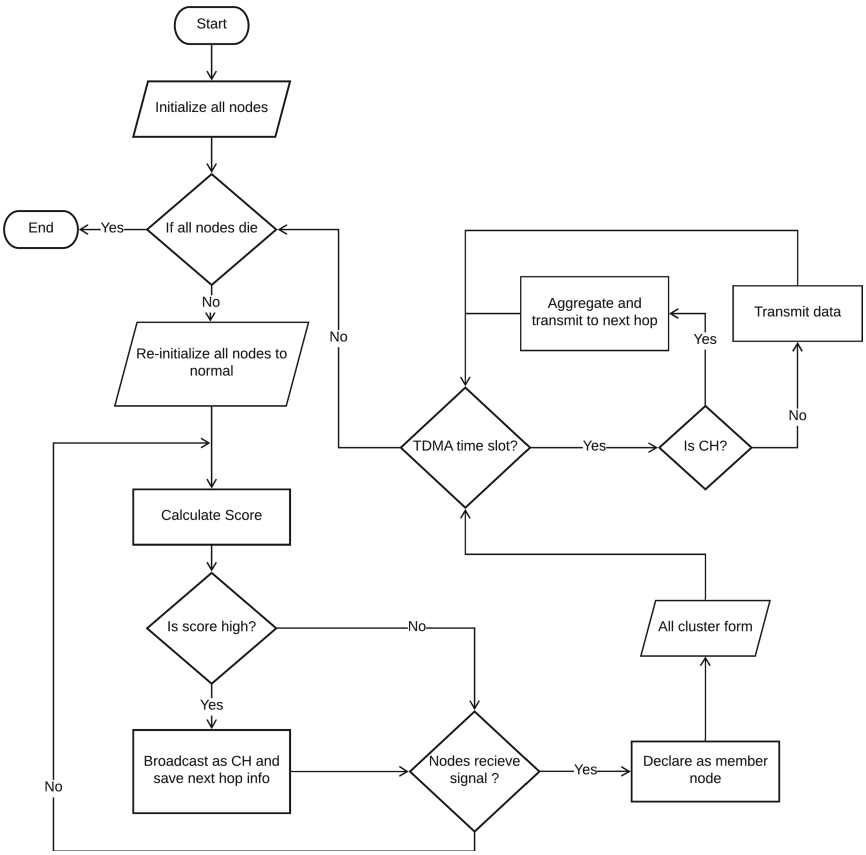


Fig. 2. Flowchart to explain the experimental setup of the EDN algorithm

3.2 Score Method

The scoring technique used for electing CH in the setup phase discussed later, is giving an individual score to each node taking a weighted score of residual energy, number of nodes and distance from BS. We simulated 13 different weights for each of the three parameters as shown in Table 6. Based on the factors of the death of the first node and the last node, we formulated the following formula to apply SCORE to each of the node i.

$$SCORE_i = \frac{1}{10} \times RE_{\%} + \frac{1}{2} \times NC_i + \frac{2}{5} \times d_{i-to-BS} \tag{4}$$

Equation 4 is the finalized model determined from the stability and lifetime of the network. In the equation, 10% RE is the residual energy of node i, 50% NC is the neighbor count of node i and 40% $d_{i-to-BS}$ is the approximate distance of node i from BS. Each node will have a different number of neighbors obtained by summing up all the neighboring nodes that have their distances within the single-hop distance from that particular node (Eq. 5).

$$NC_i = \sum_{k=1}^{n-i} \begin{cases} 1, & if\ k - i \leq d1 \\ 0, & if\ k - i > d1 \end{cases} \tag{5}$$

3.3 Initiation Phase

The phase begins with the boot of all the sensor nodes. By the end of the phase, the EDN trio parameters of each node is known. These nodes have the initial energy of E_0. We use Neighbor Identification Algorithm [30] to identify the neighbors of a node. The node maintains a Neighbor Table (NT) that stores the median RSSI value and the node ID of its neighbor. The table is formed in three processes of transmission, reception and decision processes. The transmission and reception phase occur in parallel. The transmission phase begins by sending a different number of ping messages by each node after the expiry of periodic timer plus a certain delay that allows avoiding collision. In the reception phase, a setup timer is set large enough to accept all the pings from closest nodes and then the receiving nodes update the neighboring table with node ID and median RSSI value of the pings. Any node then identifies its neighbor in the decision phase, as shown in Fig. 1, by determining if median RSSI falls between the max RSSI and max RSSI-i, i being the positive integer. The neighbors are identified once in the lifetime but the NT for each node is continuously updated in the setup phase whenever the death of any node occurs (Table 2).

Table 2. Algorithm 1 - initiation phase

Input: Set of stationary homogeneous N sensor nodes with initial energy of E_0 placed randomly in area of M x M

```
BEGIN # Begin Initiation Phase of deployed nodes
for each N nodes
    Next_hop = 0;
    Member_of_node = 0;
    SCORE = 0;
    Distance_from_BS = sqrt(Ptx - Prx);
    neighbor_count:
        for All_Nodes - current_N as N2
            node_distance = sqrt (N - N2);
            if node_distance ≤ max_distance_to_clustering
                N(count) = count + 1;
            end if
        end for
    Rem_energy = Rem_energy - (E_Rx × no_of_bits_received);
end for
END
```

Output: All nodes with initial information of neighboring table, residual energy and distance from the BS

Once the setup timer expires, when all the nodes would have identified their neighbors, BS broadcasts a short message that of transmitted power and BS header information to the sensor nodes. The sensor nodes receive the message with a certain receiving power. The approximate distance of the node is calculated using the power-distance formula given by [31] which is presented in Eq. 6. The distance calculation is done only once in the lifetime of the network as all the nodes are assumed to be stationary.

$$P_r = P_t \left(\frac{1}{d}\right)^2 \tag{6}$$

P_r is the power received by the node, P_t is the power transmitted by the base station and d is the approximate distance between the base station and the node. We have the power of 2 in the formula that represents an environment-dependent transmission factor for free space. The relative distance of the nodes from BS can also be identified using other techniques such as [32] based on the environmental setup of the network but based on our assumptions we opted for a simpler method.

3.4 Setup Phase

The setup phase resembles [19] in that the CH is selected using the maximum scoring of a node. The algorithm is presented in Table 3. Each alive nodes are initialized as a normal node while node with energy greater than the threshold energy (Eth) calculates the score from Eq. 4. The node with the maximum score broadcasts first and declares itself as the CH.

Using the neighbor table information, all neighboring nodes of this newly elected node become the members of the cluster. All other non-member nodes continue the clustering process until the nodes become either a member node or a CH. During the cluster formation, a CH also saves the next-hop information of another node potential of being a CH or member of another cluster. This is identified by the broadcasting strength P being less than X% which is a maximum distance for intercommunication between the two nodes.

Energy is also used to update the dead nodes in the neighboring table for each node, which occurs by identifying the almost dead nodes, which are still able to transmit the data in the neighboring region, and alerting all the nodes in the region.

3.5 Steady State Phase

This phase resembles that of LEACH as the nodes are allocated a distinct TDMA time slot to transmit the data to the CH and sleep for the rest of the time. The phase begins once all the clusters are formed wherein the sensor nodes transmit the data to the CH where the data gets aggregated and transmitted to the base station in single-hop or multiple hops. Thus, this phase comprises of data transmission phase for intra-cluster communication within the cluster, followed by data aggregation phase at CHs for converting all the collected data from member nodes into a single aggregated data and then data transmission phase again for inter-cluster communication between the CHs to transmit the collected information to the base station.

Table 3. Algorithm 2 - setup phase

Input: Output of Algorithm 1 (All nodes with initial information of neighboring table, residual energy and distance from the BS)

```
BEGIN # Begin Setup Phase of Sensor Nodes
For each round
   if CH_Remaining_Energy < 0.9\% * Newly_elected_CH_energy
      for each N Nodes
         SCORE = 1/10 × RE% + 1/2 × NCi + 2/5 × di to BS;
      end for
      while (node is N or R && node_energy > Eth)
         if n SCORE is maximum
            n(type) = 'CH'; cluster = cluster + 1;
            Broadcast Advertisement Message
            for neighbors_of_n as n2
               n2(type) = 'M';
               n2(member_of_node) = n;
            end for
            for other_non_neighbors as n3
               n3(type) = 'R';
               n3(next_hop) = n(id);
            end for
         end if
      end while
      All_CH(next_hop) = CH(nearest_to_BS) if distance_between_CH < distance_to_nearest_CH
   end if
end for
END
```

Output: All cluster formation with CH and its members and CH next_hop as CH or BS

We assigned TDMA time slot to each node using their node ID as the time slot so that each node gets activated only during one single time to sense and transmit the data to their CH. For the rest of the time, the sensor nodes remain in sleep mode. The sensor nodes lose energy during data transmission and by the CHs during data aggregation and transmission. As transmission and aggregation of data reduces the energy of the nodes, they ultimately die out in the later rounds. The algorithm's pseudo-code is written in Table 4.

3.6 Energy Model

The algorithm resembles the energy model proposed by [21] in which the energy consumption of each node for transmitting and receiving k-bits information to and from other nodes is calculated.

Table 4. Algorithm 3 - steady state phase

Input: Output of Algorithm 1 (All nodes with initial information of neighboring table, residual energy and distance from the BS)

```
BEGIN # Begin Setup Phase of Sensor Nodes
for each node N (TDMA_time_slot) AS n
   TDMA_Time_slot = n(node_id);
   if n(type) == 'M' AS m
      m(energy) = m(energy) - E_Tx × k_bits_transferred_to_CH;
      m_CH_energy = m_CH_energy × E_Rx × data_aggregation_energy;
   else if n(type) == 'CH' AS ch
      if ch(next_hop) == 0
         ch(energy) = ch(energy) - E_Tx × aggregated_k_bits_transferred_to_BS;
      else
         ch(energy) = ch(energy) - E_Tx × aggregated_k_bits_transferred_to_ch1;
         ch1(energy) = ch1(energy) - E_Rx × received_k_bits_from_ch + data_aggregation_energy;
      end if
   end if
end for
END
```

Output: Energy consumed by each node while communicating, TDMA slot

All node signals, before communication, is amplified by a factor modeled by the distance d between the two nodes. This amplification factor is defined by two energy models namely the free space model and multi-path fading model. A threshold distance d_0 is used to distinguish the two energy model where if $d \geq d_0$ then multi-path fading factor (Emp) is used and if $d < d_0$, then the free space model $(\in fs)$ is used. The threshold energy d_0 is given by Eq. 7.

$$d_0 = \sqrt{\frac{\varepsilon fs}{Emp}} \tag{7}$$

We can calculate the energy spent in transmitting E_{Tx} and receiving E_{Rx} the data using the following formula.

$$E_{Tx} = \begin{cases} E_{elec} \times k + k \times \varepsilon fs \times d^2 & if\ d < d_2 \\ E_{elec} \times k + k \times Emp \times d^4 & if\ d \geq d_0 \end{cases} \tag{8}$$

$$E_{Rx} = E_{elec} \times k \tag{9}$$

4 Simulations and Result

We used Octave 4.2.2, a powerful mathematics-oriented syntax scripting tool for GNU/Linux system, to simulate WSN networks of EDN, LEACH, Q-LEACH and RDBC algorithms.

To model the algorithms, we simulated a 100 × 100 environment for the sensor network of 100 randomly placed nodes with different weights of the EDN trio to identify Eq. 1 as the optimal weight for each of the parameters. Table 5 illustrates the WSN environment in which simulation of the algorithm was performed. We consider all nodes to be of initial energy (E_0) of 0.5 J. Threshold energy for each node is defined as 0.25% of E_0 which is used to determine if a node can actively participate to elect itself as the CH.

Table 5. WSN network environment for simulation

Network parameters	Value of the parameters
System	100 × 100
Sensor Nodes	100, homogeneous and stationary
Initial Energy of the node (E_0)	0.5
Threshold Energy (E_{th})	25% * E_0
Transmission Energy (E_{Tx})	50e−9
Receiving Energy (E_{Rx})	50e−9
Free-space energy model ($\in f s$)	10e−12
Multipath fading energy model (Emp)	0.0013e−12
Energy for data aggregation (E_{DA})	5e−9
k-bits	2000
Header-bit information	500

The base station is always fixed at a location of (50, 150). The maximum distance for inter-cluster communication is set as 50 m. This is according to [33] that ensures data transmission without packet loss which otherwise would have been lost in the real-world due to external environmental factors. Likewise, the maximum distance for intra-cluster communication is taken as 30 m, which is also considered a threshold for identifying any node as the neighboring node.

4.1 Models Simulation

The model of EDN algorithm in Eq. 4, where 10% is supplied to the residual energy, 40% to the node-BS distance and 50% to the neighborhood count, is identified by supplying thirteen different combination of weights to EDN trio to identify that the finalized model outperforms other in terms of network stability and longevity. The simulation resulted in a 1603 stability period of rounds and a 2334 longevity of rounds. This simulation result along with twelve other simulations results is tabulated in Table 6. As seen in Table 6, we applied maximum weights of 70% to each of the parameters in Simulation 3 to 10 to identify that neighborhood and distance with higher weights had a better impact on network than the residual energy. Simulation 11, 12 and 13 were done to break-tie between the two parameters to identify that neighborhood had a slightly better impact on distance when provided with the highest weights. Simulation 2 performed better with better stability period and network lifetime while

Simulation 11 was the closest competitive result to it. Simulation 2 not only better than the twelve other simulations but also better than the other existing algorithms. We thence finalized our algorithm SCORING model to use the weights of Simulation 2.

Table 6. Simulation run of different weighted score in EDN algorithm

Parameters	Simulation run numbers												
	1	**2**	3	4	5	6	7	8	9	10	11	12	13
Distance to CH	40	**40**	30	60	30	10	20	70	20	10	45	40	35
Neighbor count	40	**50**	60	30	10	30	70	20	10	20	45	55	50
Residual energy	20	**10**	10	10	60	60	10	10	70	70	10	5	15
Rounds until all nodes are dead	2316	**2334**	2320	2293	2254	2283	2315	2301	2167	2152	2332	2267	2158
First node death	1543	**1603**	1567	1566	1520	1551	1542	1568	1547	1544	1588	1490	1587
Second node death	1562	**1607**	1636	1600	1550	1573	1619	1615	1574	1567	1606	1613	1603

We used the finalized model in our algorithm and compared it to three previously discussed algorithms in LEACH, Q-LEACH, and RDBC. We used the following factors for analysis on how well EDN performed against the existing algorithms.

1. Death of Nodes Per Round: This allowed comparing algorithms for stability period and lifetime of the nodes.
2. Average Remaining Energy per Round: This allowed us to understand how much energy is invested by algorithm in each round for cluster formation and communication.
3. Packets Transmitted per Round: This showed the participation of nodes in each round by assuring the transmission of the data.
4. Total Packets Transmitted in Network: This showed the total number of packets transmitted by the nodes before the death of all the nodes.

Figure 3 uses the first factor of analysis showing the dead nodes count per round of simulation. When compared to LEACH, Q-LEACH, and RDBC where the death of the first node occurs at round 1141, 1528 and 930 rounds, EDN has the highest stability period as the network transmits data till round 1603 without any death of the nodes. This showcased that EDN is the most stable algorithm among the four algorithms in comparison. Our algorithm also has a longer lifetime as its lifetime of 2334 rounds is higher to the lifetime of LEACH which survives till 2202, of Q-LEACH which no longer communicates after 2362 rounds and RDBC which only survives 2304 rounds as shown by Fig. 3. The primary objective of the paper is achieved from the analysis. The death of the nodes for EDN, however after 1950 rounds, occurs faster than RDBC until 2200 rounds, which are due to energy invested in updating NT of the remaining alive nodes.

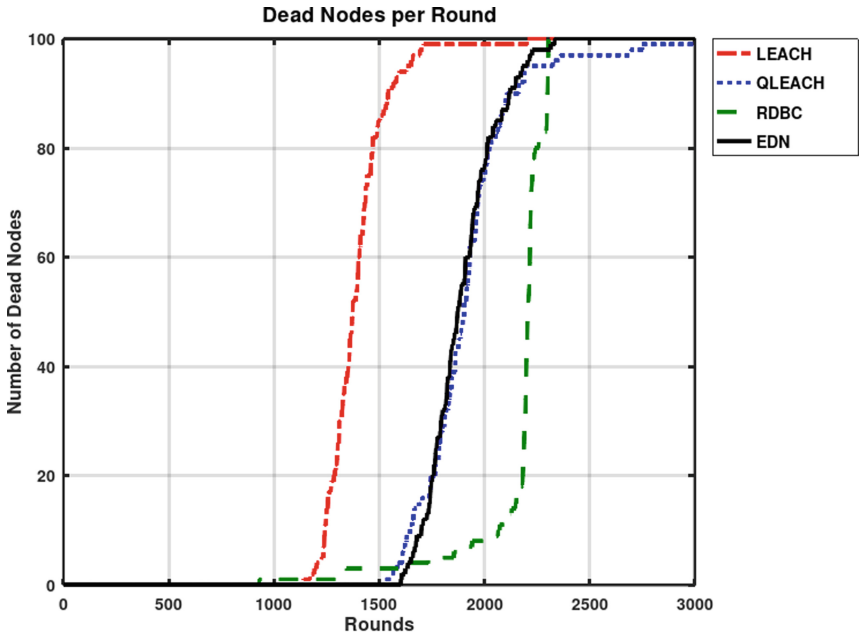


Fig. 3. Graph of dead nodes per round in algorithms. Shows the graph of the number of nodes that die in each round for the algorithms in comparison (LEACH, Q-LEACH, RDBC, EDN)

The slope of average energy in Fig. 4 suggests that for EDN energy is invested for identifying and updating neighbor nodes in each round and hence the remaining average energy is low after 1000 rounds when compared to RDBC but the average energy persists until the death of all nodes. The gradual decrease in average energy is due to the multi-hop approach that EDN takes and the difference from RDBC is seen only in updating the neighbor node information. EDN is comparable and slightly better to Q-LEACH when compared to average energy remaining per round while both being much better to LEACH.

As per Fig. 5, the total number of data packets transmitted per round by EDN is better than all the three existing algorithms for almost 1650 rounds (or the stability period). EDN transmission of data for almost up to round 1900 is better than RDBC and more data is transmitted in these rounds. However, RDBC has total packets transmission better from 2000 to 2200 rounds than EDN when the death of nodes for EDN occurs faster at those stages than RDBC. EDN surpasses RDBC in packets transmission after round 2200 and assures that nodes form the cluster and are active in data transmission until the death of all the nodes.

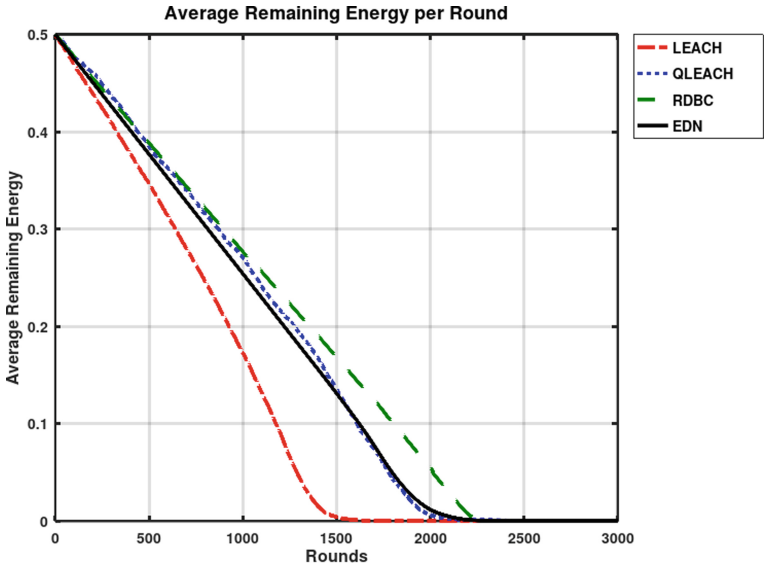


Fig. 4. Graph of average remaining energy per round in algorithms. Shows the graph of total average energy in Joules of all the alive nodes in the network in comparison (LEACH, Q-LEACH, RDBC, EDN)

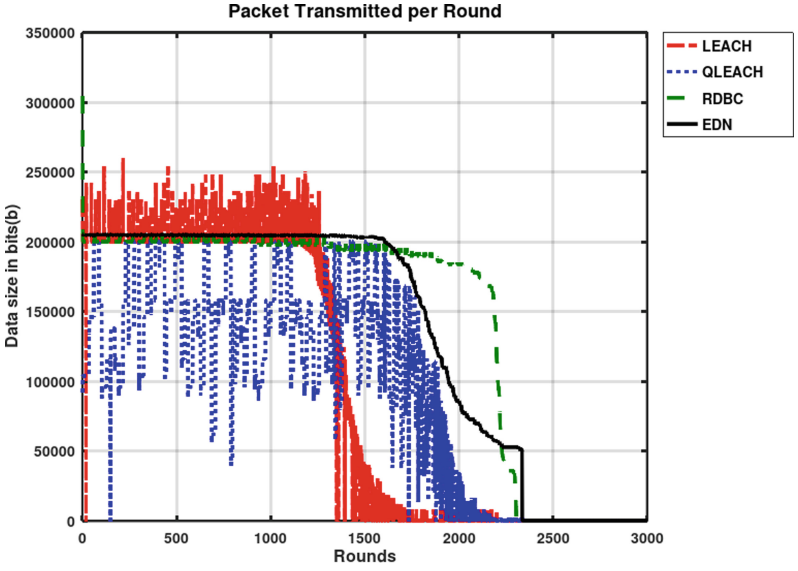


Fig. 5. Graph of packet transmitted per round in algorithms. Shows the graph of total message packets in bits transmitted by all nodes to BS per round in network in comparison (LEACH, Q-LEACH, RDBC, EDN)

Total packets transmitted in the network lifetime for EDN are better than LEACH and Q-LEACH as both of the latter algorithms stops transmitting data by round 2000 arrives, which is also shown in Fig. 6. EDN transmission of data for almost up to round 1900 is better than RDBC as more data is transmitted in these rounds. However, RDBC total packets transmission is better for 2000 to 2200 rounds than EDN when less number of nodes are left in those stages.

The new algorithm also assures cluster formation in each round like that of RDBC which otherwise is not confirmed for LEACH and Q-LEACH as the formerly elected cluster has the chance to become cluster head after 1/p rounds.

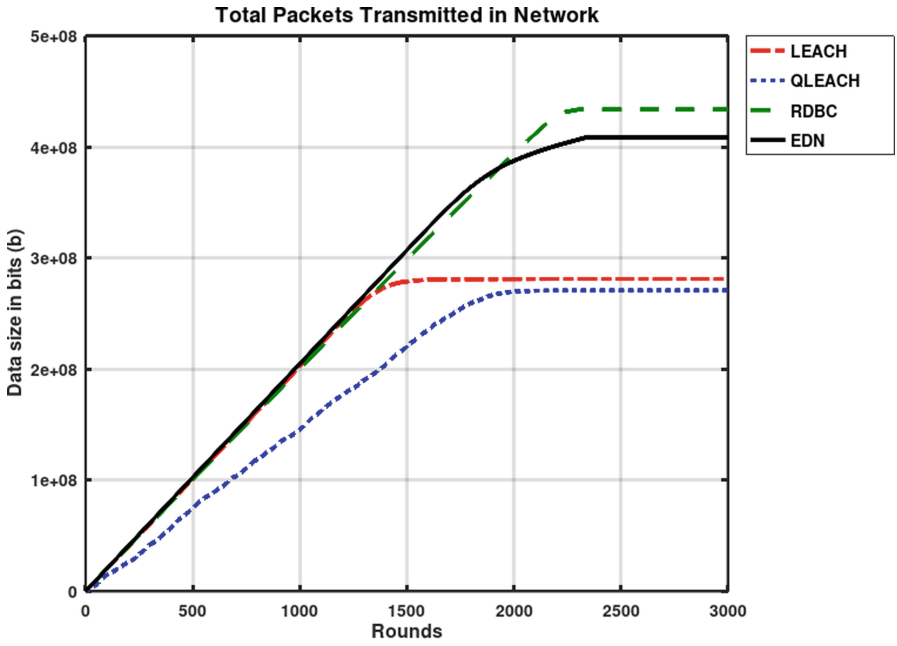


Fig. 6. Graph of total packets transmitted by algorithms. Shows the graph of the total number of message packets in bits collected by BS at the end of the lifetime by network in comparison (LEACH, Q-LEACH, RDBC, EDN)

4.2 Scalability Test

The new algorithm was also simulated to test it in terms of scalability. The simulation environment is the same as in Table 5 except for the network system. We simulated for two different scenarios: first to test if the network was scalable as the size of the network and the size of the node is increased and second to test the area coverage of the network when the size of the network is fixed with varying number of nodes.

Table 7. Simulation of scalability test for N × N area with N nodes

Environment	Number of nodes	Round when first node dies	Round when last node dies	Total packets transmitted in network
50 × 50	50	1740	2093	199.09 Megabits
100 × 100	100	1603	2334	408.338 Megabits
150 × 150	150	1502	1950	574.451 Megabits
200 × 200	200	1420	2225	789.0095 Megabits
250 × 250	250	621	2290	974.0595 Megabits
300 × 300	300	317	2308	1.1043 Gigabits

For the first case, we took areas of N × N area with N number of nodes where we took 50 × 50, 100 × 100, 150 × 150, 200 × 200, 250 × 250 and 300 × 300 area with nodes 50, 100, 150, 200, 250 and 300 respectively. The base station is fixed at (N/2, N + 50) distance while the nodes are stationary and randomly distributed. The simulation result is enlisted in Table 7. The test suggests that the network is scalable and does not show abruption wherein network lifetime is almost over 2200 rounds. Meanwhile, the test suggests that the network is more stable if the network has a lower number of nodes.

The second case of simulation, testing area coverage, was tested for a network system of 200 × 200 with nodes increased in a series of 50, 100, 200 and 400 as shown in Table 8. The base station is always fixed at (100, 250) while the nodes are randomly distributed but stationary.

Table 8. Simulation of scalability test for varying nodes in 200 × 200 environment.

Environment	Number of nodes	Round when first node dies	Round when last node dies	Total packets transmitted in network
200 × 200	50	832	2162	170.283 Megabits
200 × 200	100	716	2223	383.4375 Megabits
200 × 200	200	1420	2225	789.0095 Megabits
200 × 200	400	1492	2247	1.577 Gigabits

The test suggests that the algorithm is scalable in terms of area coverage. The tables show that the increase in nodes means more stability in the network. This is because as the number of nodes increases, the high weight-age of neighbor count allows more nodes to form a single cluster rather than many and these member nodes will have to transmit data to a relatively closer CH. Both the simulation tests also suggested that the nodes closer to the base station survive more rounds than nodes farther away.

5 Conclusions

We devised a new clustering hierarchical algorithm, EDN, which proved to increase the stability of the network and survive for a longer period hence increasing the energy efficiency of the network. The algorithm uses a weightage based scoring technique considering three parameters in the form of neighboring node count, distance from the base station and residual energy. It is found that the new algorithm is more stable and has a higher network lifetime when compared to the existing algorithms. The new algorithm extensively improves in different factors when compared to LEACH and Q-LEACH while offers minimum and improved or similar difference to RDBC.

The network latency for data transmission is high for EDN than other networks as the nodes needs to update its information on the neighbors that are dead during each round. If neighbor node information updates could be removed, this adds to the election run as well as improves the latency of the network. The improvement of this network latency can be considered in future work to further improve the network lifetime of the network.

The different parameters used in the algorithm can be used in a round-robin fashion on a priority basis and queued to elect the CH in each round until the node cannot be elected as the CH, which can also serve a basis for future work. Plus, the network model proposed here can be modified to analyze other properties of sensor node which might further help in the energy efficiency of the network and hence is an area of futuristic research.

With the advent of newer technologies such as WSN, studying several properties relative to that technology allows us to resolve the problem of energy efficiency and make the resource more sustainable. EDN algorithm studied three important properties of WSN to identify the relationship amongst them to conserve the energy of the overall network. The paper opens the area of research to study several other properties of the WSN and their relationship in order to make the network resource more sustainable.

Acknowledgment. We would like to thank Mr. Anmol Shakya, co-author of the RDBC algorithm, for providing technical support at the beginning of this research.

Conflict of Interest. Each author certifies that he or she has no commercial associations (e.g., consultancies, stock ownership, equity interest, patent/licensing arrangements, etc.) that might pose a conflict of interest in connection with the submitted article.

References

1. Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.): Futuristic trends in network and communication technologies, FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
2. Hong, W.-C., Li, M.-W., Geng, J., Zhang, Y.: Novel chaotic bat algorithm for forecasting complex motion of floating platforms. Appl. Math. Model. **72**, 425–443 (2019)

3. Fan, G.-F., Peng, L.-L., Hong, W.-C.: Short term load forecasting based on phase space reconstruction algorithm and bi-square kernel regression model. Appl. Energy **224**, 13–33 (2018)
4. Dong, Y., Zhang, Z., Hong, W.-C., Dong, Y., Zhang, Z., Hong, W.-C.: A hybrid seasonal mechanism with a chaotic cuckoo search algorithm with a support vector regression model for electric load forecasting. Energies **11**(4), 1009 (2018)
5. Römer, K., Frank, C., Marrón, P.J., Becker, C.: Generic role assignment for wireless sensor networks. In: Proceedings of the 11th Workshop on ACM SIGOPS European Workshop: Beyond the PC - EW11, 2004, p. 2 (2004)
6. Wang, Q., Balasingham, I.: Wireless sensor networks - an introduction. In: Wireless Sensor Networks: Application-Centric Design. InTech (2010)
7. Lin, D., Wang, Q.: An energy-efficient clustering algorithm combined game theory and dual-cluster-head mechanism for WSNs. IEEE Access **7**, 49894–49905 (2019)
8. Bista, R., Chang, J.: Energy efficient data aggregation for wireless sensor networks. In: Sustainable Wireless Sensor Networks. InTech (2010)
9. Stankovic, J.A.: Wireless sensor networks. Computer (Long. Beach. Calif.) **41**(10), 92–95 (2008)
10. Winkler, M., Street, M., Tuchs, K.-D., Wrona, K.: Wireless sensor networks for military purposes. In: Autonomous Sensor Networks, pp. 365–394. Springer, Heidelberg (2012)
11. Zhang, Y., Sun, L., Song, H., Cao, X.: Ubiquitous WSN for healthcare: recent advances and future prospects. IEEE Internet Things J. **1**(4), 311–318 (2014)
12. Abouzar, P., Michelson, D.G., Hamdi, M.: RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture. IEEE Trans. Wirel. Commun. **15**(10), 6638–6650 (2016)
13. Jha, R.K., Singh, A., Tewari, A., Shrivastava, P.: Performance analysis of disaster management using WSN technology. Procedia Comput. Sci. **49**, 162–169 (2015)
14. Somov, A., Baranov, A., Spirjakin, D.: A wireless sensor–actuator system for hazardous gases detection and control. Sens. Actuators A Phys. **210**, 157–164 (2014)
15. Lu, W., Gong, Y., Liu, X., Wu, J., Peng, H.: Collaborative energy and information transfer in green wireless sensor networks for smart cities. IEEE Trans. Ind. Inform. **14**(4), 1585–1593 (2018)
16. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, vol. 1, p. 10 (2000)
17. Manzoor, B., et al.: Q-LEACH: a new routing protocol for WSNs. Procedia Comput. Sci. **19**, 926–931 (2013)
18. Mahapatra, R.P., Yadav, R.K.: Descendant of LEACH based routing protocols in wireless sensor networks. Procedia Comput. Sci. **57**, 1005–1014 (2015)
19. Bista, R., Shakya, A.: Randomized distance based clustering algorithm for energy efficient wireless sensor networks. Adv. Comput. Commun. Technol. **2016**, 377–389 (2016)
20. Amine, D., Nassreddine, B., Bouabdellah, K.: Energy efficient and safe weighted clustering algorithm for mobile wireless sensor networks. Procedia Comput. Sci. **34**, 63–70 (2014)
21. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**(4), 660–670 (2002)
22. Loscri, V., Morabito, G., Marano, S.: A two-levels hierarchy for low-energy adaptive clustering hierarchy (TL-LEACH). In: 2005 IEEE 62nd Vehicular Technology Conference 2005, VTC-2005-Fall, vol. 3, pp. 1809–1813 (2005)
23. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mob. Comput. **3**(4), 366–379 (2004)

24. Qiang, T., Bingwen, W., Zhicheng, D.: MS-Leach: a routing protocol combining multi-hop transmissions and single-hop transmissions. In: 2009 Pacific-Asia Conference on Circuits, Communications and Systems, pp. 107–110 (2009)
25. Khediri, S.E.L., Nasri, N., Wei, A., Kachouri, A.: A new approach for clustering in wireless sensors networks based on LEACH. Procedia Comput. Sci. **32**, 1180–1185 (2014)
26. Razaque, A., Mudigulam, S., Gavini, K., Amsaad, F., Abdulgader, M., Krishna, G.S.: H-LEACH: hybrid-low energy adaptive clustering hierarchy for wireless sensor networks. In: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT) 2016, pp. 1–4 (2016)
27. Intanagonwiwat, C., Estrin, D., Govindan, R., Heidemann, J.: Impact of network density on data aggregation in wireless sensor networks. In: Proceedings 22nd International Conference on Distributed Computing Systems 2002, pp. 457–458 (2002)
28. Parthasarathi, M., Vajravel, K.: Greedy cluster based routing for wireless sensor networks. Int. J. Comput. Sci. Inf. Technol. **9**(2) (2017)
29. Kumar, N., Singh, Y., Singh, P.K.: An energy efficient trust aware opportunistic routing protocol for wireless sensor network. Int. J. Inf. Syst. Model. Des. **8**(2), 30–44 (2017)
30. Abdellatif, M.M., Oliveira, J.M., Ricardo, M.: Neighbors and relative location identification using RSSI in a dense wireless sensor network. In: 2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET) 2014, pp. 140–145 (2014)
31. Xu, J., Liu, W., Lang, F., Zhang, Y., Wang, C.: Distance measurement model based on RSSI in WSN. Wirel. Sens. Netw. **02**(08), 606–611 (2010)
32. Gautam, P.R., Kumar, S., Verma, A., Rashid, T., Kumar, A.: Energy-efficient localization of sensor nodes in WSNs using beacons from rotating directional antenna. IEEE Trans. Ind. Inform. **15**, 5827–5836 (2019)
33. Anastasi, G., Falchi, A., Passarella, A., Conti, M., Gregori, E.: Performance measurements of motes sensor networks. In: Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM 2004, p. 174 (2004)

Recent Advances in Wireless Sensor Network for Secure and Energy Efficient Routing Protocol

B. C. Gaur Sanjay, Manish Purohit(✉), and Om Prakash Vyas

J.I.E.T., Jodhpur, Rajasthan, India
electmanish@gmail.com

Abstract. Wireless Remote Sensor Network is broadly utilized in numerous regions including security reconnaissance. The perilous essential in remote sensor systems is to accomplish ideal utilization of vitality during steering as the sensor hubs because of restricted vitality assets. It is the challenging task in the field of wireless sensor network. Most of the researchers are working to minimize it by various methodologies. One of the methods is to use efficient protocol that can minimize the energy consumption. Sensors area unit considered important parts of electronic devices. In most applications of wireless sensing element networks (WSNs), necessary and important info should be delivered to the sink in an exceedingly multi-hop and energy-efficient manner. Inasmuch because the energy of sensing element nodes is restricted, prolonging network time period in WSNs is taken into account to be a vital issue. So as to increase the network time period, researchers ought to take into account energy consumption in routing protocols of WSNs [16]. For such applications, routing protocols must support mobility and discover optimum P2P routes along with the energy efficiency. The nodes in IoT have limited energy. Fast energy depletion of nodes leads to the creation of energy holes in the network, which hinders the intended services to IoT application. Hence, energy-efficiency is also one of the fundamental objectives of routing protocols. In the literature, many researchers have proposed energy-efficient routing protocols that provide optimum P2P routes. But most of them do not support mobility of nodes in the network [17].

This paper presents a survey of energy efficient routing protocols in wireless sensor networks.

Keywords: Wireless Remote Sensor Network · Efficiency · Network lifetime · Energy optimization · Remote sensor nodes · Protocols · Routing issues · Classification · Protocol review · IoT · P2P traffic · Mobility

1 Introduction

Wireless sensing element networks are most well liked and hot space of analysis of late. These sensing element networks are consisting of many miniature sensors referred to as nodes. These nodes have 3 basic components: A sensing scheme, that acquires information from the physical encompassing surroundings, a sub-system, that stores the

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 260–274, 2020.
https://doi.org/10.1007/978-3-030-40305-8_13

native information once process, and a wireless communication scheme for information transmission. The detecting component hubs can possibly assemble partner degreed course data either to an alternate detecting component or back to an outer base station [2]. The energy economical routing protocol is important for minimising the energy consumption. sensing element nodes carry restricted, typically irreproducible power sources [1]. Runtime of a sensing element network depends on keep energy offer. A sizable amount of nodes are typically put in in vital parcel of land space, thus it's troublesome to exchange or recharge the batteries. Therefore, planning of energy economical routing protocol is basically needed.

In this respect, several routing, power management and information dissemination protocols have already been designed for wireless sensing element network. Routing in Wireless sensing element Network (WSN) is incredibly difficult thanks to inherent characteristics of wireless sensing element network. These constraint combined with a usually deployed an oversized range of sensing element nodes create several challenges to the planning and managing the Wireless sensing element networks.

In Wireless detecting component Network, detecting component systems are put discretionarily and in matrix looking on the strategy wont to convey the system. As detecting component hubs utilizes vitality from batteries for detecting {the information|the info|the information} and transmittal information it devours the vitality for these tasks. Dodging the utilization of vitality in detecting component hubs is amazingly hotly debated issue in the present time and conjointly troublesome assignment. A few conventions and calculations are wont to maintain a strategic distance from vitality utilization on the grounds that the batteries in Wireless detecting component Network, that are non-superfluous.

In this, a top to bottom study has been made on the ongoing issues in Wireless detecting component Networks and referenced changed issues with pertinence absolutely different|completely different} outcomes also as various procedures. Likewise, this paper centers around the methodologies utilized for keeping away from vitality utilization of Wireless detecting component Network, {the different|the varied} conventions and calculations by different creators.

2 Routing Factors and WSN Design

Akyildiz et al. and Jamal et al. have addressed the following challenging factors for designing the routing protocols for WSN.

Prashant Krishan had a word that routing in Wireless Remote sensor Network is very challenging due to its wireless nature. There are many reasons:

(a) WSNs have countless sensor hubs, it is preposterous to expect to apply a worldwide tending to plot for the organization of an enormous number of sensor hubs as the overhead will be high to keep up the Ids of the sensor Network.

(b) Sensor hubs are firmly compelled as far as vitality, preparing, and capacity limit. So there must be some instrument to deal with the assets. There are numerous difficulties and configuration gives that influence the steering procedure in Wireless sensor Network.

2(a) Fault Tolerance
Due to the shortage of power, some detector nodes could fail or block. Generally thanks to physical harm or environmental interference sensors don't work with efficiency. Ultimately, there ought to be arrangement of backup for the failure of detector nodes. It shouldn't have an effect on the task of the wireless detector network.

2(b) Node Deployment
Node preparation in WSN is application dependent. It is either manual or irregular. In manual preparation, the sensors area unit placed manually, and knowledge is routed through planned ways. However, the detector nodes area unit wet every which way in random node preparation.

2© Energy Consumption Without Losing Accuracy
Sensor nodes will create use of their restricted offer of energy for playing computations and transmittal info in an exceedingly wireless setting. The saving of Energy consumption mustn't lose the accuracy.

2(d) Scalability
The number of device nodes deployed within the sensing space depends on the geographical demand of the world, could also be on the order of a whole bunch or thousands, or more. The routing style should be ready to work with large variety of device node.

2(e) Heterogeneity
The existence of a heterogeneous set of sensors raises several technical problems associated with knowledge routing. For instance, some applications would possibly need a various mixture of sensors for observance temperature, pressure, and wetness of the encircling setting, police work motion via acoustic signatures, and capturing pictures or video following of moving objects.

2(f) Quality of Service
In some applications, data should be delivered within a certain period of time from the moment it is sensed, or it will be useless. Therefore, time-constrained applications is the main base point to cover up the things for energy conservation and data delivery.

2(g) Transmission Media
In a multihop sensing element network, act nodes square measure connected by a wireless medium. The standard issues related to a wireless channel (e.g., fading, high error rate) may additionally have an effect on the operation of the sensing element network.

2(h) Connectivity
High hub thickness in gadget systems blocks them from being totally separated from each other. Along these lines, gadget hubs square measure expected to be very associated. This, in any case, probably won't prevent the group of stars from being variable and furthermore the system size from contracting in light of gadget hub disappointments.

3 Routing Protocols in WSN

When all is said in done, steering in remote gadget systems might be partitioned into 3 very surprising classifications as, level based directing, various leveled based steering, and area put together directing checking with respect to the system structure. The characterization of convention is appeared in figure one. In level based directing, all hubs square measure naturally named equivalent jobs or common sense. In progressive based directing, every one of the hubs assume their particular job inside the system. In area based steering, gadget hubs positions square measure vanquished to course data in the system.

Whenever bound framework parameters might be controlled to adjust to the present system conditions and available vitality levels, at that point a directing convention is considered to be adjustive in addition, these conventions might be arranged into 5 classes as multipart-based generally, question based, exchange based, Qos-based, or directing methods depending on the convention activity. Furthermore to the higher than, depending on anyway the stock sends a course to the goal, directing conventions might be characterized into 3 classes, viz. proactive, receptive, and half breed conventions. In proactive conventions, all courses square measure registered before they're required, though in receptive conventions, courses square measure processed on request. Cross breed convention utilizes a blend of higher than ideas. It's alluring to have table driven steering conventions, when gadget hub is static, rather than abuse responsive conventions. A significant amount of vitality is utilized in course revelation and arrangement of responsive conventions. Another entirely unexpected classification of steering convention is named the agreeable directing; during which hubs send data to a focal hub any place data might be aggregate and ought to be dependent upon any procedure if necessary. Henceforth, it lessens the course cost as far as vitality utilization.

Higher-vitality hubs square measure used to strategy and send the information, while low-vitality hubs square measure used to play out the detecting at interims the nearness of the objective. The arrangement of bunches and task uncommon missions to group heads can incredibly add to by and large system timespan, and vitality strength. Hierarchic sort of steering is partner conservative gratitude to bring down the vitality utilization at interims a group, playacting data accumulation hence on decline the amount of transmitted messages to the sink hub. Hubs could assume completely very surprising jobs at interims the system like bunch heads, group individuals in Hierarchical-based steering.

Because of the serious vitality imperatives of gigantic assortment of thickly sent gadget hubs, it needs a lot of system conventions to execute various system the executives and the board capacities like synchronization, hub limitation, and system security.

The traditional routing protocols have many shortcomings once applied to WSNs, that square measure in the main thanks to the energy-constrained nature of such networks (Fig. 1).

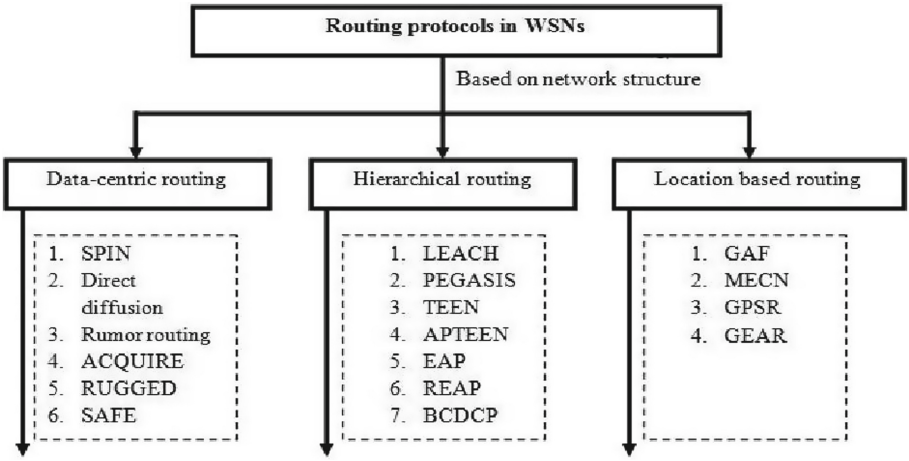


Fig. 1. Classification of routing protocols

On the off chance that definite framework parameters might be controlled in order to adjust to the present system conditions and out there vitality levels, at that point a steering convention is considered to accommodate. Likewise, these conventions might be characterized into 5 classes as multipart-principally based, question based, exchange based, Qos-based, or directing strategies figuring on the convention activity. Moreover to the higher than, figuring on anyway the stock sends a course to the goal, directing conventions might be ordered into 3 classes, viz. proactive, receptive, and mixture conventions. In proactive conventions, all courses square measure processed before they're required, while in receptive conventions, courses square measure registered on request. Half and half convention utilizes a blend of higher than thoughts. It's attractive to have table driven steering conventions, when detecting component hub is static, rather than abuse receptive conventions. A significant amount of vitality is utilized in course disclosure and arrangement of receptive conventions. Another totally unique classification of directing convention is named the helpful steering; inside which hubs send data to a focal hub any place data might be total and ought to be dependent upon more procedure if necessary. Subsequently, it decreases the course cost as far as vitality use. The implementation of this method was done mistreatment WSN. On these lines, the interval of image was diminished that increased the continual execution of framework adequately and understands the optimizing of cutting direction more and more. The system has varied blessings viz. tiny volume, reconfiguration of package and hardware, flexibility of programming, movableness, robust generality et cetera. The trial comes regarding demonstrate that the composed framework has high truth and therefore the atmosphere has very little impact on the framework once it runs [9].

4 Literature Review of Energy Efficient Protocols

The approach supported energy potency. This section covers the survey of literature of the protocols that square measure energy economical. The first protocol supported AN adjustive agglomeration has been planned by Heinzelman, referred to as LEACH for distributing energy load among the detector nodes in network. LEACH uses a single-hop routing. Every detector node severally transmits data on to the cluster head or the sink. The planned protocol works in two phases [4].

The first part additionally referred to as setup part during this part, clusters square measure organized, and cluster heads square measure elect. The random rule is employed by every node in every spherical to work out the chance of turning into a cluster head.

The steady state phase- the information is shipped to the bottom station ruled by LEACH rule. The length for the steady state part is larger than the setup innovate order to attenuate overhead.

Cluster head creates a TDMA (Time Division Multiple Access) schedule supported the amount of nodes within the cluster within the cluster CDMA (Code Division Multiple Access) code is employed for absolute communication. LEACH isn't appropriate for big network areas.

Hierarchical protocols square measure outlined to scale back energy consumption by aggregating knowledge and to scale back the transmissions to the bottom Station. LEACH is taken into account because the most well-liked routing protocol that use cluster based mostly routing so as to attenuate energy consumption. to investigate LEACH protocol then additional we'll discuss the phases of LEACH protocol. Shortly we have a tendency to outline varied potential attacks on.

PEGASIS (Power Efficient Gathering in Sensor Information Systems)

The subsequent strategy dependent on an eager chain convention [5] settles the information gathering issue of the remote sensor systems. The primary concern for every hub is to get and transmit to close neighbors and alternate being the pioneer for transmission to the base station. This methodology equitably disperses the vitality load among the sensor hubs in the system. At first the hubs are set arbitrarily in the field, and later the sensor hubs are organized to frame a chain.

It very well may be cultivated by the sensor hubs themselves utilizing an eager calculation beginning from any hub. On the other hand, the base station can make sense of the tie and communicate it to the various sensor hubs. All hubs have worldwide information on the system that is the reason a voracious calculation can be utilized on any hub for building the chain. Development of a circle to guarantee that all hubs have close neighbors is exceptionally troublesome as this issue is like the voyaging sales rep issue. Before the first round of correspondence begins, the voracious calculation is utilized for building the total chain. It shows better outcomes when contrasted with the past strategy by LEACH. It can additionally improved by:

- Neglecting the overhead of dynamic cluster formation,
- Reduction the number of transmissions,
- Using only one transmission to the base station per round.
- This approach shows further improvement when network size increases.

PEGASIS is that it utilizes every one of the hubs to transmit or get with its nearest neighbor hubs. Every one of the hubs which gather the information combine it with the information got by the neighbor hub and transmit it to the following closest neighboring along these lines every one of the hubs get and intertwine their information, and pass it to the following neighbor in a chain position till they all arrive at the base station. Each hub in the system alternates as a pioneer of the chain and the one answerable to transmit the entire intertwined information gathered by the chain of hubs to the base Station. Along these lines the normal measure of vitality spent by every hub is decreased. Covetous calculations are utilized to see that all hubs are utilized during the chain arrangement. PEGASIS expect that every one of the hubs with changing or low vitality levels can be remunerated so as to ascertain the vitality cost of the transmissions with the rest of the vitality they are left with. It isn't fundamental that every one of the hubs need to know its neighboring hubs, the base station can decide the way or structure the chain for all hubs, or every one of the hubs can decide their neighboring hubs by sending a sign. Contingent on the sign quality, the hubs modify their sign to such an extent that they hear just the closest neighbors in the system. This methodology will convey the vitality load equitably among the sensor hubs in the system as it utilizes every one of the hubs of the system to frame the chain and perform straightforward information sending tasks. On the off chance that any hub kicks the bucket in the chain, another chain is framed, dispensing with the dead hubs obviously PEGASIS enhances LEACH by sparing vitality at various stages C.

PEACH (Power-Efficient and Adaptive Clustering Hierarchy)
The third approach is a convention by Peach [6] which is control an effective and versatile bunching chain of command convention for remote sensor systems. In remote sensor systems, by catching a hub can perceive the source and the goal of bundles transmitted by its neighbor hubs. In light of the caught data, PEACH shapes the bunches without extra parcel transmission overhead, for example, notice, declaration, joining, and planning messages. So as to give a versatile staggered bunching, PEACH is intended to work on probabilistic directing conventions approach. As a result of the convention configuration, PEACH is typically progressively adaptable and productive to the different situation than the current bunching conventions of the remote sensor systems. PEACH can be utilized in the two sorts of sensor arrange area unconscious and area mindful. The area mindful PEACH convention can be utilized when the area data of every hub isn't accessible on the system. The area mindful PEACH comprise of the confinement component, for example, a GPS like equipment. It possibly works when this sort of equipment is accessible on sensor hubs. For any WSN, the general correspondence cost can be diminished by the decreasing the information parcels, and the grouping conventions improve the lifetime and the vitality utilization of the remote sensor systems. No overhead on bunch head determination is feasible for PEACH and it structures versatile staggered grouping when contrasted with the current bunching conventions.

TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol)
TEEN [7] is that the first convention created by Manjeshwar and Agrawal for responsive systems. This convention was created by Manjeshwar and Agrawal during this topic, moreover to the qualities, the group head communicates to its individuals at

each bunch correction time. 2 assortments of limit are used in this framework, to be specific, burdensome edge and delicate edge. The strenuous edge lessens the amount of transmissions. It allows the hubs to transmit just the distinguished characteristic is inside the differ of intrigue. Moreover to that the delicate edge lessens the amount of transmissions by taking out every one of the transmissions, which could have generally happened once there's almost no or no revision inside the recognized trait. Juvenile is appropriate for fundamental time applications and is furthermore very practical as far as vitality utilization and response time. It conjointly allows the client to deal with the vitality utilization and precision that suit the apparatus. The most shortcoming of this subject is that if the limits aren't accomplished, the hubs never impart. Additionally, the client doesn't get any data parcel from the system it simply recommends that system neglects to comprehend concerning the hubs in spite of the fact that they kick the bucket.

Thus, this theme isn't appropriate for applications wherever the user need the info incessantly. Another downside is that a sensible implementation would need to make sure that their collision-free cluster. If the brink doesn't reach to the specified level then information isn't communicated to the bottom station. Therefore, no messages or inform sent to the bottom station even within the case of the node gone dead. APTEEN overcomes this disadvantage [19, 20].

EEABR (Energy Efficient Ant-Based Routing)
Camilo et al. have projected a protocol, that relies on the Ant Colony optimisation heuristic approach. This protocol considers total distance and energy state of the trail traversed by the ants for choice of the nodes. At the start the forward ants are sent to any or all its neighbor nodes, that mean that detector nodes should contain all the small print of the nodes accessible relating to the right choice of path or correspondent levels of secretion path. For an outsized size networks, this can be a tangle to possess huge amounts of memory to avoid wasting all the knowledge concerning its neighboring nodes. They additionally instructed that identical algorithmic rule will be altered to avoid wasting memory. The construct is, if the forward ants are sent on to the sink, the routing tables solely ought to save the neighbor nodes that are within the direction of sink. The direction is already mounted that's why it reduces the scale of the routing tables and, ultimately, the memory required by the node [8].

SOP (Self-Organizing Protocol)
The arranged convention [9] is also expansion of LEACH's thought. It incorporates grouped structure of LEACH with multi-bounce directing to diminish transmission vitality. In a few systems of remote sensors utilizes multi-bounce directing. The equation picks a hub that transmits data to a goal hub by discovering one or different transitional hubs. The correspondence keep dynamic among every one of the hubs till the data parcels arrive at the goal [10].

The information parcel takes numerous jumps among the hubs inside the WSN arrange. The most bit of leeway of this methodology is that it expends less transmission vitality, anyway at the contrary hand inertness of the system and deferral of data bundles also will increment. In some cases, there's no flexibility within the demand of latency; the multi-hop routing will cause high energy potency. Some collision shunning

mechanism is another to CSMA waterproof protocol, so as to scale back the likelihood of collisions at setup part. Thus, it's higher than LEACH's approach.

MAEER (Mobility Aware Energy Efficient Routing)
In this paper, Chaudhari et al. have proposed a convention Mobility Aware Energy Efficient Routing Protocol (MAEER) [17] for Internet of Things is recommended that supports portability and finds about ideal courses with diminished vitality utilization. The proposed convention diminishes the quantity of partaking hubs in P2P course disclosure to diminish the vitality utilization.

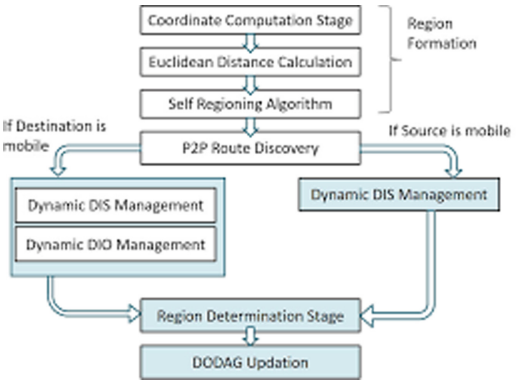


Fig. 2. Maeer algorithm

Not with standing that Fig. 2, it additionally offers a proficient way to deal with furnish portability support with expanded bundle conveyance proportion. The exhibition of our steering convention is examined with benchmark conventions for example RPL, P2P-RPL, alongside ME-RPL. The outcomes show that the proposed convention gives 24% less vitality utilization in contrast with P2PRPL which is best among RPL, P2P-RPL, and ME-RPL, and 15% preferred bundle conveyance proportion over ME-RPL which gives best parcel conveyance proportion among the three.

5 Recent Techniques for Energy Saving

This segment is based late procedures utilized for upgrading the power utilization for WSN. Each system referenced here proposes the normal components like start to finish defer or start to finish unwavering quality, group head arrangement for bigger size districts for transmission, single and multipath way transmissions, condition based changes, application-based conventions [16].

GEAR (Geographical and Energy Aware Routing)
Yan et al. [17] have proposed a Geographical and Energy Aware Routing. The arranged Geographic and Energy Aware Routing (GEAR) rule utilizes vitality intensely mindful neighbor and pick a course to move a bundle towards the objective locale.

algorithmic Geographic Forwarding or Restricted Flooding rule helps to distribute the parcel inside the objective district. This convention conveys extra scope of parcels than GPRS in arbitrary rush hour gridlock and uniform traffic.

MHHC (Multi Hop Hierarchical Clustering)
The anticipated convention improves arrange life by twenty second over the LEACH's recipe. MHHC convention pursues the grouping way upheld positioned level. This doesn't pursue totally extraordinary way to send the information from supply to goal by following static way. On account of static way, the vitality of the contrary gadget hubs can get down and a hub kicks the bucket. In this manner, it's low vitality, that will expand the system life expectancy.

SPIN (Sensor Protocol for Information Negotiation)
The SPIN rule is anything but difficult to actualize and see with regards to the SPIN a hub promotes for information to convey the goal hub. At that point the halfway hubs. Then the intermediate nodes which recover the advertisement send the solicitations for the data transmission around then the specific information is moved to the ideal hub [20].

SPIN-I
It is propelled adaptation of SPIN. This class of conventions deals with sending and accepting inquiries to its whole neighbor for information transmission. Simultaneously the goal hub additionally sends a question of enthusiasm from a hub through system. At the point when enthusiasm between every one of the hubs go under a most limited way coordinates the question then it begins transmission. This convention is intended for lossless system, fills in as "Indiscriminately forward" and "Information difficult to reach". Transmission time is longer than the SPIN convention in light of the fact that every hub does some computation before picking the following jump transmission. Subsequently, it isn't proper for enormous size systems. This convention adjusts vitality hubs as opposed to sparing it (Fig. 3).

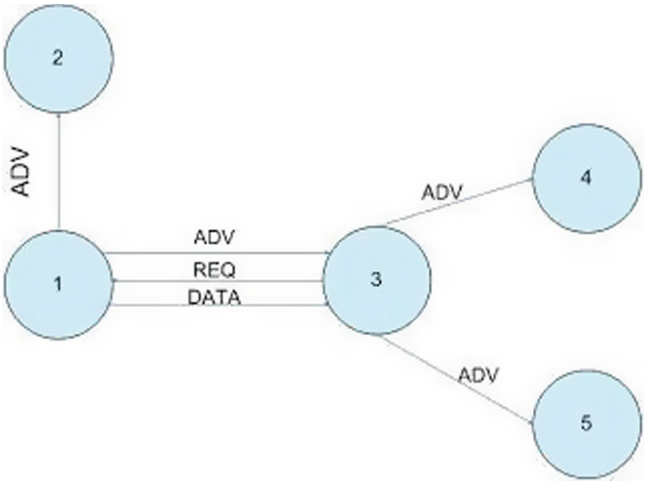


Fig. 3. SPIN protocol

Node Hub 1 sends ADV message to all its neighbors, 2 and 3. Node 3 solicitations for information utilizing REQ message for which hub 1 send information utilizing message DATA to hub 3. After getting the information hub 3 sends AV message to neighbors 4 and 5 and the procedure proceeds. This convention additionally makes hubs increasingly savvy making each hub as asset chief.

6 Rendezvous Algorithm

This algorithm proposes groups of nodes which serves as meeting point and amassed the data from source and transfer to the base station when arrives.

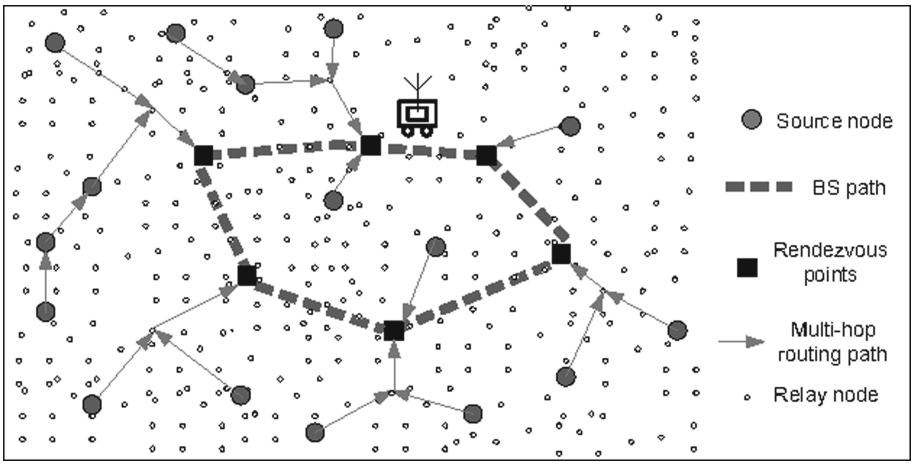


Fig. 4. Rendezvous algorithm energy efficient data collection and execution

This algorithm combines the approach of smothered quality and knowledge caching in network as shown in Fig. 4. The quality enabled WSN will increase the latency in knowledge assortment, therefore, giving bottleneck performance [25]. a briefing purpose is chosen for each cluster through greedy formula with geometrical relationship between cluster head and its members to understand the goal of optimal/suboptimal energy consumption, the optimise mechanism is planned based mostly on Rendezvous formula in step with the energy mode.

7 Conclusion and Future Scope

In this paper, significant issues of steering have been considered which affecting the sensor organize plan. Numerous affordable directing conventions are anticipated by the researcher for remote identifier systems. Any way during this paper, exclusively those conventions are referenced that makes them vitality conservative. From the audit

conventions, it's unmistakably observed that the presentation of conventions is cost promising regarding vitality strength. Anyway it's excruciating to style a directing convention which can defeat all arranging issues with WSN, yet as have brilliant execution for all remote finder systems applications. In this the total review gives the vitality efficient of the trail with least utilization of vitality gives most output. Protocols like LEACH, LEER and TEEN ensure life span of locator hubs.

It also presumes that new strategies and state-of-the-art thinks about are jury-fixed in sparing the vitality and whipping the bottleneck of vitality utilization in WSNs late investigations generally speaking improved by normal pace of 25–45% in sparing the vitality. Absolutely {different completely different} systems utilized in various projections bolstered putting of finder hubs in WSNs and upheld conditions, application, very surprising situations in each space the different methods function admirably with sensible outturn.

8 Challenges Related to WSN

A. Difficulties continuously in running time: WSN upset world situations. In a few cases, gadget data ought to be conveyed at interims time requirements so satisfactory perceptions might be made or moves made. Just a couple of results exist up to now concerning gathering real time necessities in WSN. Most conventions either disregard timeframe or simply plan to strategy as brisk as potential and expectation that this speed is agreeable to fulfill cutoff times. Some underlying outcomes exist for timeframe steering. Until this point, the confined outcomes that have showed up for WSN concerning timespan issues has been in steering. A few distinct capacities should conjointly meet timespan imperatives including: data combination, data transmission, target and occasion discovery and characterization, question procedure, and security. New outcomes square measure required to guarantee delicate timeframe necessities which upset the substances of WSN like lost messages, commotion and blockage abuse criticism the board to deal with each unfaltering state and transient conduct hopes to convey guarantee. Over seeing timeframe regularly recognizes the need for separated administrations, e.g., directing arrangements should bolster very surprising classes of traffic; ensures for the fundamental traffic and less help for insignificant traffic. It's fundamental not exclusively to create timespan conventions for WSN, anyway related investigation systems ought to try and be created.

B. Difficulties in control administrations power managements: reasonable preparing is one acclaimed bit of leeway of gadget systems. limited processor data measure and little memory square measure 2 easy to refute limitations in gadget systems, which can vanish with the occasion of creation procedures. Nonetheless, the vitality limitation is probably not going to be settled after a short time because of moderate advancement in creating battery ability. Additionally, the neglected idea of gadget hubs and perilous detecting conditions block battery substitution as potential goals. On the contrary hand, the police examination nature of the numerous gadgets arranges applications needs an extended lifetime; along these lines, it's a significant investigation issue to create a style of vitality proficient police examination

administration for a geological region. A ton of this examination centers around the best approach to give full or incomplete detecting inclusion inside the setting of vitality preservation.

C. System Scale and Time-Varying Characteristics of WSN underneath extreme vitality requirements, gadget hubs work with limited figuring, stockpiling and correspondence abilities [32] depending upon the apparatus, the densities of the WSNs could differ broadly, beginning from appallingly flimsy to horrendously thick. In these gadget hubs the conduct of gadget hubs is dynamic and incredibly versatile, in light of the fact that the should self-compose and monitor vitality powers gadget hubs to direct the conduct interminably because of their present degree of action. In addition, the gadget hubs could likewise be needs modifying the conduct in light of the sporadic and eccentric conduct of remote associations brought about by high commotion levels and radio-recurrence obstruction, to prevent extreme execution debasement of the machine bolstered.

D. The board a good ways off: gadget hubs will be conveyed at our entryway field like a terminal. It's extreme for chiefs or administrators to deal with the system legitimately. In this way the structure should give partner roundabout remote control/the executives framework.

9 Future Scope

The recent researchers target the protocols by choosing the necessity of specific region. It's the well-known undeniable fact that WSN could be a terribly huge field of study. The survey shows that there's still heaps of scope to figure. The topics for scope area unit, finding the answer for region freelance or structures freelance, suggestion regarding the topologies, network layers design, and formula supported completely different environmental conditions. These area unit the open topic for energy economical WSN to figure. Beneath water WSNs problems and optimized resolution also are difficult task and new space of analysis. In future, we will improve by saving the route from malicious attacks and improve the potency.

Overall, if we have a tendency to take assumptions for future work then there's one technology fits smart all told the conditions that's probable to be Artificial Intelligent. a strong system/protocol may be designed that may handle the complete completely different state of affairs.

References

1. Akyildiz, F., Su, W., Shankarasubramaniam, Y., Cayirci, E.: Wirless sensor networks: a survey. Comput. Netw. **38**, 393–422 (2002)
2. Al-Karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: a survey. IEEE Wirel. Commun. **11**(6), 6–28 (2004)
3. Mao, X., Tang, S., Xu, X., Li, X.-Y., Ma, H.: Energy efficient opportunistic routing in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **8**(4), 973–990 (2011)

4. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. Published in the Proceedings of the Hawaii International Conference on System Sciences, vol. 8, pp. 8–20. IEEE (2000)
5. Lindsey, S., Raghavendra, C.S.: PEGASIS, power efficient gathering in sensor information systems. In: IEEE Aerospace Conference, vol. 3, p. 3 (2001)
6. Yi, S., Heo, J., Cho, Y., Hong, J.: PEACH: power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks. Comput. Commun. **30**, 2842–2852 (2007)
7. Manjeshwar, A., Agrawal, D.P.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: Null, p. 30189. IEEE (2001)
8. Camilo, T., Carreto, C., Silva, J.S., Boavida, F.: An energy efficient ant-based routing algorithm for wireless sensor networks. In: International Workshop on Ant Colony Optimization and Swarm Intelligence, pp. 49–59 (2006)
9. Zhao, J., Erdogan, A.T.: A novel self-organizing hybrid network protocol for wireless sensor networks. In: Proceedings of the First NASA/ESA IEEE Conference on Adaptive Hardware and Systems, AHS 2006, pp. 412–419 (2006)
10. Shah, R.C., Rabaey, J.M.: Energy aware routing for low energy ad hoc sensor networks. In: IEEE Wireless Communications and Networking Conference (WCNC), 17–21 March 2002, Orlando, FL (2002)
11. Sara, G.S., Kalaiarasi, R., Neelavathy Pari, S., Sridharan, D.: Energy efficient clustering and routing in mobile wireless sensor network. Int. J. Wirel. Mob. Netw. (IJWMN) **2**(4), 1–9 (2010)
12. Amala Shiny, V.A., Nagarajan, V.: Energy efficient routing protocol for mobile wireless sensor network. Int. J. Comput. Appl. **43**(21), 1–5 (2012). 0975-8887
13. Saini, S., Singh, R.S., Gupta, V.K.: Analysis of energy efficient routing protocol in wireless sensor networks. Int. J. Comput. Sci. Commun. **1**(1), 113–118 (2011)
14. Liu, C.H., Hui, P., Branch, J.W., Yang, B.: QOI-aware energy management for wireless sensor networks. In: IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 8–13 (2011)
15. Banerjee, I., Chanak, P., Sikdar, B.K., Rahaman, H.: EER: energy efficient routing in wireless sensor networks. In: Proceeding of the 2011 IEEE Students Technology Symposium, pp. 92–97 (2011)
16. Ghaffari, A.: An energy efficient routing protocol for wireless sensor networks using A-star algorithm. J. Appl. Res. Technol. **12**(4), 815–822 (2014)
17. Chaudhari, S., Maurya, S., Jain, V.: MAEER: mobility aware energy efficient routing protocol for Internet of Things, pp. 1–6 (2017). https://doi.org/10.1109/infocomtech.2017.8340624
18. Thakkar Mansi, K., Patel, M.M.: Energy efficient routing in wireless sensor network. In: Proceedings of the International Conference on Inventive Research in Computing Applications, ICIRCA 2018 (2018). IEEE Xplore Compliant Part Number: CFP18N67-ART; ISBN 978-1-5386-2456-2
19. Mahmoud, M.M.E.A., Lin, X., Shen, X.: Secure and reliable routing protocols for heterogeneous multihop wireless networks. IEEE Trans. Parallel Distrib. Syst. **26**(4), 1140–1153 (2015). https://doi.org/10.1109/TPDS.2013.138
20. Das, A., Swaroop, A.: Energy efficient routing protocol for linear wireless sensor network. In: International Conference on Computing, Communication and Automation, ICCCA 2017 (2017)
21. Kurian, A., Divya, R.: A survey on energy efficient routing protocols in wireless body area networks (WBAN). In: 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, pp. 1–6 (2017). https://doi.org/10.1109/iciiecs.2017.8276162

22. Bhoge, S.G., Chawhan, M.D., Suryavanshi, Y., Taksande, V.K.: Cross-layer approach for energy & communication efficient protocol of mobile ad hoc networks. In: International Conference on Communication and Signal Processing, 6–8 April 2017, India (2017)
23. Kaur, B., Singh, B.: Enhanced energy efficient LEACH protocol using adaptive filter in WSN. In: 2018 4th International Conference on Computing Sciences (ICCS), Jalandhar, pp. 7–14 (2018). https://doi.org/10.1109/iccs.2018.00008
24. Mahmoud, M.M.E.A., Lin, X., Shen, X.S.: Secure and reliable routing protocols for heterogeneous multihop wireless networks. IEEE Trans. Parallel Distrib. Syst. **26**, 1140–1153 (2018)
25. Oh, Y.-J., Lee, K.-W.: Energy-efficient and reliable routing protocol for dynamic-property-based clustering mobile ad hoc networks. Int. J. Distrib. Sens. Netw. **13**(1), 1–16 (2017)
26. Khan, H.: A survey on hierarchical cluster-based energy efficient routing protocol for wireless sensor networks. IJET **7**, 216–221 (2018)
27. Karthikeyann, A., Arunachalam, V.P., Karthik, S., Dhivya, P.: Energy efficient structure free and location based routing protocol in WSN. In: 2018 International Conference on Soft-Computing and Network Security (ICSNS) (2018)
28. El Hajji, F., Leghris, C., Douzi, K.: Adaptive routing protocol for lifetime maximization in multi-constraint wireless sensor networks. J. Inf. Netw. **3**, 67–83 (2018)
29. Durrani, N.M., Kafi, N., Shamsi, J., Haider, W., Abbsi, A.M.: Secure multi-hop routing protocols in wireless sensor networks: requirements, challenges and solutions. IEEE Transactions
30. Shao, X., Wang, C., Gao, J.: Research on network coding aware energy efficient routing for wireless sensor networks. EURASIP J. Wirel. Commun. Netw. **2018**, 231 (2018)
31. Krishan, P.: A study on dynamic and static clustering based routing schemes for wireless sensor networks. Int. J. Mod. Eng. Res. (IJMER) 3(2), 1100–1104 (2013). www.ijmer.com. ISSN 2249-6645
32. Indu, S.D.: Wireless sensor networks: issues & challenges. IJCSMC **3**(6), 681–685 (2014)
33. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)

Energy Efficient Routing Protocols for Wireless Sensor Network

Sumit Kumar Gupta[1,2(✉)], Sachin Kumar[2], Sudhanshu Tyagi[3], and Sudeep Tanwar[4(✉)]

[1] Department of Electronics and Communication Engineering, SRMS CET&R, Bareilly, UP, India
sumikg@gmail.com
[2] Department of Electronics and Communication Engineering, Amity University, Lucknow Campus, Lucknow, UP, India
[3] Department of Electronics and Communication Engineering, Thapar Institute of Engineering & Technology, Deemed to be University, Patiala, Punjab, India
[4] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
sudeepl49@rediffmail.com

Abstract. Wireless sensor network is a network of sensor nodes which are connected together wirelessly. Sensor node has the capability to sense, process and communicate the data to the distinct location which is known as base station or sink or destination sensor node. The purpose of sensor node is to sense the data and transmit to sink but the transmission of data is crucial which depends on how it is routed. Another factor which affects the sensor network, is energy. So These two factors are very crucial for WSN. Hence in the chapter we will cover the routing protocols used in wsn in detail. We will cover the types of sensor node, how can be routed the data using sensor node and how we can classify routing protocol so that we can have energy efficient network. We also discuss different IEEE standards related to WSN.

Keywords: WSN · Routing protocol · Energy efficiency · Homogeneous environment · Heterogeneous environment

1 Introduction

A very wide range of applications have been identified with the help of sensor nodes when they form a connected network which is known as Wireless Sensor Network (WSN). A WSN has a variety of applications like border surveillance, civilian surveillance, health care, environment monitoring such as temperature, sound, vibration, pressure, motion, pollution levels, humidity, wind speed and direction etc., agriculture monitoring such as water level, insect infection etc., home utility application, industrial process control and many more. All these varieties of applications cannot get without any efforts. These efforts are known as challenges in WSN. Hence WSN has a variety of challenges like deployment of sensor node, energy

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 275–298, 2020.
https://doi.org/10.1007/978-3-030-40305-8_14

efficiency, path routing of sensor node, security of data, architecture of sensor node, types of sensor node, distribution of energy among the sensor nodes data collection etc.

So the routing protocol is the process of discovering suitable path for data transmission from source sensor node to destination sensor node or base station or sink. The process of selecting right path is not so easy because it depends on other factors like type of network, channel characteristic etc. The sensed data sends to base station where that base station may be connected to some other network where it is analyzed and action will be taken on the basis of sensed data.

But wireless sensor network has different scenario as compared to wireless network which make it very challenging to implement. The challenges are

1. Since the deployment of sensor node is random which makes it difficult for uniform addressing scheme for sensor node.
2. Since we have a number of sensor node which sensed data and send to base station or any other sensor node so we must have efficient network.
3. Since base station are getting data from a number of sensor node so base station has data redundancy which creates problems to take right decision.
4. Since we are deploying sensor node randomly and they have limited battery life so it is very difficult to change battery of sensor node.

Because of all above mentioned problem, we have to design a routing protocols so that we can have active sensor node for a long period of time and can get information from required field.

Hence collectively we can say that by minimizing the overall energy consumption of the sensor network, we have to design different types of algorithms that can generate different routing protocols. As we have seen in the literature studied, we have a lots of protocol all across the world. The lifespan of a WSN can be significantly increased if the software of sensor node like operating system, network layer and the application layer are planned in such a way that they can use optimum energy. The algorithms & derived protocols are designed such that they are aware of the hardware circuitry and use special features of the microcontroller & transmitter and receivers to minimize the energy withdraw capacity. Such modification can proceed toward a customize resolution in designing of different types of sensor node. Because of such modification, we can have different types of sensor nodes that can deployed and form different types of sensor networks. Hence we have generated such algorithms that can be energy effective in WSN.

A wireless sensor network (WSN) can be defined as a network of electronic devices, which are defined as sensor nodes, that can be sensed the surrounding environment and can transfer the information collected from the surrounding environment via wireless links. The collected data is transferred to distinct location which is known as base station (BS) or sink or processing center unit through single hope or multiple hops. The sink or BS can be locally situated within the network or can be connected to other networks (e.g., the Internet) through a gateway. Sensor nodes can be classified on the basis of hardware, position, application, energy and mobility as shown in Fig. 1. Sensor node is classified on the hardware basis as below

- **Single Board Computer:** These sensor nodes are designed such that they can have sufficient energy for computing & can run complete systems such as Windows, Linux etc. The consumption of power may vary depending on used system. During the deployment of such sensor node in the field, they are dependent on external power supply such as solar power etc. [51].
- **Embedded Sensor Module:** Such embedded sensor nodes are high ended sensor nodes. Such sensor nodes are embedded with different component like CPU for computation power, RAM for internal storage, flash for external storage & several other peripherals like analog to digital converter, digital to analog converter, general purpose input/outputs, RF etc. They have sufficient peripherals to run for different OS. Such sensor nodes consume huge power and are estimated to run for few weeks or months such long periods [51].
- **Low-end Embedded Sensor Module:** Such embedded sensor nodes are low ended. These sensor nodes are designed to run on batteries for months and years of long periods. These sensor nodes are designed for low-power consumption & cheaper microcontrollers like TI CC2538, Freescale MC13234 etc. [52] that are implemented the IEEE 802.15.4 standard protocol. These sensor nodes require optimized operating systems such as Tiny OS etc. Power consumption of such devices are typically in the order of a few mW [51].

The sensor nodes can be stationary means the sensor nodes are not movable and they can't change their position after deployment. The sensor nodes can be movable, mean the sensor node can change their position after deployment. Sensor nodes can be classified on the basis of energy. They can be homogeneous and heterogeneous SN. Homogeneous SNs are those in which all SNs have same energy and Heterogeneous SNs are those in which some SNs have different energy.

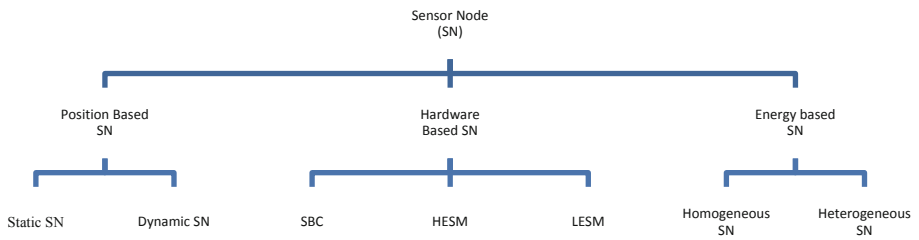


Fig .1. Types of SN

After deployment of SNs, the next essential question raised that on which route messages must be routed when multiple paths are available from a source sensor node to a destination sensor node. Moreover, what options are available for routing and how to execute the shortest routing path along which messages must be sent?

Routing is ideally defined as the algorithm of determining a sequence among the source node, intermediate sensor node and the destination node upon request of message propagation. In WSNs, the routing of data messages is implemented in the network layer.

In case of large multi-hop communication networks, the source node can't deliver the information to the destination directly, therefore, intermediate sensor nodes are used to deliver the information. An intermediate sensor node has to decide to which neighboring sensor node is used to forward the information so that it can reach to the destination.

The chapter is arranged in such a way that the reader can understand the IEEE standard related to WSN in Sect. 2. In the next Sect. 3, what are the basic requirement to select any routing protocol is discussed. In the next Sect. 4, a classification of routing algorithms is discussed which are based on various different criteria discussed in Sect. 3. After that we will discuss the different routing algorithms which have used in WSN in Sect. 4. After covering the different routing algorithm, the final section of the chapter provides a brief description of the routing algorithm for WSNs.

2 IEEE WSN Standards

As we have seen that wireless sensor network is a collection of tiny sensor node. Sensor node has a very small size but can do wonders. In this small size, sensor node has power supply, microcontroller, transreceiver and antenna. Sensor node has a battery to supply the power to sensor node circuitry. Sensor node has different section to consume of its limited power because sensor node has no provision to replace the battery as it deployed in the experimental field.

Figure 2 shows the commonly used infrastructure for wireless sensor network in which the sensor nodes are deployed randomly in the required experimental field. All the sensor nodes will send the data to base station.

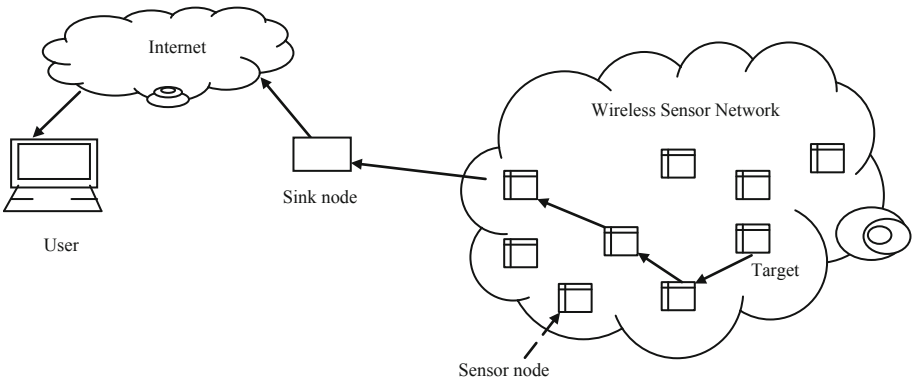


Fig. 2. Sensor node deployment

Each sensor node (SN) is embedded with its processing unit, limited wireless area, sensing module along light-weight storage capacity. Every SN is constructed by active and passive components like sensor, signal controlling & processing by using micro-controller unit, signal transmissions by transceiver, antenna, and power supply unit. Figure 3 shows the wireless SN architecture. Now days, a number of commercial

wireless SNs are available for different industrial & home automation applications. Table 1 shows the basic requirement for sensor node device.

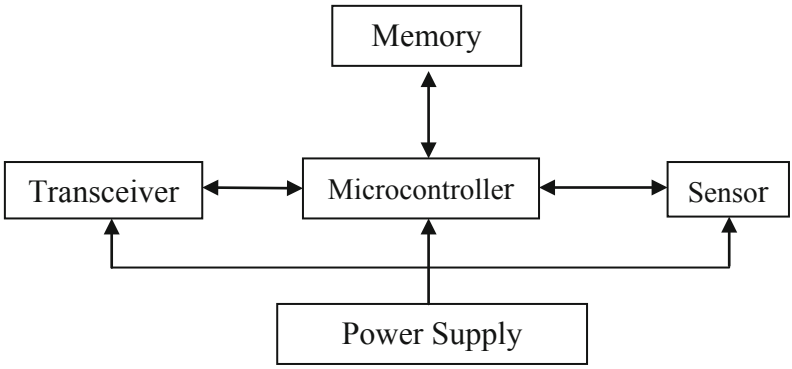


Fig. 3. Sensor node architecture

Table 1. Sensor device specification

Component	Specification rating
Processing Speed	4 MHz
Internal Memory	4 KB RAM
External Memory	128 KB Flash
Radio Communication	916 MHz 40 Kbps
Power Management	2 AA Batteries

Since we have very limited power of sensor node so we have different methods to maximize the use of battery power like different routing algorithms which can consume less power to send the data to base station, different types of sensor node used in the network can increase the life of wireless sensor network. We can also increase battery life by using proper standards of wireless networks. We have different wireless sensor network protocols like ZigBee, Wireless HART and ISA.100, IEEE 1451 and IEEE 802.15.4 which are released for wireless network and is interesting for industrial applications [1, 2].

The mostly used wireless sensor network standard is IEEE 802.15.4 which have many variants. The key element of IEEE 802.15.4 is low power as it is used in many areas where sensors are deployed remotely and need to operate on battery power without attention.

The IEEE 802.15.4 standard is used for the first two layer of OSI model as shown in Fig. 4 i.e. the physical layer and MAC layer of LoWPAN. This protocol is used for low-power and low-rate communications, mainly suitable for embedded devices like sensor nodes. Such protocol allows for duty cycle of sensor nodes from 100% to a minimum value of 0.1% [3].

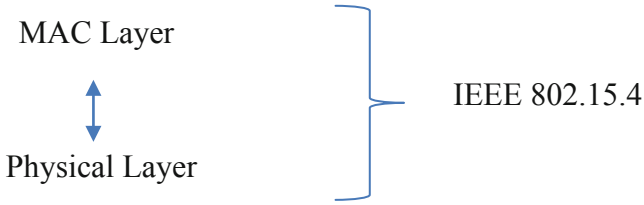


Fig. 4. OSI layers of IEEE 802.15.4

IEEE 802.15.4 standards use MAC layer and physical layer along with Logical Link Control (LLC) and Service Specific Convergence Sub-layer (SSCS) to communicate with upper layers of OSI model as defined by other standards. The 802.15.4 have different versions for different application as shown in Table 2.

Table 2. Different versions of IEEE 802.15.4

S. No.	802.15.4 version	Application
1.	802.15.4a	Base radio protocol
2.	802.15.4b	Base radio protocol
3.	802.15.4c	Used for China
4.	802.15.4d	Used for Japan
5.	802.15.4e	Used for Industrial Application
6.	802.15.4f	Used for RFID
7.	802.15.4g	Used for smart utility network

The IEEE 802.15.4 is used direct sequence spread spectrum (DSSS) modulation. It offers coding gain for improving link reliability and it is highly forbearing of noise and interference. Standard BPSK is used low-speed versions, while offset-quadrature phase-shift keying (O-QPSK) is used for the higher-data-rate version. O-QPSK has a constant wave envelope meaning that more efficient non-linear power amplification techniques can be used to minimize power consumption. With regard to channel access, 802.15.4 uses carrier sense multiple access with collision avoidance (CSMA-CA). This multiplexing approach lets multiple users or nodes access the same channel at different times without interference.

3 Routing in Wireless Sensor Networks

Routing is a path determination process between sensor node and sink upon the requirement of data transmission. In WSN, the network layer is used to route the sensed data. We know if sensor node is not near to sink then sensed data can't reach directly to sink so network uses the multi-hop concept to send the sensed data to the sink. So, the solution of this problem is intermediate sensor nodes those are used to relay their

packets by using the routing-table. These routing-table contain the node option list for any given packet for the transmission to destination. The routing-table performs the task of routing algorithm along with their construction and maintenance using routing algorithm. In general, WSNs are not required routing table for flat and clustering routing approach. For flat routing, data can be directly communicated to the sink, whereas for clustering, cluster head is responsible for the data transmission of the respective cluster. Different routing objectives will be discussed in the next session.

3.1 Key Requirements for the Routing

Selection of appropriate routing is always a challenging issue. However, application plays important role for the selection of a routing protocol. Therefore, in this section we discuss the key parameters for the selection of a routing protocol. Parameters are not limited; we have selected these for our work only.

3.1.1 Network Lifetime

Network lifetime is a crucial parameter for the wireless sensor network. As there is no proper definition for lifetime but as the name suggests, Network Lifetime is time span in which we can get the information from the network as long as. As per the literature, we can divide the lifetime, as per the performance parameter like stability, reliability etc. into three categories like FND, HNA and LNA. FND stands for First Node Die, HNA stands for Half Node Alive and LNA stands for Last Node Die. FND can be stand for the accuracy and stability of the network. HNA gives the information about the sensor nodes that only half sensor nodes are alive and we will get the information with less accuracy. LNA can be stand for the stability with compromise of data reliability.

3.1.2 Optimization

Optimization means to take the maximum output from the available resources. Hence the Optimization in wireless sensor network is very important to take maximum advantage from the network since we have limit resources like limited battery power. Hence we have to optimize our resources to take maximum output from the limited battery power. In WSN, optimization technique can be categories in two parts as static and dynamic optimization. In Static Optimization, optimization will be done at deployment time and will remain same for WSN's lifetime whereas in Dynamic Optimization, optimization will be flexible continuously during the runtime of the WSN.

3.1.3 Data Gathering

Data Gathering is the key function of the sensor node in the network. Sensor nodes gather the information from the environment & forward this information as per the protocol. As a result, data gathering is the most important and very critical function provided by a WSN. In data gathering, sufficient amount of energy is consumed for sensory data. The techniques for data gathering have proposed for WSNs so that energy consumptions will reduce in the network by exploiting correlations among sensed data. We can classify them into two categories broadly as compression-oriented and networking-oriented [4]. The most common application of data gathering is agriculture

which required precision in real time data gathering and that data can be used by other user with the help of sensor cloud [23].

3.1.4 Data Aggregation

Data Aggregation is the technique to combine the information received from various sensor nodes. Since every sensor node collect the information from the region and send to the cluster head. In such case, Cluster Head will have redundancies about the information so in such case Cluster Head will aggregate the information. After the aggregation of the information, this will have transferred to the base station. Different techniques for data aggregation have been proposed to reduce the redundancy of data also collected from sensor nodes before transmitting to the sink, while data aggregation occurs at the cluster head (CH) level [5].

3.1.5 Data Delivery

In some application of WSN, they require only the successful delivery of messages between the sink and sensor node. However, there are many applications that require more assurance. There are several issues for the appropriate routing, we are selecting only few and are not limited to this work only. Data delivery packets from sensor node to the sink can be time specific or not. These are known as real time delivery and non-real time delivery; next session will give the brief explanation of both.

(a) Non-real time delivery:
In some application, it is requisite that the message must be delivered in all routing protocols but the delivery time is not important. It means that the routing protocol should find the route between the sensor nodes and sink and deliver the data to sink irrespective of time delay. This assurance delivery can be confirmed in a formal way, while the performance can be evaluated by delivery ratio.

(b) Real-time delivery:
In some application, it is requisite that the message must be delivered in all routing protocols but the delivery time is play a crucial role, otherwise the importance of message becomes useless or its content of information is declining after the confined time. Therefore, the main purpose of such protocols is to control the network delay effectively. Hence the average performance of such protocols can be assessed by measuring the delivery ratio within time frame.

4 Classification of Routing Protocols in WSNs

WSN has no wired infrastructure whereas wireless links are not reliable, sensor nodes may be failed but routing protocols have to strictly save the energy requirements [6]. WSN Routing Protocols can be classified in three ways as per the routing paths are established, as per the network structure, as per the protocol operation. In [59], author has provided a detailed review on routing protocol. Figure 5 shows the classification of WSN routing protocols.

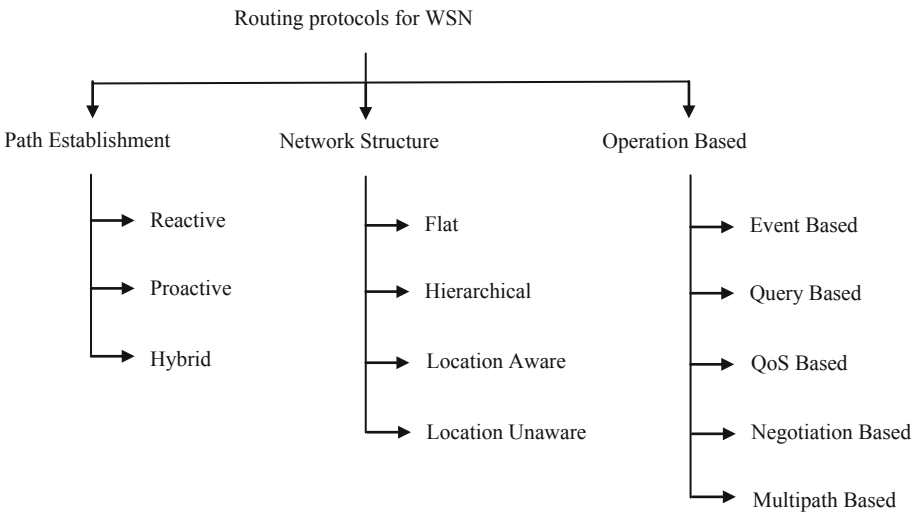


Fig. 5. Classification of routing protocols in wireless sensor network

4.1 Path Establishment

Routing paths can be established in one of the three ways, such as reactive, hybrid, or proactive path.

4.1.1 Reactive Protocol

In reactive protocols [7], it computes the routes only when it is needed. Some application like water requirement in the crop, requires the information on particular time, in such case sensor nodes will find the route to send the information. It means that this protocol finds the route only on-demand basis. The best example of such protocol is "Ad-hoc On Demand Distance Vector (AODV)". Route discovery and Route maintenance are the two basic operations in AODV protocol. For route discovery and route maintain, it requires three messages as (i) RREQ as Route REQuest, (ii) RREP as Route REPly and (iii) RERR as Route ERRor messages [8]. For route discovery, a sensor node, acts as source, needs a route to reach the another sensor node, acts as destination, a RREQ signal is generated in the active network. As soon as a destination sensor node receives request, it will check previous requests if it is former one, it rejects the RREQ signal else it will update the routing table. In this way, the destination sensor node sequence number refreshed in the route list. For the route maintenance, if there is detected any breakage in the active link route, the sensor node informed to the source node about the link breakage by a RERR message signal. Now the source senor node will again start searching the route searching process if source sensor node requires to send the data. Flooding [9], Gossiping [10] and TEEN [11] are some more examples of reactive protocol.

4.1.2 Proactive Protocol

Proactive protocols [12] are such protocols in which the selection of the entire route is discovered before their requirement and the routing table saves them. When a set route alters, the altered route has to be updated throughout the network. Since a sensor network might have a large number of sensor nodes, the fixed routing path has to keep the record of each sensor node that will be vast & so that proactive protocols are not suitable for sensor network. So to improve this problem, a protocol is proposed as "Optimized Link State Routing protocol (OLSR). In this protocol, control message has been flooded in the network by selected sensor node which are called MPR (Multi Point Relays) [8]. So with help of MPRs, such proactive OLSR protocol are suitable for those application where active devices pairs are changeable with time. So such protocol is suitable for traffic system where a large number of vehicle are interactive to each other.

4.1.3 Hybrid Protocol

ZRP [13] is the hybrid protocol which uses a combination of two protocols i.e. reactive & proactive protocol. ZRP uses two sub-protocol like IntrA-zone Routing Protocol (IARP) and Inter-zone Routing Protocol (IERP). The IARP (proactive routing) is generally used within the routing zone of the node and IERP (reactive routing) is used between routing zones. ZRP also uses a technique known as Bordercast Resolution Protocol (BRP) to manage traffic between zones. BRP is used to spread the reactive route request, if a sensor node has no topology information given by IARP. Intra-zone routing protocols keep an up to date information of the zone topology, which results in no initial delay while sending information to the destination nodes within the zone. The IERP get rid of the need for nodes to keep a proactive fresh state of the entire network.

4.2 Network Structure

In general, network structure routing can be classified into four categories in WSN referred as (i) flat-based routing, (ii) hierarchical-based routing, (iii) location aware and (iv) location unaware based routing. In first routing which is flat-based, each sensor node plays the similar role. In second routing which is hierarchical-based, each node will play dissimilar role in the active network. In third routing which is location-based, sensor node's position is exploited to route data in the network rather in whole network.

4.2.1 Data Centric Protocol

It is impossible to allocate address identifiers to each & every sensor node due to the enormous of sensor nodes in the networks. Such shortage of address identification and random positioning of sensor nodes, it creates the difficult to select an explicit set of sensor nodes. Therefore, data is conveyed from each node in the selected area with weighty amount of data. This concept has led to data-centric routing. The sink sends request to certain regions and waits for the data from the sensors nodes located at the selected regions in data-centric routing. SPIN [14], Direct Diffusion [15] and many more protocols are the example of data-centric routing as shown in Fig. 6.

Directed Diffusion (DD): Directed diffusion [15] is an example data-centric routing protocol for WSN. It come across the main desires of WSN for example energy

efficiency, robustness and scalability. Directed diffusion has different key parameters such as data propagation, interests and gradients, data naming, and reinforcement. In the establishment process of the directed diffusion, the sink insists on a low data rate for incoming events. In this process, sink will send its interest to its neighboring sensor node. Sensor node will keep it in cache and as soon as the event occurred, it will send the data to sink. It differs from SPIN [14] like sensor node will send the data which sink demands whereas in SPIN, sensor node will send the availability of data if sink requires.

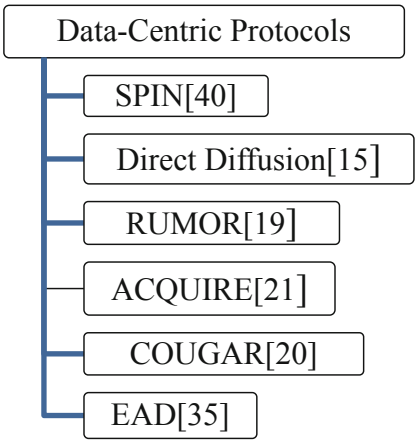


Fig. 6. Different data-centric protocols

RUMOR: Rumor [19] is another data-centric protocol which works on the basis of Direct Diffusion [15] but has the different flooding. It is the middle ware routing protocol for query & event flooding. It is based on to target such sensor node which has particular information rather than to announce every sensor node. This protocol uses agent that has the information about event occurred in the region. This protocol maintains only single path between source node and destination node whereas DD used multiple path between source node and destination node [53].

COUGAR: Cougar [20] is another data-centric protocol which is based on leader node that can take readings from other nodes, & averaging them if it is more than the threshold value than it will send to BS. This protocol proposed the architecture for sensor data-base system in which sensor nodes chooses its leader node. This architecture provides support for computational capability within the network. Every protocol has its own disadvantage like it has that it increases additional query layer for every sensor node that increase overhead cost of energy consumption [53].

ACQUIRE: ACQUIRE [21] is another data centric routing protocol which is abbreviated ACtive QUery forwarding In sensoR nEtworks (ACQUIRE). It is most appropriated protocol for complex queries which have many sub queries along with

distributed database. ACQUIRE proposed for one shot and complex queries in which several sensor nodes provided many responses.

4.2.2 Hierarchical or Clustering Protocol

Hierarchical or Clustering network are used in routing protocol to manage the additional burden and cover the huge region without degrading the performance. Since the sensors nodes cannot accomplish the long distance communication then sensor node required a hierarchy of several nodes to send the data for a huge number of sensors nodes. Hierarchical or cluster routing protocol mechanism in two different stages. In the 1st stage, cluster head (CH) is selected and in the 2nd stage, routing is selected. Clusters are formed to make efficient routing network and data aggregation or data fusion are assigned to them as the special tasks. Such technique upgrades the scalability, increases the network lifetime and more energy efficiency.

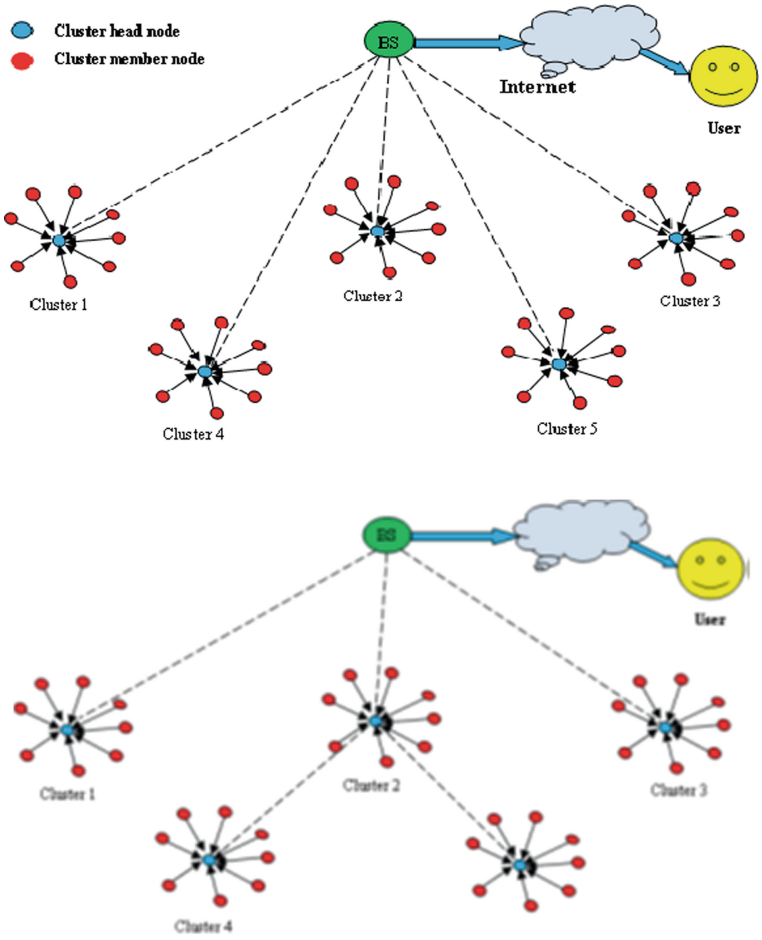


Fig. 7. Hierarchical routing through other CH or directly CH to Base Station [28]

In hierarchical approach, different clusters are formed of different sensor nodes on the basis of their energy levels. Sensor nodes are grouped into different clusters with a cluster head (CH) that has the responsibility of routing from the one cluster to the other cluster heads to base station or directly send to base station [24]. Data transfer from a lower cluster level to a higher cluster level as shown in Fig. 7. Although, it transfers from one SN to another SN, but as it transfers from one level to another level, it covers larger distances. Such movement transfer the data faster to the base station. On the basis of different sensor node energy, we can also classify these hierarchical protocols into two more groups as shown in Fig. 8. Homogeneous protocols are those which have all the sensor nodes with equal energy like [16] whereas heterogeneous protocols are those which have different energy levels of sensor node. Such sensor nodes are known as Intermediate SN, Advance SN, Super SN etc.

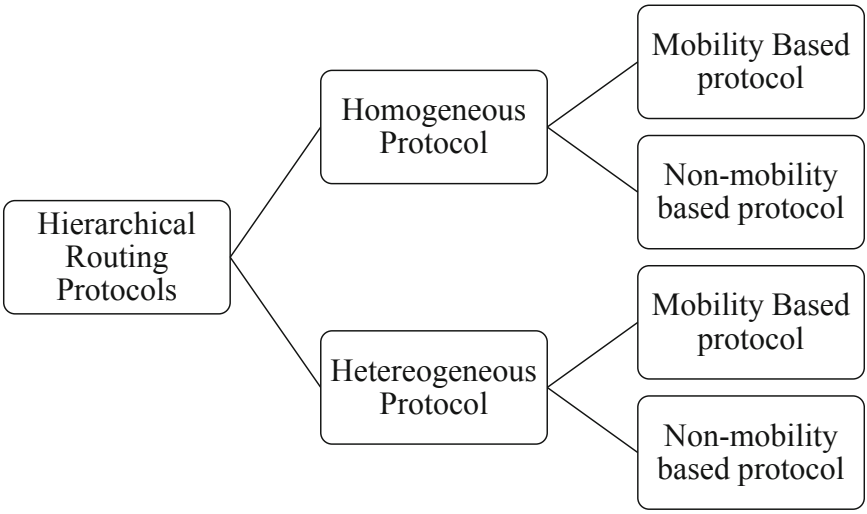


Fig. 8. Classification of hierarchical routing protocol

Homogeneous Routing Protocols: Homogeneity of sensor node depends on the characteristic of sensor node. The characteristic of sensor node can be energy of the sensor node, number of sensor node in the field, different type of sensor node etc. So generally on the basis of energy, we classified routing protocols. In this section, we discussed very basic protocols of homogeneous routing protocol. Summary of such homogeneous protocol are tabulated in Table 3.

Low Energy Adaptive Clustering Hierarchy (LEACH): LEACH [16] is hierarchical clustering protocol for WSN in homogeneous environment. LEACH is the most promising and popular energy efficient hierarchical clustering protocol for sensor network. It is very basic protocol for clustering that proposed for decreasing energy consumption. LEACH arranges the sensor nodes into small regions known as cluster and selects one of them as the cluster-head (CH). Sensor nodes first find its cluster head and then send the significant information to its CH. After that the CH aggregates the

data and compresses the information received from the sensor nodes and sends it to the base station (BS). Hence LEACH uses random rotation of the sensor nodes required to be the cluster-heads to equally distribute energy utilization in the network. TDMA technique is used to reduce inter cluster and intra cluster collisions. Operation of LEACH is divided in two phase like (i) setup phase and (ii) steady state phase. In the first phase, the clusters are created and a cluster head (CH) is chosen for each created cluster. Whereas in the second phase of operation, required information is sensed using sensor and sent to the BS. The period of steady state phase is longer than the period of setup phase so that it can reduce the cost of overhead.

A. **Setup phase:** During the first phase, a predefined probability (p) of sensor nodes are selected themselves as cluster head (CHs). This is done as per the threshold value T(n) as defined the given equation. The threshold value is selected on the basis of predefined probability to become a CH (p), r the value of current round and sensor nodes which have not selected from the last1/p rounds, which is denoted by G. Threshold value T(n) can be defined as:

$$T(n) = \begin{cases} \left\{ \frac{p}{1-p*\left(r*\mathrm{mod}\left(\frac{1}{p}\right)\right)}, & n \in G \\ 0, & otherwise \end{cases} \right.$$

B. **Steady phase:** In the steady state phase, sensor nodes start sensing the required information and send it to their respective CH according to the decided TDMA schedule. As soon as information received from respective CMs, CH aggregates the received data and transmits to the BS after a definite time. As soon as, the data transmits to BS, the network will start again to setup phase and new CHs are elected. Every CH communicates with BS using different CDMA code so that it can reduce interference from sensor nodes belonging to other CHs.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS): Lindsey et al. [24] proposed a "Power-Efficient Gathering in Sensor Information Systems (PEGASIS)" which forms the chain of sensor nodes rather than clustering the sensor nodes, so that every sensor node can transmit & receive the information from a neighboring sensor node & only and only one sensor node is selected from the selected chain to send the received information to the BS. The information is gathered and transmitted from one sensor node to neighborhood sensor node, aggregated and ultimately transmit to the BS through CH. The chain creation is performed using greedy algorithm. Unlike LEACH protocol, PEGASIS avoid cluster creation and uses only one sensor node in a chain to transmit the information to the BS instead of multiple CHs. PEGASIS introduces an excessive delay for distant sensor node on the chain. Major problem is that if CH dies in between the processes of data communication then CH become a blockage. Finally, although in most circumstances, sensor nodes will be immobile or fixed as assumed in PEGASIS, some sensor nodes may be allowed to move and hence can affect the protocol functionality.

LEACH-SF [35] proposed an algorithm which used adaptive fuzzy clustering by Sugeno fuzzy inference system & fuzzy c-means are adopted to create a cluster in

which all SNs participate into balance clustering and choosing efficient CHs, one-to-one. If we compare it with further protocols, it applies artificial bee colony algorithm to amend the fuzzy rules for LEACH-SF.

UMBIC [36] proposed a new protocol to address hot-spot problem in which neighboring CH to BS acts as relay node for distant CH & it deplete its energy quickly so authors proposed "Unequal Multi-Hop Balanced Immune Clustering protocol" in which this protocol is bifurcated into two parts so that the energy depletion can be balanced. In the first part of the protocol, it uses unbalanced clustering approach i.e. UCM for energy consumption of within cluster in which the active network is bifurcated into unbalanced cluster depends on the remaining energy of the SN & distance from sink and in the second part of the protocol, it uses MOIA i.e. the algorithm for multi objective for energy consumption of different cluster in which optimum cluster is built in the network so that it generate a tree for routing among SNs so that entire network is covered.

E-LEACH-SC [17] proposed selective cluster based homogeneous wsn for temperature monitoring system. It is used for specific body area monitoring system for health care. In this protocol, data is transmitted from ill persons using direct transmission & selective cluster based transmission.

HHO-LEACH [22] proposed hybrid homogeneous routing protocol for wsn in which author used learning automata (LA) and Bayesian Coalition Game (BCG). Sensor nodes are assumed as player using distance as threshold for making partition in the network field. Whoever sensor node is near to base station will transfer the data using single hop.

Table 3. Parameter comparison of homogeneous routing protocols

Protocols	Year	Mobility	Hopping	Clustering	Topology	Selection of CH	Stability
LEACH [16]	2002	Static	Single-hop	Intra Cluster	Distributed	Probabilistic	–
PEGASIS [24]	2002	Static	Multi-hop	–	Distributed	–	–
LEACH-AP [25]	2016	Static	Single-hop	Intra Cluster	Distributed	Probabilistic	Moderate
UMBIC [36]	2016	Static	Multi-hop	Intra & Inter Cluster	Distributed	Probabilistic	High
LEACH-SF [35]	2017	Static	Single-hop	Intra Cluster	Centralized	Fuzzy based	High
HHO-LEACH [22]	2015	Static	Single-hop	Intra Cluster	Distributed	Bayesian Coalition Game based	High

Heterogeneous Routing Protocols: Heterogeneity of sensor node depends on the characteristic of sensor node. The characteristic of sensor node can be energy of the sensor node, number of sensor node in the field, different type of sensor node etc. So

generally on the basis of energy, we classified routing protocols. In this section, we discussed very basic protocols of heterogeneous routing protocol. Summary of such heterogeneous protocol are tabulated in Table 4.

Table 4. Parameter comparison of heterogeneous routing protocols

Protocol	Year	Mobility	Hopping	Clustering	Heterogeneity	Selection of CH	Stability
EHE-LEACH [26]	2013	Static	Single	Intra Cluster	Two Level	Probabilistic	High
ETSSEP [27]	2015	Static	Single	Intra Cluster	Three Level	Probabilistic	Medium
LE-MHR [28]	2015	Static	Multi-hop	Inter Cluster	Multi-Level	Probabilistic	High
SEECP [29]	2017	Static	Multi-hop	Inter Cluster	Three Level	Deterministic	Medium
SEEC [31]	2017	Static	Single-hop	Intra Cluster	Two Level	Fixed	Medium
MLHEED-n [32]	2016	Static	Multi-hop	Inter Cluster	n^{th}-Level	Fuzzy based	High
ACDH [33]	2017	Static	Single-hop	Inter Cluster	Two Level	Probabilistic	High
DDLE [30]	2019	Static	Multi-hop	Inter Cluster	Three Level	Deterministic	Medium
LA-EEHSC [60]	2014	Static	Multi-hop	Inter Cluster	Two Level	Learning Automata	High
DB-MCR [61]	2015	Static	Multi-hop	Inter Cluster	Two Level	Cognitive Radio-based	High

LE-MHR [28] is multi-levels heterogeneous routing protocol for wireless sensor networks. In this protocol, authors have proposed k levels horizontal energy heterogeneity which improves network lifetime at a significant level.

LA-MHR [18] is multi-level heterogeneous routing scheme based on learning automata for WSNs. Authors addressed the communication power consumption than computation power consumption which consume more power. So for improvement in communication power, S-model based learning automata (LA) is used for cluster head selection which showed sufficient improvement as compare to E-SEP, LA-EEHSC, and MCR.

SEEC [31] has proposed stable and energy efficient clustering protocol for heterogeneous WSNs. In this paper network has divided into several cluster in which each cluster has only Normal Nodes (NN) which sense the data and transmit to CH. Each cluster has only one Advance Nodes (AN) which collected the data and transmit to base station. In this protocol advance nodes make sure have enough energy and maintain minimum energy with respect to normal nodes.

MLHEED-n [32] has proposed multilevel heterogeneous network model which is based on HEED protocol. In the proposed Multi Level HEED protocol, the heterogeneity is divided into nth-level. This protocol has two parameters as primary &

secondary parameter. The primary parameter decides the heterogeneity level using the secondary parameters. At every level of heterogeneity, the numbers of nodes are determined by the secondary parameter. The MLHEED protocol has implemented fuzzy in which four variables are used for deciding the cluster head like residual energy, node density, average energy and distance between BS and SNs.

ACDH [33] proposed dynamic heterogeneity of sensor node in terms of energy in which they combined static heterogeneity and dynamic heterogeneity. They added a certain percentage (%) of SNs in the active network during the operations are evolved. In this protocol, CH is elected as per the initial energy of the SN, remaining energy of SN & average remaining energy of the entire network.

DRESEP [34] proposed Residual Energy Efficient Stable Election Protocol (DRESEP) based on distance for wireless sensor network. This is event driven protocol and a reactive algorithm. It uses dual hop communication between CH and BS to balance the load. This protocol improved the utilization of energy and network lifetime significantly.

Kumar *et al.* [54] proposed node energy based approach to improve network lifetime and throughput in WSN for heterogeneous environment & cluster based approach. They have proved that more than 30% heterogeneity of advance node is not good for network.

HetSEP [56] proposed node heterogeneity at five levels. It is based on stable election protocol (SEP) and generate heterogeneity as HetSEP-1, HetSEP-2, HetSEP-3, HetSEP-4, and HetSEP-5 which shows that they have increased the lifetime because of increased energy.

4.3 Location-Aware Protocols

In such protocol, the location information is needed in order to calculate the distance between two particular sensor nodes so that energy consumption can be calculated. Generally, two techniques can be used to find location; one is to find the coordinate of the neighboring sensor node and second is to use Global Positioning System (GPS). Since, there is no addressing scheme for sensor nodes like IP-addresses and they are randomly deployed on a region, location information can be utilized in the routing path in an energy efficient way. Location Aware Routing Protocol is such as PEGASIS [24], HEED [37] etc.

4.4 Location-Unaware Protocols

In such protocol, the location information of the sensor node is not known in order to calculate the distance between two particular sensor nodes so that energy consumption can be calculated. Location Unaware Routing Protocol is such as LEACH [16], LEACH-C [38], SEP [39] etc.

4.5 Operation Based Protocol

We have different protocol based on different operations such Event based, Query based, QoS based, Negotiation based and Multipath based routing protocol.

4.5.1 Based on Event Routing Protocol

This protocol is event based protocol in which all the sensor nodes will sense the information and send the information when a particular event will occur. In many sensor network applications, it is sufficient to have the information only when event will occur. This is very important wireless sensor application for Seismic event. Such protocol is very important in terms of energy consumption.

4.5.2 Based on Query Routing Protocols

Query-based routing protocol is designed for both energy and distance under consideration during packet transformation across the network. In such routing protocol, the source nodes propagate a query for data through the network and the node that having the data sends back to the required node. Usually such queries are used in natural language, or in high-level query languages. These protocols are divided into two phase (1) Query broadcasting (2) Data forwarding as shown in Fig. 9 [47].

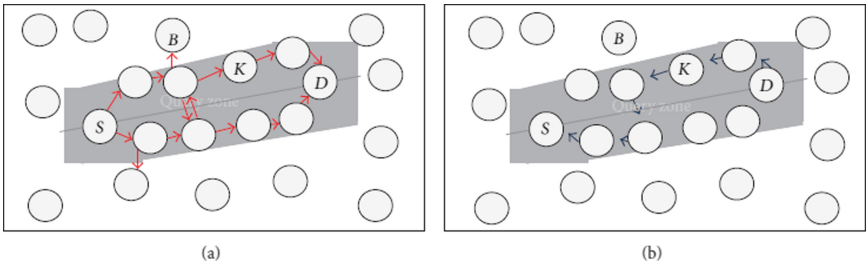


Fig. 9. Query based mechanism (a) Query broadcasting (b) Data forwarding [47]

DECSA [48] proposed optimization algorithm which optimize the criteria of CH election to guarantee the effective transmission and query based routing protocol in WSNs. This algorithm is hybrid optimized algorithm which is the integration of two algorithms i.e. crow search algorithm & dolphin echolocation algorithm such that the hybrid optimization insures the election of CH based on the different constraints effectively & with high conjunction rate.

RER [50] proposed query-based applications and real time energy efficient routing protocol in WSNs which offers an efficient routing protocol between traditional energy balancing and energy saving objectives while supporting a soft real time packet delivery. With the help of fuzzy sets and learning automata techniques, this protocol achieved less energy consumption along with zonal broadcasting.

4.5.3 Based on QoS Routing Protocols

Quality of Service (QoS) is the another important parameter to provide the energy efficient in the sensor network. We can have the following parameters in QoS for example, time delay, bandwidth, reliable delivery of data etc. While delivering the data to destination sensor node, it must have reached within time frame so that balance can maintain between energy consumption and quality of data.

EQSR [49] proposed the protocol which maximize the network lifespan using balancing energy consumption through multiple sensor nodes. This protocol based on TAT (Turn Around Time) in which highly important required data must reach the destination within acceptable time that reduces delay among different paths & increases data redundancy at destination and improve the throughput. By using the following parameter like SNR, residual energy & buffer size of available sensor node, this protocol selects the appropriate hop in the route establishment phase [41].

TAEROR [55] proposed the protocol for trust aware reliable opportunistic routing protocol in which relay selection algorithm is used to avoid malicious node. Authors proposed trust factor in which they consider about energy, forward sincerity & sincerity acknowledgement.

HHE-LEACH [57] is proposed for coverage of sensing area. It is the most important to receive fruit full information from the sensing area. For achieving this, author used learning automata (LA).

MRD [58] is proposed for QoS based & energy efficient protocol for prolong life time of the network. In this protocol, author used sink based multi path diversity for finding the shortest path to reach the base station.

4.5.4 Based on Negotiation Routing Protocols

The routing protocols which are based on negotiation improves the energy efficiency of the network. Based on data flooding in the network, among sensor nodes, a large amount of data is overlapped that consume a lot of processing time & energy of the sensor node. So the main motivation behind such protocol is to reduce the data redundancy at the sensor nodes so that the duplicate data can't be reach the destination sensor node or sink & can save the energy of the sensor node that can participate in the network for longer time.

Sensor Protocols for Information via Negotiation (SPIN): SPIN [40] is data centric protocol which was designed to rectify the problem of classic flooding & find the solution of implosion and overlap. In this protocol, the key feature is "meta-data" which was exchanged among sensor nodes. As soon as, new meta-data is received, neighboring sensor nodes would update its data through a request message. Such mechanism removed the problem of flooding and avoid redundant data which improved the energy efficiency. In this protocol, three messages were used to update the data like ADV, REQ & DATA [53]. The advantage of this protocol is reduced the redundant data so that energy consumption will reduce but it didn't provide delivery guarantee of data. Hence this protocol is not suitable for detection of intrusion.

4.5.5 Multipath Routing Protocols

If we have only single path for data routing, it can create problem some time such as the route has broken down then in such case, the required data can't be reached to the destination. Because of this problem, multipath routing protocols are introduced which uses different routing path for data transmission and can enhance the performance of network. When the primary path fails between the source and the destination node then a secondary path exists for the delivery of the data. This can be increased by

maintaining multiple paths between the source and the destination nodes. But such routing technique increases the energy consumption and traffic. The secondary paths are kept alive by sending messages. Due to such protocol, network reliability can be increased but on the cost of overhead of maintaining the alternate paths. Such protocols are also as energy aware routing (EAR) protocols. The objective of such protocols is to maximize the system lifetime [41].

Energy-Efficient Multipath Routing Protocol (EEMR): EEMR [42] proposed a scalable, distributed, and localized multipath search protocol to discover multiple node-disjoint paths between the sink and source nodes. It is also a load balancing algorithm to distribute the traffic over the multiple paths discovered. This protocol showed higher node energy efficiency, lower average delay and control overhead.

Maximally Radio-Disjoint Multipath Routing (MR2): MR2 [43] proposed a protocol which provide the necessary bandwidth to multi-media applications using radio disjoint paths so that the network lifetime can increased. In this protocol, one path is built at once for a given session and other path is built when it is required such as path congestion or lack of bandwidth [41].

Energy-Efficient and Collision-Aware Multipath Routing Protocol (EECA): EECA [44] is a disjoint multipath routing algorithm for WSNs. This protocol is used the broadcast nature of wireless communication to avoid collision between two discovered routes without extra overhead. This protocol restricts the route discovery flooding and adjusts node transmit power with the aid of node position information, resulting in energy efficiency and good performance of communication that proposed scheme in terms of the average packet delivery ratio, the average end-to-end delay, the average residual energy, and the number of nodes alive [41].

Energy Constrained Multipath Routing (ECMP): ECMP [45] protocol proposed efficient bandwidth utilization along with minimal usage of energy. The strength of the ECMP model is that it selects minimum number of hops and minimum energy by selecting a path with minimum number of hops only when it is the path with minimum energy or a longer path with minimum energy satisfying the constraints. It shows that the QoS should be based on well-defined constraints to avoid unnecessary energy consumption when delivering data. It has a designing challenge for such an energy constrained network [46].

5 Conclusion

As we have seen in the literature review of many researchers, wireless sensor network is promisingly increasing application in different fields day by day. Now-a-days WSN is the integral part of IoT. Hence we have to focus on every corner of prospect of the WSN, in which energy efficiency and routing protocol is the most important prospect because every sensor node is operated only on battery and the power management is very critical. Power management is done in circuitry operation and data transmission. power consumption in circuitry operation can be controlled at hardware level and on

the other hand, we have to control the power consumption on routing level. Hence in this chapter, we show different routing protocols that perform energy efficiency using data routing from source sensor node to destination sensor node i.e. sink or base station. Further, using the perfect routing protocol may enhance the energy of the sensor node & increase the overall energy of the network.

As we have seen that IoT is very fast growing field in this era in which WSN is playing very vital role. Since sensor nodes are integral part of IoT hence this chapter is very useful for upcoming researchers for understanding the importance of energy efficiency & routing protocols. As the scope of IoT is increasing day by day hence undoubtedly number of sensor nodes will increase and the problem of energy efficiency will come. Hence this chapter will provide a significant help to researchers.

References

1. Radmand, P., Talevski, A., Petersen, S., Carlsen, S.: Comparison of industrial WSN standards. In: 4th IEEE International Conference on Digital Ecosystems and Technologies, IEEE DEST (2010)
2. Kher, S., Chen, J., Somani, A.K.: IEEE 1451 standard and wireless sensor networks: an over view of fault tolerant algorithms, pp. 227–232 (2006)
3. Toscano, E., Bello, L.L.: Comparative assessments of IEEE 802.15.4/ZigBee and 6LoWPAN for low-power industrial WSNs in realistic scenarios (2012)
4. Campobello, G., Segreto, A., Serrano, S.: Data gathering techniques for wireless sensor networks: a comparison. Int. J. Distrib. Sens. Netw. **2016**, 17 (2016)
5. Ullah, I., Youn, H.Y.: A novel data aggregation scheme based on self-organized map for WSN. J. Supercomput. **75**(7), 3975–3996 (2019)
6. Misra, S., Woungang, I., Misra, S.C.: Routing in wireless sensor networks. In: Guide to Wireless Sensor Network. Springer Science (2009)
7. Perkins, C., Belding-Royer, E., Das, S.: Ad-hoc on-demand distance vector (AODV) routing. RFC 3561 (2003)
8. Govindasamy, J., Punniakody, S.: A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. J. Electr. Syst. Inf. Technol. **5**, 1–10 (2017)
9. Kulik, J., Heinzelman, W., Balakrishnan, H.: Negotiation-based protocols for disseminating information in wireless sensor networks. Wirel. Netw. **8**, 169–185 (2002)
10. Hedetniemi, S.M., Hedetniemi, S.H., Liestman, A.: A survey of gossiping and broadcasting in communication networks. Networks **18**, 319–349 (1988)
11. Manjeshwar, A., Agrawal, D.P.: TEEN: a protocol for enhanced efficiency in wireless sensor networks. In: 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA (2001)
12. Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., Qayyum, A., Viennot, L.: Optimized link state routing protocol. IEEE (2001)
13. Haas, Z.J., Pearlman, M.R., Samer, P.: The zone routing protocol (ZRP) for ad hoc networks (2003). draft-ietf-manet-zone-zrp-02.txt
14. Heinzelman, W.R., Kulik, J., Balakrishnan, H.: Adaptive protocols for information dissemination in wireless sensor networks. In: ACM MobiCom 1999, Seattle, WA (1999)
15. Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., Silva, F.: Directed diffusion for wireless sensor networking. IEEE/ACM Trans. Netw. **11**, 2–16 (2003)

16. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Hawaiian International Conference on Systems Science (HICSS) (2000)
17. Tyagi, S., Tanwar, S., Gupta, S.K., Kumar, N., Rodrigues, J.J.P.C.: Selective cluster based energy efficient routing protocol for homogeneous wireless sensor network. In: Wireless BANs for Pervasive Healthcare & Smart Environments, ZTE Communication vol. 12, no. 3, pp. 26–33, September 2014
18. Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S.: LA-MHR: learning automata based multilevel heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of WSN. IEEE Syst. J. **13**(1), 313–323 (2019)
19. Braginsky, D., Estrin, D.: Rumor routing algorithm in sensor networks. In: Proceedings ACM WSNA, in Conjunction with ACM MobiCom 2002, Atlanta, GA, September 2002, pp. 22–31 (2002)
20. Yao, Y., Gehrke, J.: The Cougar approach to in-network query processing in sensor networks. SGIMOD Rec. **31**(3), 9–18 (2002)
21. Sadagopan, N., Krishnamachari, B., Helmy, A.: The ACQUIRE mechanism for efficient querying in sensor networks. In: Proceedings SNPA 2003, Anchorage, AK, May 2003, pp. 149–155 (2003)
22. Tyagi, S., Tanwar, S., Gupta, S.K., Kumar, N., Misra, S., Rodrigues, J.P.C., Khan, S.U.: Bayesian coalition game-based optimized clustering in wireless sensor networks. In: IEEE International Conference on Communication, IEEE-ICC-2015, 08–12 June 2015, pp. 5150–5155. IEEE Communication Society, London (2015)
23. Tyagi, S., Obaidat, M.S., Tanwar, S., Kumar, N., Lal, M.: Sensor cloud based measurement to management system for precise irrigation. In: GLOBECOM 2017 - IEEE Global Communications Conference, Singapore, 04–08 December 2017
24. Lindsey, S., Raghavendra, C.S.: PEGASIS: power efficient gathering in sensor information system. In: Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, MT, March 2002, pp. 1125–1130 (2002)
25. Sohn, I., Lee, J., Lee, S.H.: Low-energy adaptive clustering hierarchy using affinity propagation for wireless sensor networks. IEEE Commun. Lett. **20**(3), 558–561 (2016)
26. Tyagi, S., Gupta, S.K., Tanwar, S., Kumar, N.: EHE-LEACH: enhanced heterogeneous LEACH protocol for lifetime enhancement of wireless SNs. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp 1485–1490 (2013)
27. Kumar, S., Verma, S.K., Kumar, A.: ETSSEP: enhanced threshold sensitive stable election protocol for heterogeneous wireless sensor network. Wirel. Pers. Commun. (2015). https://doi.org/10.1007/s11277-015-2925-x
28. Tyagi, S., Tanwar, S., Gupta, S.K., Kumar, N., Rodrigues, J.J.P.C.: A lifetime extended multi-levels heterogeneous routing protocol for wireless sensor networks Telecommun. Syst. **59**, 43–62 (2015)
29. Mittal, N., Singh, U., Sohi, S.B.: SEECP: a stable energy efficient clustering protocol for wireless sensor networks. Wirel. Netw. **23**, 1809–1821 (2017)
30. Gupta, S.K., Kumar, S., Tyagi, S., Tanwar, S.: Dynamic distance based lifetime enhancement scheme for HWSN. In: Second International Conference on Recent Innovation in Computing, ICRIC-2019, Central University of Jammu, Jammu on 08–09 March 2019
31. Rizk, R., Farouk, F., Zaki, F.W.: Towards energy efficiency and stability in heterogeneous wireless sensor networks. Wirel. Pers. Commun. **96**, 4347–4365 (2017). https://doi.org/10.1007/s11277-017-4390-1
32. Singh, S., Chand, S., Kumar, B.: Multilevel heterogeneous network model for wireless sensor networks. Telecommun. Syst. **64**, 259–277 (2017)

33. Zhang, J., Chen, J.: ACDH: an adaptive clustering algorithm for dynamic heterogeneous wireless sensor networks. Wirel. Netw. (2017). https://doi.org/10.1007/s11276-017-1648-1
34. Mittal, N., Singh, U.: Distance-based residual energy efficient stable election protocol for WSNs. Arab. J. Sci. Eng. **40**, 1637–1646 (2015)
35. Shokouhifar, M., Jalili, A.: Optimized Sugeno fuzzy clustering algorithm for wireless sensor networks. Eng. Appl. Artif. Intell. **60**, 16–25 (2017)
36. Sabor, N., Abo-Zahhad, M., Sasaki, S., Ahmed, S.M.: An unequal multi-hop balanced immune clustering protocol for wireless sensor networks. Appl. Soft Comput. **43**, 372–389 (2016)
37. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad-hoc networks. IEEE Trans. Mob. Comput. **3**(4), 366–369 (2004)
38. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: An application- specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**(4), 660–670 (2002)
39. Smaragdakis, G., Matta, I., Bestavros, A.: SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. In: Proceedings of Second International Workshop on Sensor and Actor Network Protocols and Applications, Boston, MA (2004)
40. Kulik, J., Heinzelman, W., Balakrishnan, H.: Negotiation-based protocols for disseminating information in wireless sensor networks. Wirel. Netw. **8**(2–3), 169–185 (2002)
41. Masdari, M., Tanabi, M.: Multipath routing protocols in wireless sensor networks: a survey and analysis. Int. J. Future Gener. Commun. Netw. **6**(6), 181–192 (2013)
42. Lu, Y.M., Wong, V.W.S.: An energy-efficient multipath routing protocol for wireless sensor networks. Int. J. Commun. Syst. **2007**, 747–766 (2007)
43. Maimour, M.: Maximally radio-disjoint multipath routing for wireless multimedia sensor networks (2008)
44. Wang, Z., Bulut, E., Szymanski, B.K.: Energy efficient collision aware multipath routing for wireless sensor networks (2008)
45. Bagula, A.B., Mazandu, K.G.: Energy constrained multipath routing in wireless sensor networks. In: Ubiquitous Intelligence and Computing, pp. 453–467. Springer, New York (2008)
46. Anasane, A.A., Satao, R.A.: A survey on various multipath routing protocols in wireless sensor networks. Proc. Comput. Sci. **79**, 610–615 (2016)
47. Ahvar, E., Ahvar, S., Lee, G.M., Crespi, N.: An energy-aware routing protocol for query-based applications in wireless sensor networks **2014**, 9 p. (2014). http://dx.doi.org/10.1155/2014/359897. Article ID 359897
48. Mahesh, N., Vijayachitra, S.: Neural Comput. Appl. **31**(Suppl 1), 47 (2019). https://doi.org/10.1007/s00521-018-3637-4
49. RanjideRezaie, A., Mirnia, M.: CMQ: clustering based Multipath routing algorithm to improving QoS in wireless sensor networks. IJCSI Int. J. Comput. Sci. Issues (2012)
50. Ahvar, E., Lee, G.M., Crespi, N., Ahvar, S.: RER: a real time energy efficient routing protocol for query-based applications in wireless sensor networks **61**(1), 107–121. https://doi.org/10.1007/s11235-015-0072-z
51. Tiete, J., Domínguez, F., da Silva, B., Touhafi, A., Steenhaut, K.: MEMS microphones for wireless applications. In: Wood head Publishing Series in Electronic and Optical Materials 2017, pp. 177–195 (2017). https://doi.org/10.1016/B978-0-08-100449-4.00008-7
52. Weiss, J.: New low-power wireless standards expand wireless sensor network applications. In: Wireless Congress 2011: Systems & Applications, Munich, Germany. Dust Networks (2011)
53. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**, 325–349 (2005)

54. Kumar, H., Singh, P.K.: Node energy based approach to improve network lifetime and throughput in wireless sensor networks. J. Telecommun. Electron. Comput. Eng. **9**(3–6), 79–88 (2017). e-ISSN 2289-8131
55. Kumar, N., Singh, Y., Singh, P.K.: An energy efficient trust aware opportunistic routing protocol for wireless sensor network. Int. J. Inf. Syst. Model. Des. (IJISMD) **8**(2), 30–44 (2017)
56. Singh, S., Singh, P.K.: Performance investigation of energy efficient HetSEP for prolonging lifetime in WSNs. In: Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958, pp. 496–509. Springer, Singapore (2018)
57. Tyagi, S., Tanwar, S., Kumar, N.: Learning automata-based coverage oriented clustering in HWSNs. In: 2015 Second International Conference on Advances in Computing and Communication Engineering, Dehradun, pp. 78–83 (2015). https://doi.org/10.1109/ICACCE.2015.20
58. Rishiwal, V., et al.: Base station oriented multi route diversity protocol for wireless sensor networks. In: 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, pp. 1–6 (2018). https://doi.org/10.1109/GLOCOMW.2018.8644227
59. Tyagi, S., Kumar, N.: A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. J. Netw. Comput. Appl. **36**(2), 623–645 (2013)
60. Kumar, N., Tyagi, S., Deng, D.J.: LA-EEHSC: learning automata based energy efficient heterogeneous selective clustering for wireless sensor networks. J. Netw. Comput. Appl. **46**, 264–279 (2014)
61. Tyagi, S., Tanwar, S., Kumar, N., Rodrigues, J.J.P.C.: Cognitive radio-based clustering for opportunistic shared spectrum access to enhance lifetime of wireless sensor network. Pervasive Mob. Comput. **22**, 90–112 (2015)

Security & QOS in Wireless Sensor Networks

Low-Cost Architecture of the Universal Security Threat Detection System for Industrial IoT

M. Hajder[1], P. Hajder[2(✉)], and M. Nycz[3]

[1] University of Information Technology and Management, Rzeszow, Poland
miroslaw.hajder@gmail.com
[2] AGH University of Science and Technology, Krakow, Poland
piootr.hajder@gmail.com
[3] Rzeszow University of Technology, Rzeszow, Poland
mar.nycz@gmail.com

Abstract. The chapter presents the new architecture of the distributed threat detection system for broadly understood information system security. Unlike existing systems, the system is heterogeneous in terms of information, communication, operation and hardware, architecturally using industrial Internet of Things solutions. Additionally, it is separated from the entity's basic IT structure and based on the extensive use of parallel and distributed processing. In most of the available literature, improvements are sought in the way of wireless communication. In this work, the wired communication environment is examined, that is the backbone of any wireless sensor network. From the algorithmic point of view, it uses intelligent data analysis and biologically inspired methods. Communication environment is described using mainly graph theory, graph algebra and probability. The data collected by a heterogeneous group of autonomous traffic analyzers located at all levels of the communication hierarchy of the industrial information system is subjected to permanent analysis. Depending on the operating mode, the analyzers communicate with the central security node in one of three possible, complementary modes of transmission. Operating mode also determine how data is processed. In the simplest case it is carried out on the central node resources. On the other hand, in the most advanced one the system is in fact a parallel computer based on analyzers resources. The proposed architecture in the standard operating mode is integrated with the classic information system, in each of the emergency modes is separated from it. The work ends with the presentation of the empirical research results on the effectiveness of the proposed architecture.

Keywords: Industrial information system · Industrial networks · Self-adjusting communication architecture · Attack detection system · IDEF0 diagrams

1 Introduction

Although in the last years information security has been given a lot of attention, getting a satisfactory solution to the users is still very difficult. There are many reasons for this. First, with the dedication of methods and protection measures developed and

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 301–324, 2020.
https://doi.org/10.1007/978-3-030-40305-8_15

implemented to current threats and organization of information systems. Secondly, the activity of cybercriminals is still growing, which can be explained by the relatively simple obtaining of significant benefits from such activities [1–5]. An example of the correctness of the thesis is the concentration of researchers' interest in the sphere of services, with partial or complete omission of the sphere of production, i.e. the area of industrial information systems (IIS). As a result, research into the security of industrial systems is lagging the mainstream work. The signaled delays were reduced but not eliminated thanks to the research published in 2018–19 [6]. The need for continuous work in the area of security is also the result of permanent changes taking place in the organization, architecture and functionality of the Internet. Typically, existing methods and measures do not provide any acceptable level of security for new services on the network.

When designing new security architectures, attention should be paid to several important phenomena occurring on the IT market. The first is the emergence and intensive development of Edge computing networks, including wide spectrum of organizations and architectures, among others:

- Sensor networks, mobile data collection, mobile signature analysis;
- Shared peer-to-peer and ad hoc networks;
- Local clouds, fogs and computing dews;
- Computational grids and clusters;
- Distributed storage with recovery;
- Remote cloud services and others.

The transfer of resources to the edge of the network significantly changes the approach to information security issues. A lot of research on the network and its operation is still ongoing.

The second phenomenon visibly affecting security is the use of computer networks in industrial systems. It is dated to the beginning of the 90s of 20th century and its effect was previously unknown increase in the range and size of industrial production, as well as a visible improvement in its quality. Over time, edge networks have also found application in industrial systems, bringing with them all the benefits and disadvantages.

Unfortunately, the implementation of new types of network has not been correlated with the unification of communication standards. Currently, there are known over 50 types of industrial networks and data transmission protocols usually named Fieldbus. Among them, the best known are: ProfiNet, HART, Modbus, Profibus, DeviceNet, CAN, CANopen, LonWorks, FoxCom, ControlNet, SDS, Seriplex, BACnet, FIP, ASI, Industrial Ethernet, Wordfip, Foundation Fieldbus, Interbus, BitBus, and others. Only some of them are widely used. Although a special Field Device Tool (FDT) interface has been designed to ensure interoperability between devices, technologies, data transmission protocols, their different versions, standards, generations and manufacturers, the need for communication between various system components remains a problem.

The above conditions significantly impede the use of edge networks in industrial systems. Internet of Things has attracted particularly wide interest among IT

professionals working in industry. Its industrial implementation is called the Industrial Internet of Things (IIoT). The solutions used in it differ from the applications in consumer IT systems – the use of security methods and measures known from classic IoT often turns out to be unsatisfactory.

To illustrate the complexity of the interoperability problem in industrial networks, Fig. 1 one shows its hierarchical mode.

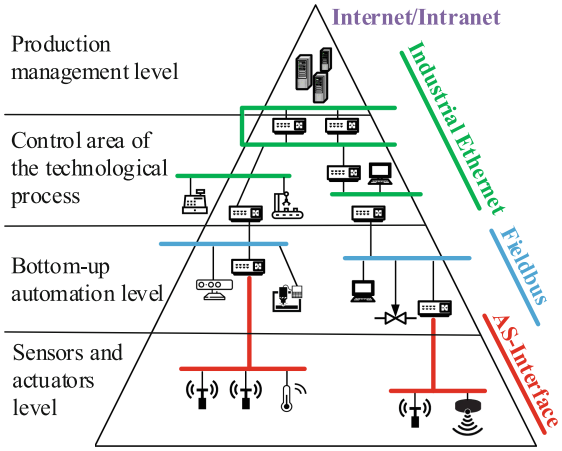


Fig. 1. Hierarchical model of an industrial computer network

The multilayered model shown in Fig. 1 raises another, third problem regarding the construction and operation of security systems. In most Polish enterprises, security is analyzed only at the production management level. Lower levels are rarely or not at all controlled. First, this is due to the communicative and computational heterogeneity of the levels.

The solution to the above problem is to monitor phenomena occurring in IIS using software and hardware traffic analyzers based on Arduino and Raspberry microcomputers. They should be deployed in all network segments, both wired and wireless. For security reasons, they should not be connected to any of the automation, electronics or industrial metrology components used in the system. Thanks to this, the functioning of the monitoring subsystem in any negative way does not translate into the operation of the enterprise's integrated information service system. Unfortunately, in several cases this solution can be troublesome or even impossible to implement. An acceptable solution is the use of the further reconfigurable connection network proposed.

The solution based on the additional sensors analyzing traffic that can operate autonomously ensures a high level of security, but the costs of its implementation are usually unacceptable. Much more interesting may be an organization in which

industrial IT devices would be made in the form of IIoT components, and their use for threat monitoring would be their additional function, available only in special cases. Unfortunately, changes in industrial systems are relatively slow and most of the devices used are not adapted to the IIoT technology. Therefore, the solution offered as part of the described research combines both above approaches. Designer's task will be to look for the golden mean between the level of security and the costs generated mainly by dedicated measuring nodes.

The fourth complicating phenomenon, the operation of the security system, is the degradation of computational and communication resources used in the security subsystem that occurs during the attack. If the threat detection system is considered only as a product based on polynomial combinatorial algorithms or the analysis of limited data resources, the problem of resource deficit rather does not appear. It becomes valid at the time of application of time-complex algorithms, e.g. providing machine learning or analysis modeled on biological phenomena. If the detection system functions as part of the top layer (Fig. 1) during the attack, degradation of its resources is highly possible. Therefore, in most current solutions, independent computing resources are built with low efficiency, designed solely to operate the detection system.

The solution proposed by authors assumes the separation of scaled computing resources, independent of other components of the upper layer of IIS. It was decided to prioritize the procedures for parallelizing processing in a heterogeneous environment with multi-channel optical connections. Communication is based on a bus that has been folded many times, with the possibility of physical division and virtual reconfiguration of the connection network. The first level of parallelization is based on a separate security server and uses CUDA GPU to improve performance of the main computing unit.

At the second level, in a situation of computing power deficit, a heterogeneous computing system using free analyzer resources is dynamically built. A multi-channel optical connection network allows to efficiently connect or disconnect computational nodes from the subsystem. Depending on the formally determined necessity, the subsystem autonomously changes its architecture, organizing its resources to ensure maximum performance and reliability or minimum response time to service requests. In this way, as part of the company's existing IIS, an independent subsystem with variable parameters and characteristics is separated, functioning based on IIoT components. Its task is to detect and counteract threats, its functioning does not affect the operation of IIS.

The solutions described in this chapter have also been used in environmental monitoring system. Soon, such a system will be implemented in one of the satellite cities of Rzeszow.

Due to the large number of symbols used in this chapter, a summary list of the most important symbols and abbreviations has been made in the form of Table 1.

Table 1. A summary list of symbols and abbreviations used

No.	Symbol/Abbreviation	Description
1	IIS	Industrial Information System
2	IIoT	Industrial Internet of Things
3	ADS	Attack Detection System
4	IDEF0	Icam DEFinition for Function Modeling, where Icam – Integrated Computer Aided Manufacturing
5	HPC	High-Performance Computing
6	MTBF	Mean Time Between Failures
7	S_r	Primary servers
8	K_n	Supporting servers
9	B_m	Connection buses

2 State of the Art in the Area of IIS Architecture and Security

2.1 Security of Industrial Information Systems

According to the group of ISO/IEC 27000 standards in the field of information security, detection of security threats is carried out by specially established organizational units of the enterprise, often separated from the IT department. According to [7–11] their basic tasks include:

1. Detection of attacks on resources, including:
   a. Identifying attacked nodes, segments, networks;
   b. Determining the nodes from which the attack is carried out;
   c. Determining the optimal location of analyzers detecting anomalies in the operation of a network segment and others.
2. Prevention of attacks, in particular: setting potential targets, forecasting methods, methods and sources of their implementation, etc.;
3. Detecting cybercriminals' groups and tracking their activity.

The cited sources present the most important methods and means of traditional implementation of the above objectives. Most of the conducted activities are a direct implementation of the recommendations of the ISO/IEC 27 standards. Due to the scale of the problem, these activities are widely known, implemented and documented. Countermeasures are based on the simultaneous use of technical and organizational methods and to a very limited extent involve the system's edge resources [12, 13].

The application of the above methodology in the IoT is not very effective, because a significant part of resources is accumulated in them on the network edge. Methods and means taking into account the above conditions addressed to IoT are discussed, among others in [13–18]. They assume a broader than usual protection hierarchy, the roles in blockchains, new protocols in traditional security services and artificial intelligence methods.

Security in IIoT networks is not the same as security known from the pure IoT. Even though the consequences of lack of protection are as much or more expensive

than in IoT, until recently the protection of IIS has often been neglected. This was due to a mistaken belief that cybercriminals were less interested in industrial networks. At present, IIS security is relatively widely described in recent literature, although the number and content of IIoT publications should be considered insufficient. The results of research in this area were presented, among others in [19–24]. In these publications, IIoT is treated as a subset of IoT, with widespread embedded computing and communication technologies. In the first place, these systems are oriented on the support of sensor technologies, on the collection and transmission of acquired data. In many solutions, security is based on clouds using SCADA technology.

2.2 National Realities of Information Security

The implementation of information security solutions in Polish industry is, as in other countries, a complex task that faces resistance from both employees and management staff. Sociological research in the area of applying modern information technologies, conducted by independent researchers, has repeatedly shown the reluctance of employees at various level to implement new solutions. In their opinion, a desirable solution is a copy of the existing one, made using new information technologies. Being aware of this, the Polish legislature, like other European Union countries, has prepared several legal acts describing the treatment of special groups of information. In this way, nearly 40 legal acts were created defining the rules of treatment, e.g. with public, personal data. The obtained effect was opposite to the intended one – the confusion of applicable regulations meant that the entities covered by them were preparing for possible controls, treating security itself as tertiary goal [25–27]. It is estimated that during the 20 years around 20% of entities did not take any actions related to personal data protection [27].

Some progress in the area of personal data protection has been achieved with the entry of General Data Protection Regulation (GDPR). The main benefit of the Regulation was the creation of user groups responsible for the data protection problem, having in-depth knowledge of a given area, willing to exchange their knowledge.

In addition, all users performing public tasks are subject to the so-called National Interoperability Framework – a document specifying the requirements for information systems in the area of security and accessibility. Unfortunately, this document applies to industrial enterprises to a limited extent.

In their work over the past few years, the authors have proved that in order to make industrial enterprises more interested, the authors consider the following actions to be effective:

1. All security level analyzes and search for threats to IIS were conducted free of charge;
2. The management of enterprises was trained free of charge on information protection;
3. All documents (policies, regulations, instructions for use) were provided free of charge to interested entities;
4. Fees for services were charged only if their implementation could not be carried out by a local IT specialist.

The effect of the above actions was a radical change in the approach to security in several entities cooperating with authors. The solutions described in this chapter,

ensuring the highest available level of security, are implemented in several entities. In each of them, managers consider expenditure on security as a profitable investment.

2.3 Scalability and Parallelism of Processing in Industrial Systems

For industrial IT systems, computational performance is a secondary parameter. Typically, these systems do not perform tasks with a high time complexity, and the range of tasks solved in unchanged and known before. Therefore, the scalability and parallelism of processing are not very important feature in them. However, if such requirements appear before the designer, MPP (Massive Parallel Processing) and CoW (Cluster of Workstations) cluster systems are used for this purpose. A much more important feature from the point of view of realizing the tasks in the system is its availability and related characteristics such as reliability and survivability. Many publications about parallelism and security in parallel systems can be found [28–30].

However, transferring previous scalability and parallel experience to the proposed Attack Detection System (ADS) is not recommended. Note that the detection is based on advanced data analysis collected by sensors installed in various network segments. Insufficient computational performance may therefore be the reason for unacceptable detection delays [31]. In addition, it should be noted that improvement of detection efficiency soon will be obtained by algorithmic methods [19].

Although the scalability of computational system was defined back in the 80, interest in this topic increased noticeably in the mid-90 [32]. Scalability is a property of computer system that provides a predictable increase in selected system properties, such as the number of supported users, response time, overall system performance, etc. [33, 34]. Traditional computer systems use two scaling methods: vertical and horizontal. Vertical scaling consists in increasing the efficiency of processing units, while horizontal scaling their number. Typically, both scaling methods are used, which is possible due to the software compatibility of information processing units in classic computer systems [30].

In IIS, especially in the fragment supporting production technology, the application of traditional scalability may be difficult. In these systems, processing elements are secondary components and any modernization of them usually involves the replacement of components of the lower layers in the system (e.g. measuring sensors). Therefore, such activities are performed much less frequently than e.g. in IT management systems.

There are significant differences in the purpose of scaling. In the case of high-performance computing (HPC) systems, this goal is primarily to increase the computational performance of the system. In IIS, an equivalent scalability goal is to ensure an appropriate level of resource availability. In information management systems, scalability is used for two reasons. First, the conditions of modern business changes so quickly that it is impossible to determine the long-term requirements for computational components of the system. Scalability provides a gradual increase in computational power. Secondly, changes in technology lead to new technical solutions and lower equipment prices, which potentially makes information systems architecture more accessible [35].

The use of traditional solutions for scaling IIS is also limited due to their desire to maximize the efficiency of resource usage. In scalable computing systems, a significant increase in the number of components used leads to a reduction in MTBF coefficient, and approximately 20% of the computational power of HPC systems is lost due to

failure and recovery. Topological conditions of scalability are also important. In HPC systems, the connections of processing elements are based on extensive networks, often having regularity and symmetry properties [36–38]. In IIS, the basis for communication are bus systems and their derivatives [6, 23], in which scaling is much more difficult.

Application of optical connections for scaling of computing systems was proposed back in the 1990s for the area of massively parallel computing [39]. In the area of IISs, electrical communication still dominates [6].

3 Definition of the Design Process

3.1 Mathematical Definition

Let's consider the mathematical definition of the ADS design process, based on the method discussed in detail in [31]. Define the functional of the generalized effectiveness of detection, classification and prevention of attacks, characterizing the stable functioning of IIS in the case of cyber-attacks. This functional has the form:

$$F = f\left[\left(A_{IIS[m,n]}, N_{RAP}\right), \left(N_{OS}, t_{tcc}\right), \left(P_{ISM}, B_{ADS}, S_{ADS}, D_{ADS}\right)\right], \tag{1}$$

where: $A_{IIS[m,n]}$ – attack matrix of known types and IIS components attacked during them, m – number of detected attack types, n – number of attacked components; N_{RAP} – a set of recognizable attack patterns; N_{OS} – a set of IIS operating states, during one technological control cycle; t_{tcc} – duration of the IIS technological control cycle; P_{ISM} – parameter for managing the functioning of IIS; B_{ADS} – a set of methods for detection, classification and prevention of attacks; S_{ADS} – a collection of program and technical means of detection, classification and prevention of attacks; D_{ADS} – a set of actions performed to detect, classify and counteract attacks. A more detailed description of the selected elements of the expression (1) is presented below.

If ADS design is based on functional (1), this process boils down to determining the acceptable subsets of its parameters, ensuring the maximum value of the generalized F index. When searching for a solution, one must consider the limits of parameter values on which efficiency depends directly. We note that the time of the attack detection t_{wyk} is equal to the sum of attack type identification time t_{idn} and the time of its classification t_{kl}, i.e. $t_{wyk} = t_{idn} + t_{kl}$. In order to ensure the stability of the IIS functioning, it is recommended to meet the condition: $t_{tcc} > t_{wyk}$. Combinatorial optimization methods can be used to solve the design tasks presented by the functional (1).

Assume that ADS will distinguish between m types of attacks, which have been ordered in the m-element set $A_{IIS} = \{a_1, a_2, \ldots, a_m\}$, each of a_i, $i = 1, \ldots, m$ elements of which is the identifier of a particular type of attack. Each of the attacks defined in A_{IIS} was described by means of a subset of IIS objects questioned during the execution of an attack associated with a_i. So, $a_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,n}\}$. In the A_{IIS} set, substituting the identifier a_i with its elaborated description, the matrix A_{IIS} with the size $m \times n$ is obtained, containing a list of defined attacks and objects attacked during them. Using the existing designations, this matrix can be written in the following form [31]:

$$A_{IIS[m,n]} = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{bmatrix}. \quad (2)$$

Similarly, other functional (1) components can be defined, which has been accurately presented, among others in [40]. This paper describes other ways of formally defining attack detection systems, including methods that operate in an incomplete specificity environment, using machine learning and Big Data methods.

3.2 Functional Definition

The security of any information system, including an industrial one, equally depends on the organization of the system itself and the conditions of the surrounding environment. To present the above relationships, the information system and its immediate environment are mapped using IDEF0 methodology, designed for functional modeling of business processes [41, 42]. The model of the information system operating in a real environment, made in this standard, is shown in Fig. 2. Such models are also called context diagrams.

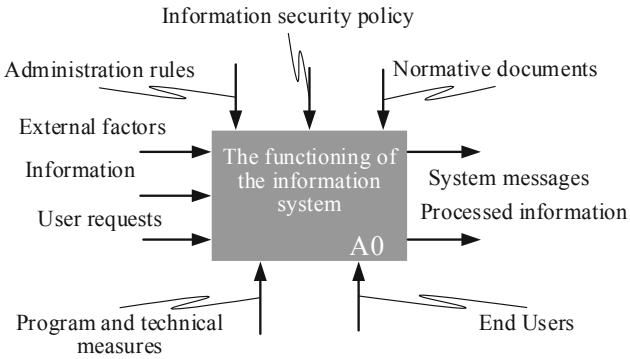


Fig. 2. Context diagram of the information system

This description can be refined using components with the required level of abstraction. Elements of the model are in the form of black boxes which are entered with information processed by the block in accordance with users' requests, as well as external factors that can destabilize the work of the entire system. They can be both catastrophic phenomena and cyber-attacks of varying nature and intensity. The functioning of the information system is determined by its software and hardware resources and end users. In turn, its security is ensured by means of general administration principles, normative documents such as laws, ordinances, standards and the information security policy created on their basis. The result of the system work is processed information and messages notifying, for example, of program execution errors. A detailed context diagram of the information system created by expanding Fig. 2 is shown in Fig. 3.

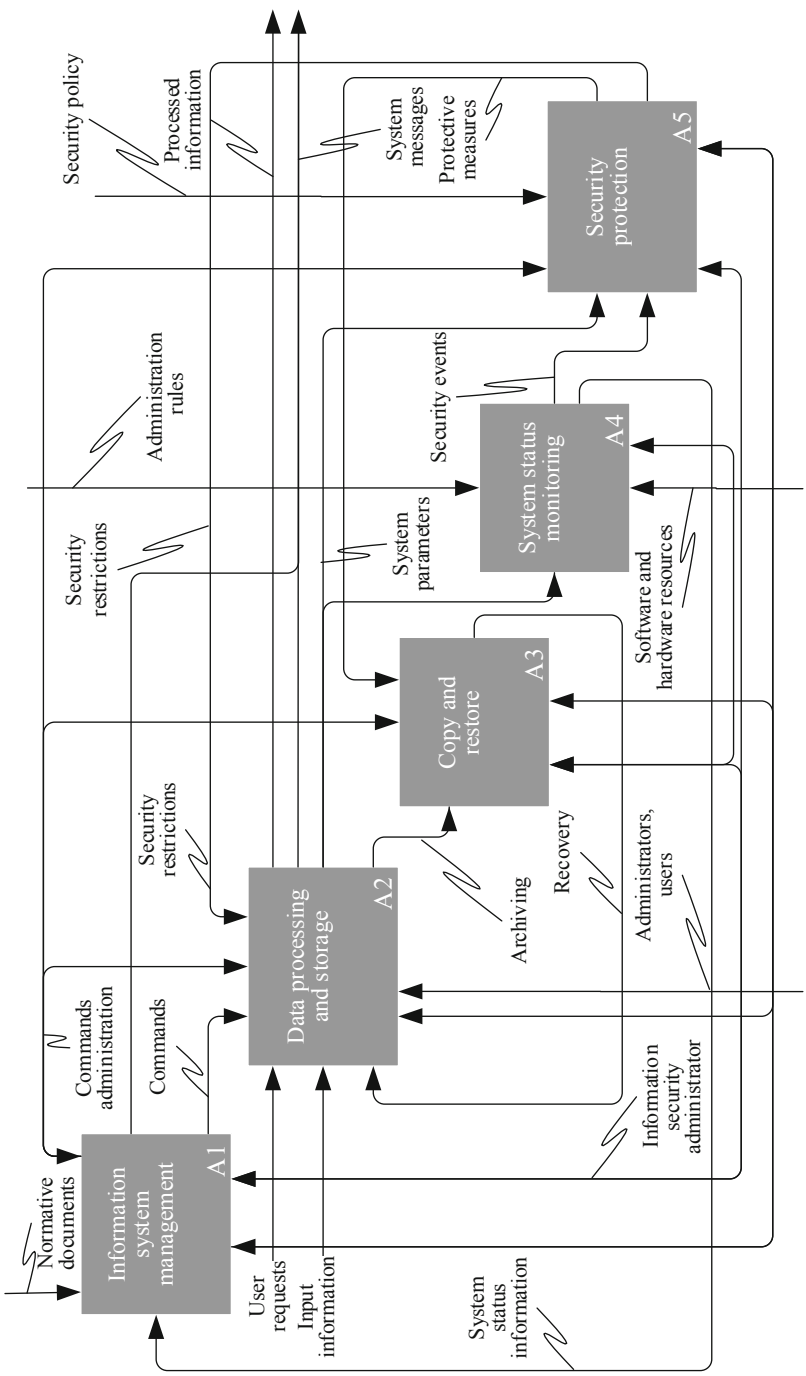


Fig. 3. A detailed context diagram of the information system, including protective elements

The context diagram contains all the most important elements of the information system functioning in real environment. From the security point of view, the A5 block responsible for security protection plays a key role. It derives information for its functioning both from the outside world and from the information system itself.

4 Basic Properties of the Threat Detection System

4.1 Attack Classification

Time has a decisive influence on the level of destruction resulting from cyber-attacks. Therefore, the most important requirement for ADS is real-time attack detection. The main problem of ADS is the instability of functioning when trying to reconcile the restrictions on the length of the IIS technological cycle with the need for rapid detection and counteracting threats. In the event of an attack, the computational and communication components of the system can be overloaded and the minimum cycle length increases. At the same time, detection and countermeasure time should decrease as much as possible.

Attack detection systems based on intelligent data analysis can operate in two modes. The first assumes detection of threats based on a comparison of the characteristic features of current network behavior with the patterns collected in the knowledge base. In this case, meeting stringent time requirements is usually easy. The basis for the functioning of the second mode was the assumption that the attack was new, and its patter is the knowledge did not exist. Therefore, decision-making procedure is longer and may exceed acceptable limits.

To clarify the reason for this behavior, consider the mathematical interpretation of the detection procedure. The basis of ADS's functioning is a classification model, based on which the decision is made to classify the traffic being examined as normal network activity or any of the attacks. Classification, next to detection and counteracting effects, is one of the three main activities of ADS.

Consider the mathematical definition of a classification task. The input set of $\psi = \{\varsigma_1, \varsigma_2, \cdots, \varsigma_k\}$ network activity records provided by the sensors and the output set of $\mathrm{T} = \{\tau_1, \tau_2, \cdots, \tau_l\}$ classes are given. Cardinality of sets ς and T usually meet the condition $|\psi| > |\mathrm{T}|$. Let's assume that the $F : \psi \rightarrow \mathrm{T}$ mapping function exists, meanings of which are known for the value of the finite learning sample $\varsigma^m = \{(\varsigma_1, \tau_1), \cdots, (\varsigma_k, \tau_l)\}$. Therefore, an algorithm $a : \psi \rightarrow \mathrm{T}$ that can classify any record of network activity $\varsigma_i \in \psi$, $i = 1, 2, \cdots, k$ must be constructed [43, 44]. The above task is presented graphically in Fig. 4.

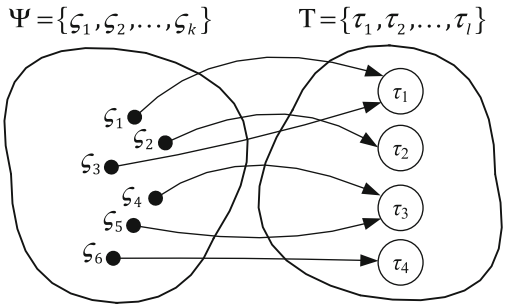


Fig. 4. Graphical illustration of the traffic interpretation task

To illustrate the classification rules, let's consider a trivial example in which we will assign two labels ς_1 i ς_2 to two classes τ_1, τ_2 of network traffic. Four alternative results of this process are possible [31, 44]:

1. The label s_1 is correctly assigned to the type τ_1 i.e. $\varsigma_1 \rightarrow \tau_1$. The probability of correct classification can be calculated using the expression: $P_{p\tau_1\varsigma_1} = P\{\tau_1|\varsigma_1\}$;
2. The label ς_2 is correctly assigned to the type τ_2 i.e. $\varsigma_2 \rightarrow \tau_2$. The probability for correct classification can be calculated using the expression: $P_{p\tau_2\varsigma_2} = P\{\tau_2|\varsigma_2\}$;
3. The label ς_1 is incorrectly assigned to type τ_2. The probability of $P_{n\tau_2\varsigma_1}$ of such an event is equal to $P_{n\tau_2\varsigma_1} = P\{\tau_2|\varsigma_1\}$;
4. The label ς_2 is incorrectly assigned to type τ_1. The probability $P_{n\tau_1\varsigma_2}$ of such an event is equal to $P_{n\tau_1\varsigma_2} = P\{\tau_1|\varsigma_2\}$.

For the example above, the probability P_p of the correct attack classification is equal to:

$$P_p = P_{p\tau_1\varsigma_1} + P_{p\tau_2\varsigma_2} = P\{\tau_1 \,|\, \varsigma_1 \cup \tau_2 \,|\, \varsigma_2\} \tag{3}$$

and incorrect P_n respectively:

$$P_n = P_{n\tau_2\varsigma_1} + P_{n\tau_1\varsigma_2} = P\{\tau_2 \,|\, \varsigma_1 \cup \tau_1 \,|\, \varsigma_2\}. \tag{4}$$

To treat the intrusion detection system as effective, the P_p value should be greater than 95%. Using the method based on conditional probability of events, ADS parameters of any size (number of labels and classes) can be specified. A broader analysis of attack classification is presented, among others in [31, 40] (methods using conditional probability) and [45, 46] (methods based on machine learning).

4.2 Functional Components of the Attack Detection System

In order to describe the functional organization of the detection system, the context diagram will be used. The model in Fig. 5 consists of six functional blocks.

These blocks are:

1. *Console control* – allows the administrator in the dialog mode via the operator console to configure ADS settings;
2. *Data collection from sensors* – the system is equipped with a set of intelligent measuring sensors that track movement at selected points in the system. Information from their output is downloaded, collected and pre-processed to obtain information about the security status of the local network;
3. *Learning* – the task of the module is to create a classification model during the learning process, carried out during real network operation;
4. *Construction and usage of knowledge database* – collects sampling signatures, contains classification models and system configuration settings;
5. *Attack detection* – performs an analysis of events occurring in the protected network and, based on specified, criteria, determine the degree of harmfulness of the tracked activities, and if necessary, classifies them as an attack;
6. *Decision-making process* – based on the developed methodology, it displays alerts on the console and defines a set of protective measures used to block attacks.

All hardware components of the above models were made using Raspberry Pi microcomputers. At the design stage, the available computational performance of the devices used raised reasonable doubts. The system should work in real time, which could be difficult to achieve, especially in learning mode. Therefore, the hardware architecture used has parallel nature and is based on several (four) processing modules forming a multi-machine system.

The system works in two basic modes:

1. *The learning mode* in which the symptom base is created. It contains records binding a specific type of attack with a traffic parameter vector consisting of values indicated by measuring sensors. A decision maker, which classifies symptoms in cases where such a decision cannot be taken, is automatically involved in creating the symptom database;
2. *Attack detection mode* when the values of traffic parameters determined by the sensors are direct input for the expert subsystem. Based on the previously defined analysis, the expert subsystem determines whether the network under analysis operates in normal mode or is the object of attacks. In the second case, the signaling subsystem is started.

To detect attacks efficiently, the system should be able to distinguish between transmission components for each of the communication protocols used. In the case of the upper layers of the IIS model, these will be the IEEE 802.11 protocol frames, the IEEE 802.15 protocol and the others will be used below. The proposed system accepts any communication components used in industrial networks.

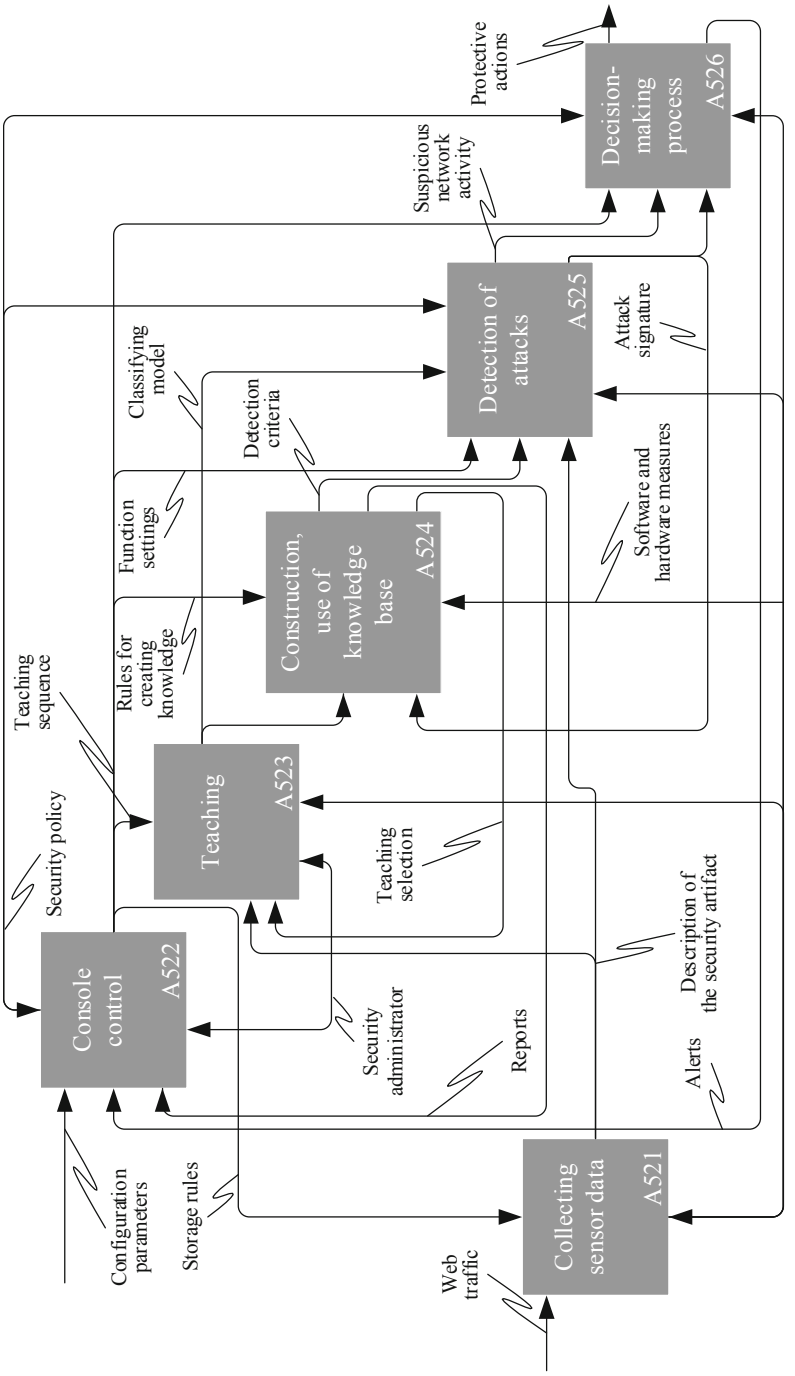


Fig. 5. Context diagram of attack detection system

5 Hardware Architecture of the System

5.1 Bus Systems and Their Representation

In addition to the algorithmic side, the effectiveness of the attack detection system will be determined by the architecture of the computing system. In the described solution, all components of the detection system are connected into one common network using multi-bus. The target solution will be based on optical fiber and optical channels. Electrical connection was used at the initial testing stage. The architecture will reflect trends characteristic for IIoT.

The organization of a parallel reconfigurable computing system with multi-bus connections is shown in Fig. 6.

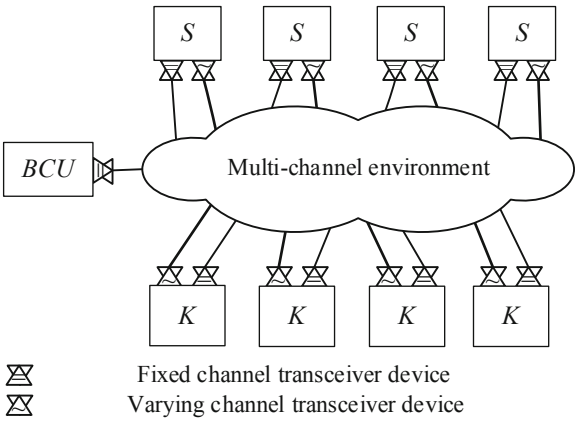


Fig. 6. The basic organization of a parallel reconfigurable computational system. BCU – bus control unit

Each of the computing nodes is equipped with at least one fixed and one adjustable single-channel communication interface. If it is possible, then the parameters of each of the fixed channels are unique throughout the organization, thanks to which there is no limit to setting up networks with any connection architecture. A deviation from the above rule is the management channel, to which all computational nodes are connected. This channel always uses broadcast mode and is only intended for sending information about the configuration of adjustable transceiver devices.

Each of the computing nodes is equipped with at least one fixed and one adjustable single-channel communication interface. If it is possible, then the parameters of each of the fixed channels are unique throughout the organization, thanks to which there is no limit to setting up networks with any connection architecture. A deviation from the

above rule is the management channel, to which all computational nodes are connected. This channel always uses broadcast mode and is only intended for sending information about the configuration of adjustable transceiver devices.

Let's assume that a parallel computer system with bus communication is a combination of two types of equal objects: N computational nodes and B buses. A node can be incidental with any number of buses. A network of n nodes and m buses is usually denoted as $[n, m]$ and is described by an incidence matrix $I = \{b_{ij}\}$ of size $n \times m$. Element $b_{ij} \in I$ is equal to 1 if with node number $i = 1, \ldots, n$ there is an incidental bus with number $j = 1, \ldots, m$, otherwise $b_{ij} = 0$. From the definition of incident matrix, it follows that bus networks do not allow loops for both, buses and nodes. Therefore, if there are multiple connections (i.e. selected node will be integrated with the selected bus using several connections), the traditional way of describing the bus cannot be used.

If the number of incident buses with node i (node degree) is s_i^w, $i = 1, \ldots, n$ and the number of incident nodes with bus j (bus degree) as s_j^b, then for any bus network $[n, m]$ there is a relationship between the summary degree of nodes and buses:

$$\sum_{i=1}^{n} s_i^w = \sum_{j=0}^{m} s_j^b = s. \tag{5}$$

Expression (5) is the basis for the bus network synthesis method developed by authors with single connections, presented among other in [47, 48]. Unlike networks with direct connections, for a bus network $[n, m]$ with an I incident matrix, there is always a network with transposed I^T incident matrix.

Bus networks are structurally equivalent to hypergraphs. Bipartite graphs are used for their analysis [49]. The number of nodes in X_0 and X_1 parts of the bipartite graph is equal to n and m respectively. Its edges are local connections $l_{p,q}$, where: p, q – number of computational nodes and buses respectively, whose task is to connect the computational nodes with buses. The above description is in the PBL (**P**rocessor-**B**us-**L**ink) neighborhood graph.

The PBL graph $G = (V, B, L)$ containing $|V_G| = n$ nodes, $|M_G| = m$ buses and L_G link set is the bipartite graph G_{PBL} which can be described by following pair: $(V_{G_{PBL}}, B_{G_{PBL}})$ and $V_{G_{PBL}} = VV_{G_{PBL}} \cup VB_{G_{PBL}}$, where $VV_{G_{PBL}} = V_G$ and $VB_{G_{PBL}} = B_G$. Connections in graph G between buses and nodes are represented by $B_{G_{PBL}}$. The nodes $v_{G_{PBL},i}$ and $b_{G_{PBL},j}$ are connected by the edge $b_{G_{PBL},k}$ if and only if in the source bus system, the bus b_i is connected to the node v_j with link l_k. Such a representation of the bus system is shown in Fig. 7.

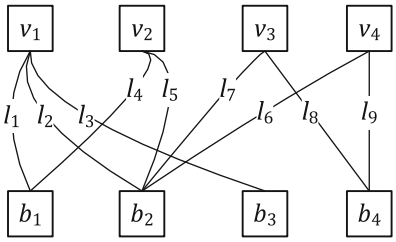


Fig. 7. Generalized form of multi-bus system

To describe the graph in the simulation programs, a neighborhood matrix with block structure was used:

$$A = \begin{bmatrix} 0_{n,n} & W \\ W^T & 0_{m,m} \end{bmatrix}. \tag{6}$$

where: $A-$ matrix with the size of $n \times m$ elements; $0_{n,n}$, $0_{m,m}$ – zero matrices with the size of $n \times n$ and $m \times m$ elements respectively. When saving to computer memory, these elements can be omitted. All information about the graph is contained int the W submatrix, sometimes called the bi-neighborhood matrix. For the bipartite graph G with the parts $V = \{v_1, \cdots, v_n\}$ and $B = \{b_1, \cdots, b_m\}$ the bi-neighborhood matrix W is binary matrix of size $n \times m$, where $w_{i,j} = 1$ if and only if $(v_i, b_j) \in L$ [50].

The designed parallel processing system is heterogeneous, consists of server units with relatively high computing power and dynamically connected low-performance Arduino or Raspberry units. Therefore, for the mathematical description of the system tripartite graph was used. Its components are S servers, K supporting servers, and B buses. It is shown in Fig. 8.

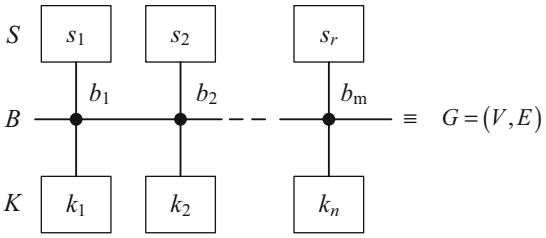


Fig. 8. Multi-bus system presented as tripartite graph

The description of the tripartite graph in the matrix form was proposed in [49, 51]. Their representation is reduced to a diagonal graph, then presented as a subgraph of an upper graph, which is the algebraic graph.

As an alternative method of describing the bus network topology, graph algebra specially developed for this purpose was used [51]. Let the sets $S = \{s_1, s_2, \cdots, s_r\}$,

$B = \{B_1, B_2, \cdots, B_m\}$, $K = \{k_1, k_2, \cdots, k_n\}$ describe the sets of primary servers, buses and supporting servers respectively. Informally, connections between set items can be described using the following rules:

1. The service recipient prefers service provider. Preferences are not permanent and can be changed without any restrictions during work;
2. The connections of service recipients with service providers is made using logical bus channels.

The formalization of the above process takes place as follows. Let's define a threefold relation $P \subseteq K \times S \times B$ on sets K, S, B: $(k, s, b) \in P \Leftrightarrow k$ prefers provider s and these preferences are carried out using the b bus $(k \in K, s \in S, b \in b)$. The relation P induces two equivalence relations R and $\bar{R}$ on sets K i B respectively:

$$k_i \, R \, k_j \Leftrightarrow (k_i, s', B'), \left(k_j, s'', B''\right) \in P; \; s' = s'', \tag{7}$$

$$b_i \bar{R} \, b_j \Leftrightarrow (k_i, s', b_i), (k_i, s', b_i), \left(k_s, s'', b_j\right) \in P; \; s' = s''. \tag{8}$$

Informally, R and $\bar{R}$ relationships mean that the supporting servers k_i i k_j prefer the same server and connecting to it is done via the b_i and b_j buses. Let's describe the case when the connection of the selected server to the secondary server is done using one and the same bus, i.e.: $k_i R k_j \Rightarrow b_t = b_l, \quad i,j = 1, \cdots, n, \quad t,l = 1, \cdots, m$ and $k_i \neq k_l \Rightarrow s_i \neq s_j$. The description of the model in the form of finite algebra of undirected connected graph can be described as:

$$\begin{aligned}
&\left(T^0_{s_1} * T^0_{B_1} \cup T^0_{B_1} * T^0_{k_1}\right) *_{f_1} T^0_{B_2} \cup \ldots \cup \left(T^0_{s_{m-1}} * T^0_{B_{m-1}} \cup T^0_{B_{m-1}} * T^0_{k_{n-1}}\right) \\
&*_{f_{n-1}} T^0_{B_m} \cup \left(T^0_{s_m} * T^0_{B_m} \cup T^0_{B_m} * T^0_{k_m}\right) = \left(T^0_{s_1} * T^0_{B_1} \cup T^0_{B_1} * T^0_{k_1}\right) \cup \ldots \\
&\cup \left(T^0_{s_m} * T^0_{B_m} \cup T^0_{B_m} * T^0_{k_m}\right) *_{f_1} T^0_{B_1} *_{f_2} \ldots *_{f_{m-1}} T^0_{B_m} \\
&= \left(T^0_{s_1 B_1} \cup T_{B_1 k_1} \cup T_{s_2 B_2} \cup T_{B_2 k_2} \cup \ldots \cup T_{s_m B_m} \cup T_{B_m k_m}\right) * f_1 T^0_{B_1} * f_2 \ldots * f_{m-1} T^0_{B_m}.
\end{aligned} \tag{9}$$

Due to the alternation of connection operations and unambiguous connection, it can be noticed that service providers and buses are equal and can be exchanged with each other. The graphical representation of the organization described by the expression (7) was shown in Fig. 7. The B bus set is an element ensuring its connectivity.

If the computational node is connected to the logical bus via several transceivers, there is a theoretical possibility of separating the signal transmitter and receiver, and thus building systems with loose connections. However, the above hypothesis raises some doubts. First, the logical bus must use the same channel along its entire length. Second, the connection of the processing node with the logical bus via several costly transceivers is only reasonable if the system's fault tolerance increases. Thus, from the point of view of definition of a system with loose and tight links, the analyzed systems

characterize tight links. Single, multiple and partial connection of a computational element (service provider or recipient) with the logical bus is schematically shown in Fig. 9.

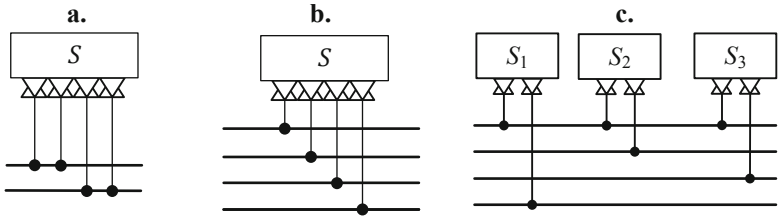


Fig. 9. Node connections with the virtual bus: a. Multiple (twice) complete; b. Single complete; c. Partial

Let's consider the condition of the computer system's readiness with equivalent nodes. Let K_{in} specify the total number of processing nodes used in the system and K_{in}^{min} – the minimum number of nodes necessary to implement all its functionalities and k_{in} – number of correctly working nodes in the system. Then, the condition of readiness has the form: $K_{in} \geq k_{in} \geq k_{in}^{min}$. In addition, it is necessary to operate a communication subsystem that ensures interoperability of at least k_{in}^{min} processing nodes. For systems with a server and supporting server, the following designations are used: K_k – the total number of supporting server; K_s – total number of servers, k_s^{min} – the minimum number of primary servers necessary to implement the systems functionality; k_k^{min} – the minimum number of supporting servers necessary to implement the systems functionality; k_s – the number of correctly working primary servers; k_k – the number of correctly working supporting servers. The readiness condition can be written as: $K_s \geq k_s \geq k_s^{min}$ and $K_k \geq k_k > k_k^{min}$. In addition, the correctness of the communication subsystem ensuring interoperability of no less than k_s^{min} service provides and k_k^{min} service recipients should be guaranteed.

5.2 Description of System Operation

In the basic operation mode, each analyzer tracks the traffic in the monitored wired or wireless network segment. All analyzers are connected by means of a common management channel supported by a broadcast communication protocol, each of the computing servers is also connected to it. The acquired data is stored in the monitoring unit and periodically sent to the security system's computational servers. For this purpose, a two-point virtual channel connecting the selected monitoring node with the appropriate server is dynamically established. The management channel participates in the connection setup procedure. Dynamic set up of the transmission channel is advantageous from the security point of view. In this way, the number of system entries available to the attacker is minimized.

The monitoring node incorporates threat symptoms, which are essentially traffic patterns in the segment that indicate a threat. The list of symptoms is not constant, it is created autonomously by computational servers based on the data sent by the nodes and the immunological threat search algorithm. Patterns are periodically sent to the monitoring nodes via management channel. If traffic like one of the patterns appears in the segment, monitoring node requests to set up a two-point communication channel connecting it to the selected computational server. The channel setup consists in determining the number of the common communication channel for the monitoring node and the server. This process was described in [52]. Until the symptom stops, the traffic is analyzed in real time on the computational server. There, further decisions are made about how to deal with the potential threat. Because the server can simultaneously support many analyzers while building a virtual connection network, the solutions presented in Fig. 9 are used.

Connections between servers and monitoring nodes use the multiple-folded physical buses descried and analyzed in [49]. Their usage is particularly beneficial from the point of view of the availability of the security subsystem. Connection network based on them retain consistency even with repeated damage to the physical network.

6 Summary and Conclusions

6.1 Practical Application of the Proposed Architecture

The effectiveness of the solution, verified by laboratory tests first results from:

1. Use of parallel processing with the assignment of processing elements to specific functions, making the system less sensitive to overloads of its components;
2. The use of a set of alternative attack detection algorithms and an expert system deciding whether to qualify network anomalies;
3. The programming team is particularly concerned about maximizing system performance on micro scale.

The cost of retail purchase of system's hardware components did not exceed EUR 200, and the effort required to develop the software for 5 man-month. Further work will focus on improving the efficiency of the algorithms used, those based on neural network. First, the process of teaching neural network will be improved, which in current version of the system takes tens of hours. It is planned to shorten it to several hours. In addition, it is assumed to expand the use of multi-factor analysis methods in application part, which will reduce size of data describing traffic necessary to detect an attack. Regarding the tool environment, it is planned to use Python to create analytical part of the system.

The goal of the authors' work was to present their own, low-cost solutions offering detection of various type of attacks, based on available database and own software. The result of the research was a parallel, intelligent software and hardware ADS that supports 8 segments of switchable network operating in 1 Gb ethernet standard in real time. The effectiveness of its functioning is presented in Table 2.

Table 2. Average values of compared algorithms

Name of the method used	Parameter			
	Correctness of classification	Precision	Completeness	Metric
Reference vectors	94%	82%	85%	83%
k-nearest neighbors	95%	83%	88%	85%
Neural networks	92%	71%	83%	76%
Decision trees	95%	85%	90%	88%

6.2 Proposed Architecture vs. Issues and Challenges in Wireless Sensor Networks

In previous studies, various methods of communication in information system were analyzed with similar accuracy, including sensors tracking traffic in the indicated network segments. It was assumed that the system components would be integrated wired optical or electrical technologies and wireless communication methods. A wireless connection of sensor tracking traffic at selected network locations was analyzed. Wireless communication between measuring sensors is beneficial, it introduces a different communication environment from the protected one. This improves the security of the entire system – additional measures, different in structure, should be used to implement any attacks.

Therefore, heterogeneous communication network will dominate in future research and applications: communication between standard components of the IIS will be carried out using wired technologies, connection of measurement sensors based on multi-channel wireless networks. In practical applications, such an organization will displace homogeneous networks based on wired communication.

6.3 Conclusions and Future Work

As a result of the research and empirical experiments, the following observations and conclusions can be distinguished:

1. At present, the system scaling applies to its selected parameters, in particular computational power, reliability and communication delays. Observations and interviews show that in standard conditions (low level of threats), users expect to build a system in which values of the above parameters are optimal. All the above restrictions will be implemented by changing the reconfiguration control algorithm. Users expect first to minimize detection time (i.e. maximize computational power) and secondly maximize reliability (wider use of communication redundancy) from functioning in threat mode. Communication delays are of interest to users only in the production technology mode and they are irrelevant to the operation of security functions.
2. While the reconfiguration process during simulation tests and empirical observations was unqualified, communication within a single bus channel seems unsatisfactory. This applies especially to the number of interfaces connected to the bus –

the channel worked efficiently with a smaller number of interfaces connected (a dozen or so) than it resulted from earlier calculations based on the conditional probability. The findings made indicate the need to modify the access protocol.
3. In the users' opinion, the most valuable feature of the developed solution is the provision of folded fiber optic buses for alternative communication between segments of the production technology management system. Since the basic task of this solution is threat detection, it can fulfill the role of an alternative communication channel, or independent communication channel will be used for such transmission.
4. Although the effectiveness of the detection system seems satisfactory, further research is needed for improvements. It may relate to the development of an expert system comparing results of test procedures and a wider use of machine learning.
5. An interesting direction of further research would be the complete elimination of computational components from the system other than Raspberry or Arduino units and reliance exclusively on a homogeneous hardware platform.

References

1. Whitman, M.E., Mattord, H.J.: Management of Information Security, 6th edn. Cengage, Boston (2019)
2. Helfrich, J.: Security for Software Engineers. CRC Press, Boca Raton (2019)
3. Beek, C., Dunton, T., Fokker, J., Grobman, S., Hux, T., Polzer, T., Rivero, M., Roccia, T., Saavedra-Morales, J., Samani, R., Sherstobitof, R.: McAfee Labs Threats Report: August 2019. McAfee Labs (2019)
4. Cyber Attack Trends: 2019 Mid-Year Report. Check Point (2019)
5. Harley, D., Myers, L., Cobb, S., Gutiérrez, C.: Cybersecurity Trends 2019: Privacy and Intrusion in the Global Village. Eset (2019)
6. Reiger, C., Ray, I., Zhu, Q., Haney, M.A. (eds.): Industrial Control Systems Security and Resiliency. Practice and Theory. Springer, Cham (2019)
7. Tipton, H.F., Krause, M.: Information Security Management Handbook, 6th edn. CRC Press, Boca Raton (2012)
8. Laplante, P.A. (ed.): Encyclopedia of Computer Science and Technology. CRC Press, Boca Raton (2017)
9. Polski Komitet Normalizacyjny: PN-ISO/IEC 27000 - Technika informatyczna. Techniki bezpieczeństwa. System zarządzania bezpieczeństwem informacji. Przegląd i terminologia. Polski Komitet Normalizacyjny, Warszawa (2014)
10. Donaldson, S.E., Siegel, S.G., Wiliams, C.K., Aslam, A.: Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against. Apress, New York (2018)
11. Otero, A.: Information Technology Control and Audit, V edn. CRC Press, Taylor & Francis Group, Boca Raton (2019)
12. Griffor, E. (ed.): Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems. Elsevier Inc., Cambridge (2017)
13. Fields, Z. (ed.): Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution. IGI Global, Hershey (2018)

14. Cirani, S., Ferrari, G., Picone, M., Veltri, L.: Internet of Things. Architectures, Protocols and Standards. Wiley, Hoboken (2019)
15. Shandilya, S.K., Chun, S.A., Shandilya, S., Weippl, E. (eds.): Internet of Things Security: Fundamentals, Techniques and Applications, Gistrup. River Publishers, Denmark (2018)
16. Banafa, A.: Secure and Smart Internet of Things (IoT). Using Blockchain and AI. River Publishers, Gistrup (2018)
17. Adaros-Boye, C.A.: Understanding Cyberrisks in IoT. When Smart Things Turn Against You. Business Expert Press, LLC, New York (2019)
18. Dehghantanha, A., Choo, K.-K.R. (eds.): Handbook of Big Data and IoT Security. Springer, Cham (2019)
19. Alcaraz, C. (ed.): Security and Privacy Trends in the Industrial Internet of Things. Springer, Cham (2019)
20. Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y.: Futuristic Trends in Network and Communication Technologies. Springer, Solan (2018)
21. Thames, L., Schaefer, D. (eds.): Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing. Springer, Cham (2017)
22. Knapp, E.: Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress, Waltham (2011)
23. Colbert, E.J., Kott, A. (eds.): Cyber-security of SCADA and Other Industrial Control Systems. Springer, Cham (2016)
24. Bhattacharjee, S.: Practical Industrial Internet of Things Security. Packt, Birmingham (2018)
25. Hajder, M., Florek, B., Kolbusz, J.: Społeczeństwo informacyjne Podkarpacia. Wyższa Szkołą Informatyki i Zarządzania z siedzibą w Rzeszowie, Rzeszów (2014)
26. Hajder, M., Nycz, M.: Zasady tworzenia skutecznych polityk bezpieczeństwa informacyjnego. In: Innowacyjna gmina. Bezpieczeństwo i ekologia. In: Hajder, M. (ed.) Rzeszów, Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie, pp. 89–106 (2013)
27. Hajder, M., Hajder, L.: Audyt systemów informatycznych. Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie, Rzeszów (2018)
28. Le, D.N., Kumar, R., Mishra, B.K., Khari, M., Chatterjee, J.M. (eds.): Cyber Security in Parallel and Distributed Computing. Wiley, Hoboken (2019)
29. Kachris, C., Falsafi, B., Soudris, D. (eds.): Hardware Accelerators in Data Centers. Springer, Cham (2019)
30. Gesh, M. (ed.): The Art of High Performance Computing for Computational Science. Techniques of Speedup and Parallelization for General Purposes, vol. 1. Springer, Singapore (2019)
31. Hajder, M., Hajder, P., Nycz, M.: Inteligentna analiza danych jako metoda detekcji atakó na sieci. In: Innowacyjna gmina. Bezpieczeństwo i ekologia, Rzeszów, Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania z siedzibą w Rzeszowie, pp. 31–56 (2013)
32. Hill, M.D.: What is scalability? ACM SIGARCH Comput. Architect. News **18**(4), 35–46 (1990)
33. Zomaya, A.Y. (ed.): Parallel and Distributed Computing Handbook, 1st edn, p. 1199. McGraw-Hill, New York (2006)
34. Donovan, J., Prabhu, K.: Building the Network of the Future: Getting Smarter, Faster, and More Flexible with a Software Centric Approach. CRC, Boca Raton (2017)
35. Huang, X., Hu, X., Wan, C., Yu, H.: Knowledge management in e-commerce: a data mining perspective. In: Management of e-Commerce and e-Government, International Conference on, Nanchang (2009)
36. Bollobas, B.: Modern Graph Theory. Springer, New York (1998)
37. Erciyes, K.: Guide to Graph Algorithms. Sequential, Parallel and Distributed. Springer, Cham (2018)

38. Ernest, R.W., Henley, J.: Graph Theory in Modern Engineering. Academic Press, New York (1973)
39. Nilsson, K., Svensson, B., Jonsson, M.: A fiber-optic interconnection concept for scaleable massively parallel computing. In: International Conference on Massively Parallel Processing Using Optical Interconnections, San Antonio (1995)
40. Hajder, M., Nycz, M., Hajder, P.: Audyt systemów informacyjnych - podejście kompleksowe. Wydawnictwo Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Rzeszów (2019)
41. Feldman, C.G.: The Practical Guide to Business Process Reengineering Using IDEFO. Dorset House, London (1998)
42. Marca, D.A., McGowan, C.L.: IDEF0 and SADT. A Modeler's Guide. OpenProcess, Inc., Auburndale (2006)
43. Bronsztejn, I.N., Siemiendiajew, K.A.: Matematyka – poradnik encyklopedyczny, XIX edn. Wydawnictwo Naukowe PWN, Warszawa (2002)
44. Bronsztejn, I.N., Siemiendiajew, K.A., Musiol, G., Muhlig, H.: Nowoczesne kompendium matematyki. Wydawnictwa Naukowe PWN, Warszawa (2004)
45. Kim, K., Aminato, M.E., Tanuwidjaja, H.: Network Intrusion Detection using Deep Learning. A Feature Learning Approach. Springer, Singapore (2018)
46. Alazab, M., Tang, M.J. (eds.): Deep Learning Applications for Cyber Security. Springer, Cham (2019)
47. Hajder, M., Bolanowski, M.: Connectivity analysis in the computational systems with distributed communications in the multichanel environment. Pol. J. Environ. Stud. **17**(2A), 14–18 (2008)
48. Hajder, M., Bolanowski, M., Byczkowska-Lipińska, L.: A set of connection network synthesis basis on the linear diophantine constraints solution in area {0, 1}. In: Ogólnopolskie Warsztaty Doktoranckie. Materiały konferencji, Nałęczów (2008)
49. Hajder, M.: Methods and facilities increasing effectiveness of designing distributed systems based on multichannels. Dissertation for the degree Doctor of Technical Science, Kyiv: National Technical University of Ukraine "Kyiv Polytechnic Institute" (2006)
50. Kunegis, J.: Exploiting the structure of bipartite graphs for algebraic and spectral graph theory. Internet Math. **11**(3), 201–321 (2015)
51. Hajder, M., Kolbusz, J., Bartczak, T.: Undirected graph algebra application for formalization description of information flows. In: 2013 The 6th International Conference Human System Interaction (HSI), Kraków (2013)
52. Hajder, P., Rauch, L.: Reconfiguration of the multi-channel communication system with hierarchical structure and distributed passive switching. In: ICCS 2019, Part II. LNCS, vol. 11537 (2019)

SYSLOC: Hybrid Key Generation in Sensor Network

N. Ambika(✉)

Faculty, Department of Computer Applications, SSMRV College, Bangalore, India
ambika.nagaraj76@gmail.com

Abstract. Sensor network provides a flexible and economical platform for its users. These are low-cost gadgets utilized to monitor and track objects of interest. Security is one of the primary concerns in this network [80]. Many security methods are available. Encryption is one such methodology used to protect data. The proposed work uses static and dynamic nodes to bring the act into play. The scheme uses hybrid key generation approach. Symmetric and location key are combined to tackle the attacks. Mutual authentication is adopted to identify the source and the destination. Endorsement keys are concatenated to the data before being transmitted. The work preserves future and past concealment in the network. Using this method the system is able to tackle various attacks. This approach secures the network against wormhole, Sinkhole and Sybil attack.

Keywords: Sensor network · Key management · Wormhole attack · Location-based keys · Pair-wise encryption key · Symmetric key generation · Sybil attack · Sinkhole attack · Markov chain property · Auxiliary node

1 Introduction

Minimizing human efforts is the need of today's world. Tiny devices [26] known as sensors with varying size and functionality aid to serve the purpose. Usage of these devices [8, 55] varies according to the customers requirement. The applications [5, 21–23, 54] includes smart homes, elderly monitoring services, military surveillance and many more. These tiny devices become a part of the system and perform the assigned task. The devices deployed aid in curtailing user supervision. The unsupervised approach adopted provides the adversary an opportunity to introduce different kinds of attacks into the network. Hence securing the nodes and the data transmitted by them becomes a priority. Key generation and its management play a vital role in preserving security and are being considered as a regular practice.

The study employs distributed-centralized system exploring the capabilities of auxiliary nodes. The nodes in the network follow clustered-based topology. The approach balances the energy among the nodes of the network. The proposed work generates encryption key using symmetric key and location key. The symmetric keys are generated prior to deployment and stored in the sensors. The advantage of using this method is it cuts down the transmission cost. The nodes generate the location keys using its co-ordinate information. This technique helps the network to create a strong

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 325–347, 2020.
https://doi.org/10.1007/978-3-030-40305-8_16

defense wall against wormhole attack. The work proves to provide better security to the data transmitted.

The study is partitioned into 7 segments. Following the introduction, Literature survey is detailed in Sect. 2. The 3 segment lists the notations used in the study. This is followed by the description of proposed work in fourth section. The analysis of the work is explained in Sect. 5. The work is simulated in NS2, explained in segment 6. The study is concluded in Sect. 7, briefing the work.

2 Literature Survey

Authentication is one of the measures adopted to ensure security in the network. Mutual authentication is where both parties are authenticated before actual communication. The cluster head and auxiliary node undergo mutual authentication in the proposed work.

Encryption is one such technique used to protect data from intrusion. Various authors have provided suggestions on deriving authentication and encryption credentials. These consist of symmetric credentials and location credentials. The details of their work are explained in this section. The setbacks and advantages of the same are considered in the proposed work. The proposed work generates the encryption credential using both. A hybrid credential is generated using symmetric and location information.

Credential generation methodologies are built using Blom's method [3]. But the method [3] was not built for credential distribution. The two matrices are taken into consideration. The symmetric table D used in the proposal is of a fixed measurement contains undisclosed credentials. The contents are made personal to the specific device. The arbitrary contents are used in the work which is unrestricted to all the devices of the system. The two conversing devices swap the contents of the unrestricted entries using the credential. Blundo methodology [4] is alike Blom's algorithm [3] with some changes. An arbitrary choice of the t-degree symmetric polynomial is considered in the work.

Eschenauer and Gligor's methodology [20] uses the collection of credentials. It is created using a unique variant. The subsets of credentials are chosen from the credential collection with a credential identity. The technique used is known as the credential ring. The devices before their organization are loaded with these credentials. The nodes willing to converse discover a mutual credential. This credential is later used for encryption. The algorithm is to find a single common credential. To address the drawbacks of [20], Q-composite credential advance allocation methodology [8] was designed. The method consisted of Q mutual vitals to overcome credential used to create a safe passage technique. To increase protection multipath credential reinforcement method was included that aids in creating a series of dislodging safety links.

The suggestion [18] is a blend of [20] and [3]. The methodology used enhances security against methods [20] and [3]. Similar to [3] arbitrary contents and symmetric contents are created. The contents created differ in number. Using [3] the symmetric table is chosen to create a transpose table. Using [20] the created table, the common credential and credential used to create safe passage is accomplished.

Polynomial pool based credential advance allocation scheme has its base in [20] and [4] of credential distribution. A collection of bivariate symmetric variants is constructed. A subset of created variants is inserted in the nodes. The nodes willing to communicate have to set-up a safe passage that should posses at least one mutual variant. Using the variant common credential is calculated using [4]. If the common polynomial is not found, they use the credential used to create a safe passage technique using [20] to accomplish the same.

Two methods are suggested using a combinatorial design based credential advance allocation scheme. The first generates the credentials using [20]. A stable partial block design is used to create the credential rings. BIBD scheme [7] works successfully when the count of nodes has to be a prime power.

To prevail the drawbacks of [7] a hybrid scheme [56] was proposed. If the number of sensors is not a prime power an alternate solution was suggested in this methodology. The closest prime power is used to generate the credential. Using this common credential is obtained using [20].

A pictorial illusion of the system is considered by assuming nodes as vertices and the conversing path as edges. Using the linking property, the expander graph is created. If an edge is discovered between two nodes, the disclosed credential is generated by the authority. This credential is allotted to the respective devices before installation. In the Expander graph-based credential advance allocation scheme [6], path credential establishment is calculated. A peer intermediate for credential establishment [9] is based on arithmetic assembly. A 2*2 grid is created by the authorizer by installing the devices in the specified position of the environment. All the devices are given an identity based on a relevant position in the network. Based on the connectives between the devices, the common credentials are provided to the devices with links inside the network.

Arbitrary allocation set selection credential advance allocation scheme [62] was proposed to take care of the availability of common credentials in various devices. The methodology creates threats to trustworthiness if the devices get negotiated. A set is generated consisting of set <credentials, count of events>. The nodes are selected arbitrarily. They are inserted with credentials considering the highest boundary before installation. To tackle the conversation burden the common credential pseudo-random function-based credential advance allocation scheme [63] is used. The authorizer inserts credentials into the specific devices that can estimates which device can hold which credential. Hence post-installation, the devices using the hash function will be able to deduce the mutual credential in both the conversation entities. If a mutual credential is not found, using [20] common credential finding and path credential establishment credential is established.

The author suggested [49] to share credentials securely presuming that the attacker will not be able to snoop on all the interaction. In the proposed methodology each device behaves as a beacon. They publicize string of arbitrary bits in their range of transmission. The nodes within the transmission range collect the bits of the transmitted string. The procedure follows with the concatenation these arbitrary bits along with some hashed mutual bits. These bits are transmitted. The mutual credential is calculated and the same is used by conversing entities.

The probabilistic credential disseminating methodology does not assure the availability of common credentials between conversing entities. The path credential establishment technique is the second approach that can be considered. The nodes are energy-constrained and hence energy is an important resource to be conserved. [14] was suggested to accomplish the same. The system has considered the installation of credentials alike [20]. It has considered credential used to establish the path phase to determine common credentials. Merkle puzzle [36] is used that transmits an arbitrary group of sequences consisting of <arbitrary sequence, credential> pair. If the accepting device can decrypt the transmitted string, the same is considered as a shared credential.

To increase links of the probability of credential share methodology a post-deployment method was suggested [57]. The methodology combines common credential concepts and credentials used to establish paths [20]. The device can appeal for a credential from its peer. If the transmission has a mutual credential alike to the peer the same is used for a safe connection between the two.

Localized encryption and authentication protocol (LEAP) [43] were suggested to bring in better security. The algorithm negotiates the common credential with their direct peer during the period used to bootstrap. The group credential validation algorithm [17] has its foundation in [20]. A 2 facet Gaussian distribution is considered. The devices in the peer are likely to share credentials. The methodology uses searching mutual credentials and credentials used to establish the path stages similar to [20]. Attack probability-based credential distribution scheme [10] is based on [17]. The suggestion aids by finding the clarification for various probability strikes on the cluster.

The authors in the Location-aware scheme [64] have used Blundo methodology in their proposal. The considered environment is logically divided into several subregions. The voting algorithm is used to elect an assistance sensor for a region. This device creates a bivariate symmetric variant using 2 prime digits. The digits created has to essentially agree with Rabin's asymmetric cryptosystem. The public credential is broadcasted by the assistance device. The devices on the accepting end create an arbitrary digit and transmit them with its position information. The assistance sensor node generates a univariate variant by embedding the positional data. The data is encrypted using the specific arbitrary digit obtained by the assistance sensor node before dispatching the same. To discover the shared credential, conversing entities communicate with the assistance device.

[65] is suggested to prevail over the drawbacks of the group-based scheme. The combinatorial theory is used to build the model. The benefit of the methodology is it can be employed to the domain where various block overlaps each other with previously count of entities. The system hikes the safety of data transmitted within the members of the group and outside the group. [37] has explored the use of the movable machine in this work. The mobile node estimates device positioning in addition to credential performing.

In [40] extra devices are installed that aim in providing coupled credential establishment. The backing device performs as a credential allotting hub in the environment. The assisting node is inserted with the hash function. The devices which are willing to form coupled credential, transmits the request to the backing nodes in their neighborhood with their ID's protected by the hash function. Using these data two copies of the arbitrary credential are created and transmitted to the requested nodes. Using this

arbitrary credential, the credentials is created by XORing bitwise on the set of arbitrary credential obtained. The Needham-Schroeder Symmetric credential [41] protocol is adopted in the study. The devices detect the backing devices within certain hop limit. They aid in coupled credentials is creation.

The Arbitrary coupled credential generation methodology [53] is proposed. The assistant device aid in the creation of coupled credentials. Preliminary credential collection and source credential collection are created for backing devices and other devices are installed in the environment. Using a preliminary pool Merkle hash tree is created. The source credential is created by hashing combination of source value and cluster identification and incorporated in the Merkle hash tree. The pair-wise credential between two sensors is commenced by transmitting source credential identification and backing device identification. The auxiliary node replies by the credential which is preloaded as the initial credential by the two parties. Using the data the devices commence the coupled credential generation stage by opting for a mutual credential from the generated credential. (Ruj et al. 2011) proposed a trust-based credential management scheme. The authors formulate the protocol by considering the finite set of elements.

Dynamic credential distribution scheme [48] uses the common credential, device identification, packets number, and arbitrary digit to create the credential. The first credential is used to encrypt the allotment credential, data credential is created from allocation credential and the created data credential is used to encrypt the packets. The local credential allocator is created using source identification, destination identification, count of packets, share the period credential and an arbitrary digit.

[35] consists of 4 stages. In Stage I, a reliable authorizer (TA) creates the system parameters and commences the devices by sending identity credentials to them through a safe path. In Stage II, devices are installed, and every device can get their position and position-based credential with the help of moving machines. In Stage III, mutual verification between peer devices is provided, and every device can establish mutual credentials with all its valid peers. In Stage IV, the coupled credential is calculated.

[16] paper presents a simple position-aware installation architecture. The proposal creates coupled credential advance allocation methodology, a neighboring coupled credentials advance allocation methodology and a position-based the coupled credentials methodology using a bivariate variant, considering the expected locations of the sensors.

In [15] cluster credential is generated by concatenating the credentials of all legitimate devices. The proposal aids in managing the conversing and calculation among the cluster devices.

[42] produces a minimum burden on available resources. The methodology is designed for the assorted system where identity-based credential creation and variant based advance allocation methodology are proposed for upper and minimal level hierarchy respectively. Group-based dispatching is performed with the device's position as the basis in the environment. The cluster supervisor is chosen using the group head option methodology is used to establish a safe association using Identity Based Cryptography with the authority. The group devices use variant based coupled credential distribution schemes to increase safety and decrease the transmission burden.

The methodology [1] uses a group-based transmission methodology. The method uses the symmetric credential method where the period credential is revised often

within the group. One way hash function and message authentication code are used to provide verification and data trustfulness. The work is based on the polynomial of the Otway-Rees protocol.

The method [34] is suggested increased safety for cluster interaction and peer-peer interaction. Elgamal public credential encryption is used to increase interaction between cluster supervisor and authority. [30] was suggested to enhance safety between peer-peer interaction and node-authority transmission. the authority transmits 2 credentials sets where interaction credentials are used to safe peer-peer interaction and individual credential is used to encrypt the device-authority interaction data. The common credential is created using the mutual credentials between the neighbors.

The method [44] is suggested using dynamic devices. The work aims to minimize the interaction burden. A safe interaction link between the group device-group supervisor and among group devices is taken care of in the proposal.

The methodology [25] was suggested to bring high safety in communication and invulnerability. The methodology is suggested using hash chains and assistance devices. The peer devices use mutual period credentials to establish reliable interaction. The authenticated chain credentials including their identifications can be differentiated using hash functions in the proposal. The proposal decreases storage, interaction and calculation burden.

The suggestion [31] is proposed to handle the foremost strike in the system. Bilinear-pairing is used in the proposal. The interaction and calculation burden is decreased in the work. [24] is suggested for the Procedure managing system or monitoring management and information acquirement structure. A advance and post privacy is considered to handle device strike.

[51] is suggested to tackle the system from negotiated devices. The work creates and allocates credentials based on hops encountered, aiding in localizing and decreasing the burden. The period credential is created to improve trustiness in the interaction between the devices. A group credential is created to use to encrypt the packets transmitted between the group associates.

[13] is a number based credential agreement. The methodology uses equivalence criteria. The device collects a credential value which is used to calculate a sole mutual credential with its group supervisor and a supervisor credential disclosed with associates of the group. The collection burden is decreased, amplifying flexibility against device strikes.

[29] uses a vigorous credential managing method for the assorted system. A hash function is used by the authority, supervisors of the group and associates of the system. The credentials are created by the devices to provide future validation and handling safety attacks. Coupled encryption credentials are created to guarantee privacy to decrease presume strikes, repeat strikes, device detains strike and DOS strike.

The work [38] uses symmetric cryptography to handle negotiated devices in the system. The credentials stocked up in the devices bring safe interaction between the device and authority. The generation of spanning hierarchy is commenced by the authority by transmitting Hello packets. On accepting the same the associates retransmit the packets to other associates of the system. After creating the hierarchy, the devices disclose symmetric credential with the authority to adhere to safe interaction. The process is completed periodically.

An Effective credential management scheme [45] is a certificateless credential management scheme designed for changing system with device movement. The credential revision is done when a device connects or disconnects from the group. The scheme also ensures future and past concealment. An Effective credential recall facility is used to handle negotiated devices in the system.

[12] proposal is based on credential disclose mechanism. Logarithm distinct illusion in the elliptic curve and credential disclosure is utilized to guarantee the safety of the devices in the system. Various stages of period credentials for interaction are created using variants in the work. The study averts a conspiracy strike in the network.

[46] is suggested to safe the dynamic devices of the system. The work utilizes two scenarios- credential mechanism which distributes the credential before and after installation. The interacting parties disclose mutual credentials to increase safety. The study increases the effectiveness of credential generation, recalling and removing of dynamic devices. The study exhibits privacy, flexibility, storage management, power utilization, and burden.

The study [52] is based on the features of the Hopfield neural system. The study ensures to decrease of storage usage and interaction burden. The study [5] focuses on device detaining, rumor based system and recall issues. Using Shamir's credential discloses methodology the credential management methodology is suggested for Alwen, a dynamic system utilized for the support system.

The credential managing system [50] incorporates credentials distributed at the earlier stage in the system. The proposal revises cluster credentials vigorously in during the device inclusion/removal. The scrutiny brings safety, future and past privacy. The proposal [33] is based on the elliptical curve cryptography and signcryption method for the chain of various devices of the system. The cyclic validation and option to include devices is imposed to increase safety in the network. In [2] the auxiliary nodes generate the pair-wise credentials with respective cluster heads using symmetric credentials stored in their memories. The respective auxiliary node, cluster head and other nodes of the network monitor each other activities at different instances of time to identify compromised node and aid in eliminating the same from the network. The work ensures security against Wormhole, Sybil and Sinkhole attack.

A secret credential generation scheme is proposed in [58]. The scheme has its foothold on cooperation between the nodes of the network. The paper analyses different active and passive attacks. The work proves to have a good hold on security with varying scalability. The author [59] has made his contribution in body-worn networks. The network is liable to channel variation due to shadowing and fading effects. The author has generated the encryption credentials using these channel parameters. Credential conciliation process is adopted to employ error-free credentials. The procedure proves to be compatible with low-power micro controllers and low-data rate transmissions.

Localization and security are the issues tackled in [60] Static and mobile nodes are supported in the work. The work proves to provide security against outside and inside attacks. Low burden is the prior advantages of the work. Authority is an active entity of the work accomplishing a majority of functionality.

The work [61] focuses on the impact of credential connectivity on efficiency of communication. System equations are used to establish credentials. The hidden

credentials are generated to establish a secure connection between the nodes. The exclusion basis system is used to implement the work.

Single mobile source, destination and relay make the co-operation model [69]. N-Nakagami distribution is applied to M2M network. The mobile source acts as a transmitter. The mobile relay acts as transmitter or receiver. The mobile destination only receives the data. The network uses two TAS schemes. Golden-section search method is employed to solve to bring in optimization. The power allocation parameter influences optimum power allocation. The system is employed in inter-vehicular, intelligent highway and mobile-adhoc video transmission applications.

In [70] outage probability of mobile D2D network is examined. Incremental amplify-and-forward (IAF) and transmit antenna selection (TAS) is considered in the study. Using the setup power allocation minimization problem is formulated. Monte-carlo simulation is applied and accuracy of optimization power is analysed.

In [71] the authors have used Elliptical curve cryptography to provide security. TinyECC is used in the work. 160 bit private credential is generated to commence authorization. 168 bit public credential is generated next. The public credential and device address act as request message. AES CCM and hard coded 128 bit start-up credential is used to encrypt. A secure bridge mote receives the message and decrypts to verify the same. The decrypted message is transmitted to management application. The user has the power to authorize the same. After positive affirmation, secure bridge is established. It transmits system credential encrypting using ECIES algorithm.

Inter-cluster multiple credential distribution scheme was proposed in [72] suspicious behavior of the nodes are detected in the proposed work. The work proves to provide better performance. The load on the individual node is reduced using this method. The work performs well reducing aggregate computation and energy consumption. In [73] the network is divided into clusters. The cluster head is made responsible to monitor its members. The observed behavior is recorded. This recorded data is transmitted to the authority. The authority assists the respective cluster head obtaining the transmitted data. Frequent pattern mining algorithm is used by the authority to check the status of the event. The cluster head uses the inferences to analyze the node as malicious.

The author in [74] has brought some improvements in q-composite scheme. The network topology in the previous work is to be worked upon. Topological properties are worked in the proposed work. Asymptotically exact probability for minimum degree is worked upon. Random graph models are considered. The on/off channel model considered to be an intersection of two graphs belonging to different categories. The study has set some guidelines for designing secure WSNs.

A credential distribution mechanism is suggested in [75]. A parameter is used to represent the maximum starting credentials. This credential is used in coupled credential establishment. A mechanism is used to generate coupled credential. A bitwise XOR operation is used to do the same. The lists of identification are stored in the link. The memory utilized to store the same is less compared to other methods. The receiver notes the identification of the source. It in turn transmits the acknowledgement message to the source. The initiator calculates the credentials and verifies the MAC. On positive affirmation, the identification is stored. A secret credential is used to provide additional security to the system.

The authors have proposed authentication protocol in [76]. An optimal percentage of group heads are chosen. The selected ones are authenticated and then allowed to communicate. The list of chosen ones is broadcasted using token-based authentication method to the network. The received token is later used in acknowledgement messages. The group heads authenticate in their vicinity. A payload-based authentication is used to accomplish the task.

3 Notations

Different notations are used in this work. Table 1, lists the notations used in the proposed work.

Table 1. Notations used in proposed work

Notation	Description
BS	Authority
N	System considered
N_i	i^{th} sensor in the system
CH_i	Group head of the i^{th} group
ID_i	Unique ID of i^{th} node of the network
r	Transmission radius
Hello	Hello packet sent by the source node
M_i	Master key
A_i	Authentication key of i^{th} auxiliary node/ key distribution centre(KDC)
E_i	Encryption key of i^{th} node of the network
EN_i	Endorsement key of i^{th} node of the network
E_s	Symmetric key
E_L	Location key
E_A	Endorsement key of the auxiliary node
E_{BS}	Endorsement key of the authority

4 Hybrid Model

The proposed work is designed to tackle different kinds of attacks. The following are the main contributions of the proposed work-

- Three kinds of attacks are reduced using the approach.
- Two categories of devices are utilized. First category of device is used to sense the environment and dispatch the collected data. Second type of device is used to authenticate the transmitted data.
- Mutual authentication is adopted in the work. The auxiliary nodes and cluster head undergo authentication. Master key is used to do the same.

- Encryption is one methodology used to bring in secure transmission to data. The proposed work adopts hybrid key generation. Symmetric and location keys are combined to generate encryption key.
- The work also embeds endorsement keys. Endorsement keys of authority and auxiliary nodes are concatenated. The keys generated vary for every session. Markov Chain concept is used to do the same. This approach provides an affirmation to the authority. The details of the work are detailed in this section.

4.1 Assumptions Made in the Study

The following are the assumptions considered in the proposal-

- The authority is considered to be reliable. It is the responsibility of the sink node to generate the key credentials. Then they are inserted into the respective devices before the organization in the environment.
- All the nodes deployed are under the assumption to be non-tamper resistant.
- The normal nodes are assumed to transmit with fixed transmission rate. The signal strength varies with time.
- The adversary is capable of introducing attacks in to the network. Sinkhole, Wormhole and Sybil attacks are considered in the work.
- The network is assumed to be attacks-free till the nodes become familiar with each other.

4.2 Deploying the Nodes in the Network

The sink node generates the key credentials. It implants them in to the nodes before their set up in the environment. The nodes fall into two categories-

- Category 1 - The nodes that engage themselves to form a cluster. They sense the environment, collecting the readings and transmit the same. These sensors are capable of generating location keys. These keys used to generate pairwise key with the symmetric keys stored in the nodes.
- Category 2 - The nodes of this class is known as auxiliary nodes/assisting nodes. They are responsible to authenticate the cluster heads in its territory. They endorse the packets of their territory. The auxiliary node generates the endorsement keys using location information. This is concatenated with keys dispatched by the authority.

4.3 Registration of the Nodes Under the Respective Auxiliary Nodes

The nodes communicate with each other using the hello message and identity. The nodes within the transmission range r fall into clusters. By default, a node among the cluster members is chosen as the cluster head. The auxiliary node broadcast *Hello*

message to the nodes in its vicinity. Notation (1), the auxiliary node A_i broadcast its presence in the network. It relays He*llo* message to the network *N*.

$$A_i \rightarrow N: \text{Hello} \tag{1}$$

The cluster heads able to hear the hello message undergo mutual authentication. The cluster head and the auxiliary node undergo authentication using the master key. In the Eq. (2), the auxiliary node A_i and cluster head CH_i are authenticating each other. Authentication is done using the master key M_i.

$$A_i \leftrightarrow CH_i: M_i \tag{2}$$

On affirmation the cluster head acknowledges with its identification. Notation (3), cluster head CH_i is acknowledging with its identification ID_i.

$$CH_i \rightarrow A_i: ID_i \tag{3}$$

The auxiliary node subdivides its territory into compound regions. For every session, the nodes of the cluster are allowed to vote with the nonce message. The group head is chosen considering the signal strength of the transmitting nodes.

4.4 Generation of Encryption Keys

Encryption is a procedure adopted to protect transmitted data. The adversary will not be read the data though captured. In the proposed work hybrid encryption is adopted. Using location keys minimizes wormhole attack. Generating keys using a randomly chosen symmetric keys and location keys increases security.

The head of the group engages itself in acquiring location coordinates. It generates location keys using the information. The group head choose symmetric key randomly. These keys with location keys aid in pairwise key generation. In Eq. (4), symmetric key E_s and location key E_L are used to generate the encryption key E_i. The cluster head distributes the same to its cluster members. This credential is used to encrypt the message. The group head aggregates the transmitted data of its cluster. It removes the redundant ones and transmits to the next available hop.

$$CE_i: E_i \rightarrow E_L \| E_S \tag{4}$$

4.5 Endorsing the Transmitted Data

Endorsing generated keys ensures more security to the transmitted message. The authority will check the legitimacy of the source. It will be able to take appropriate action in times of emergency. The sink node uses its location information to derive endorsement key. The authority dispatches the endorsement key using hash message. A legitimate auxiliary node will be able to extract the endorsement key from the received message. To bring in backward and forward secrecy, the authority uses Markov chain property. The endorsement key for every session differs.

The Markov chain property is where the state of the present value depends only on the previous value. The same is represented in Eq. (5).

$$F < P_{n+1} = A_{n+1} \,|\, P_n = A_n,\, P_{n-1} = A_{n-1}, \ldots\ldots\ldots, P_1 = A_1 > \tag{5}$$

Similarly the auxiliary node uses Markov chain property to generate its endorsement key. The location information of the node is used to derive the same.

$$A_i \rightarrow CH_i\colon EN_i(E_A \,||\, E_{BS}) \tag{6}$$

In the Eq. (6), the auxiliary node A_i has generated endorsement key from endorsement key of auxiliary node E_A and the key received from the authority E_{BS}. The key *EN_i is transmitted* to the cluster head *CH_i*. The endorsement key of cluster head and auxiliary node is attached to the aggregated data by the respective cluster head and forwarded to the next available hop. The procedure of the generation of endorsement key is detailed in Table 2.

Table 2. Algorithm to generate endorsement key

Algorithm : To generate Endorsement key
Let E_{BS} be the endorsement key transmitted by the authority.(key size=24 bits long)
Let E_A be the endorsement key generated using location details of the auxiliary node A_i (the key size = 24 bits long)
Let the i be a random number chosen by the auxiliary node A_i.
Concatenate the two endorsement keys.
Step 1: Divide the key into two halves
Step 2: Shift second half bits by i and perform XOR operation with the previous value
Step 3: Concatenate the two halves into one giving the next endorsement key E_{i+1}.

5 Security Analysis

The proposed study employs four secure steps-

- It uses hybrid key management scheme to generate encryption key. Pairwise key is generated by the cluster head. The keys used are Symmetric and location key. Location keys help tackling wormhole attack. Using symmetric key creates randomness. The key generated varies with every session.
- The auxiliary node and cluster head undergoes mutual authentication. The methodology ensures better secure transmission.
- The authority broadcasts the hash message. The legitimate auxiliary node extracts the endorsement keys. This key is concatenated with its generated key. The transmitted data is suffixed with endorsement keys. This approach provides more reliability to the transmitted data.
- The cluster heads behave as monitor nodes. They keep an eye on their members by keeping a tab on the transmitting rate and signal strength.

5.1 Assuming Auxiliary Node Is Compromised

The auxiliary node is made responsible for its territory. It involves itself in mutual authentication with the cluster head. It is also responsible to extract the endorsement key from the hash message. In addition it generates its endorsement key using location information. The keys change for every session using Markov Chain concept.

- Assume that the assisting sensors are compromised. They behave inappropriate during authentication phase with the cluster heads. The cluster heads notify the authority about its behavior. The heads do not continue with their transmission. After receiving utmost notification the authority substitutes the guilty.
- In addition the auxiliary nodes will not be able to extract endorsement keys from hash message. Hence they will not be able to suffix right keys to the transmitted data. In either ways, the guilty nodes are identified. On confirmation, the sink node replaces a new mobile node in the place of compromised one. It notifies the message to the clusters in that territory.

5.2 Assuming Group Associates Have Negotiated

All the nodes of the group belong to same category. Hence any node within its capability will be able to transmit n number of packets. The nodes are liable to transmit with the appropriate signal strength. If the nodes are compromised they will not behave normal. Their signal strength or transmission rate varies. On persistent behavior the cluster head notifies the auxiliary node. On affirmation the auxiliary node notifies the authority. The endorsement key is suffixed to the notification. The authority reverts back after evaluating the endorsement key attached. On affirmation, the authority notifies the cluster. The guilty node is isolated from the cluster.

5.3 Assuming Cluster Head Is Compromised

The group head is responsible to pass-on the encryption key to its group members. It aggregates the transmitted data, removes redundant ones. It attaches the endorsement keys received from the respective auxiliary node. The legitimate nodes follow the procedure embedded by the sink node. The compromised nodes will be working to misuse network resources. They will not follow the algorithm embedded. Hence the malicious nodes can be traced verifying these factors.

The auxiliary node undergoes mutual authentication with the cluster head. On finding the cluster head guilty, it notifies the authority. The endorsement key is suffixed to the notification. After verification the group is notified and a new cluster head is chosen.

6 Experimental Results

Sensors nodes are unsupervised and hence are liable to different kinds of attacks. Sybil, Sinkhole and wormhole attack are considered in the study. All the nodes deployed are liable to get tampered. Hence different measures are adopted to evaluate them. Four security measures are considered in the work-

- The cluster head undergoes mutual authentication with the auxiliary node. This approach provides a confirmation that the nodes are legitimate. On negative outcome, the authority is notified. The legitimate node does not proceed with communication.
- Second approach used is key generation. The proposed work generates pairwise keys using the symmetric keys and location keys. Using location key minimizes and aids in detecting wormhole attack. Using symmetric keys introduces randomness. The keys change with every session.
- Thirdly, the transmitted data is suffixed by the endorsement key. This key is generated by the endorsement key of the auxiliary node and authority. This approach certifies the transmitted data.
- Fourthly, the cluster head also behaves as the monitor node. If the signal strength or transmission rate varies substantially the node is suspected. On affirmation the node is isolated from the cluster.

The study is simulated using NS2, considering the following data set listed in the Table 3. The nodes are distributed uniformly in the environment. 500 nodes are installed in the environment. The distribution of the node is uniform. The clusters are grouped into 7 or 8 nodes. 32 groups of each are deployed. 11 auxiliary nodes are deployed. 9 mobile nodes are used as substitutes. The length of partial key is set to 8 bytes. The length of endorsement key is set to 48bits. 6160 symmetric keys are stored in each node. The total simulation time considered is 60 s.

Table 3. Parameters used in simulated work

Description	Quantity
Dimension of the network	500 m * 500 m
Total number of nodes in network	500
Distribution of nodes	Uniform
Total number of nodes dispersed in the network (excluding auxiliary nodes)	(7 nodes * 32 groups) + (8 nodes * 32 groups)
Number of auxiliary nodes	20 (11 + 9 extra)
Total Length of encryption key	132 bits
Length of partial key	64 bits(each) = 8 bytes
Length of Endorsement key	48 bits
Number of cluster members in the cluster	7–8
Number of clusters controlled by auxiliary node	5–6
Number of keys stored in nodes	6160 keys
Pair-wise keys generated for a cluster	$(6160)^n$ keys, where n is number of nodes in the respective cluster
Simulated time	60 s
Threshold value considered to evaluate the legitimate nodes	0.1
Mobile node configuration	
Data transmission speed	38,400 bps
Data payload	59 bytes
Transmission time	1.89 ms
Preamble	18 bytes

6.1 Energy Consumption

Energy is one of the limited resources in sensors. Hence some measures are taken to conserve them-

- The work uses cluster-based routing. The approach balances the energy among the nodes of the network.
- Multi-hop transmission of data is considered to minimize the energy consumption.
- The cluster head eliminates redundant data extending the lifespan of the nodes.
- If malicious node is not traced, it leads to more energy consumption. In the proposed work four measures are considered to tackle the attacks. Authentication is a prevention measure. The auxiliary node and cluster head undergo authentication. On positive confirmation from either side, communication is carried on. The cluster head act as monitor nodes. It evaluates the signal strength and transmission rate of its cluster members. On affirmation, it accepts the transmitted data. On suspicion, authority is notified. The node is isolated on affirmation from the authority. The cluster heads involve in generating encryption keys. Symmetric and location keys are used to generate pairwise key. The auxiliary nodes extract the endorsement key dispatched from authority. It concatenates its generated key with the extracted one. This key is suffixed to the data before transmission. The approach increases reliability to data. Using all these measures detects the malicious node and increases life span of the nodes. [40] Uses auxiliary nodes to generate pairwise keys. The proposed work is compared with [40] resulting in energy conservation by 10.6% (Fig. 1).

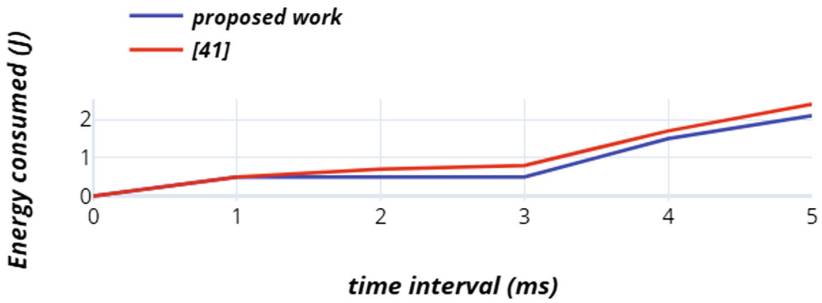


Fig. 1. Depiction of energy consumption in the network

6.2 Sybil Attack

The nodes under this kind of attack [28, 32, 66] impersonate itself with a different identity. Benefiting with the situation, the malicious node will be able to grab some of the key credentials used during the data transmission. Some of the work suggested by authors in [18] and [16] minimizes the attack to some extent. The proposed work assures validating the vital nodes. Some of the scenarios considered are-

- The node under Sybil attack behaves inappropriately. If it happens to be cluster members it will behave inappropriately. It will either transmit abruptly or use

inappropriate signal strength. The cluster head will be able to track them and notify the auxiliary node. The assisting node after affirmation suffixes endorsement key to the sending notification. On verification authority notifies other cluster members of the malicious activity. The cluster member isolates the guilty one after receiving the notification.

- If the malicious node happens to be cluster head it is also validated. The cluster head is to undergo mutual authentication with auxiliary node. On negative confirmation the auxiliary node notifies the authority. The authority reverts to the cluster members to choose another node as its group head.
- If the malicious node happens to be auxiliary node it can also be detected. The nodes undergo authentication with cluster heads. The group head can notify the authority. The authority can replace the guilty on affirmation. The hash message is dispatched by the authority. This message contains the endorsement keys. A legitimate node will be able to extract the keys. On failure, the authority can affirm using the received data.

The authors in [77] has suggested novel detection scheme to tackle Sybil attack. The work improves the lifetime of the nodes. The work uses centralized cluster-based hierarchical network. The study eliminates the malicious node from participating in cluster head selection. Any two nodes with high energy are used to detect the legitimacy. The control packets containing residual energy and identity are prepared by the nodes. They transmit to the same to the nearest detector. Using this information signal strength is calculated. This calculated value is exchanged with other detector to calculate RSSI ratio. Half-duplex communication channel is used to exchange the information. After a certain interval the same procedure is repeated. Based on identity and signal verification malicious node is detected. Comparing [77] with the proposed work, the study uses four secure measures to bring in security. Whereas [77] uses single measure to find the malicious node in vicinity. The reliability of data reaching the authority decreases in [77] compared to the proposed work. Comparing the proposed work with [77] the work provides 13.6% more security. The same is represented in Fig. 2.

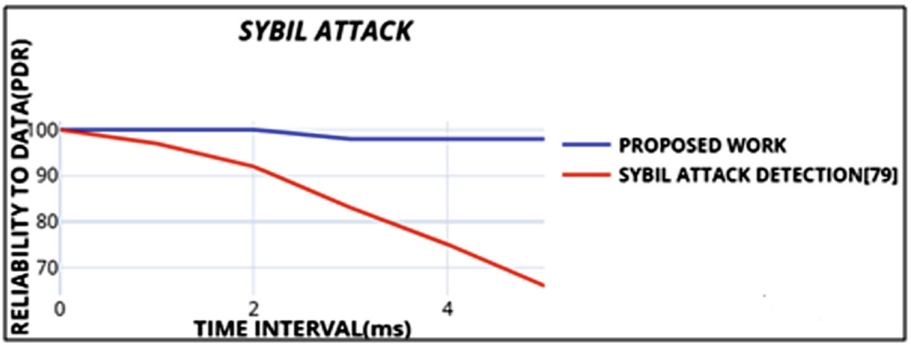


Fig. 2. Graphical representation of Sybil attack

6.3 Sinkhole Attack

The malicious nodes under sinkhole attack [16] advertise themselves as the more appropriate path to be taken to reach the destination. The nodes under this kind of attack [11, 19, 27, 47] use more signal strength to showcase themselves.

Any of the nodes deployed in the network can be malicious. The malicious node uses high signal strength to transmit its data. It has the tendency to re-transmit the data. The following steps are used to legitimate them-

- If the cluster member is assumed to be malicious. The signal strength and transmission rate is evaluated by the monitor nodes. If the doings are found inappropriate, the same is notified to the auxiliary nodes. The auxiliary nodes after affirmation, notifies the authority. The notification is suffixed with endorsement key. The authority on verification takes appropriate steps. If verification is found positive, the authority reverts back to the cluster. The malicious node is isolated.
- Second scenario is where the cluster head or auxiliary node is malicious. As both undergo mutual authentication, the guilty node is detected at early stage.

In [78] cross layer approach is adopted. LEACH protocol is used in the work. Two assumptions are considered in the work. It is assumed that cluster heads cannot be compromised. The nodes are availed flexibility to vary their transmitting power. Rectangular clustering approach is adopted. The network is divided into rectangular clusters of equal area. The average location of nodes is calculated using Dijkstra's algorithm. The MAC layer sends link information to the network layer. The information is evaluated considering re-transmissions. Using the estimations an optimal routing scheme is provided. Considering Packet-delivery ratio sinkhole attack is evaluated. [78] Considers only retransmission to locate sinkhole attack. But according to the behavior of Sinkhole attack, it displays both the characteristics-

- The transmission rate of the malicious nodes varies to divert all the packets towards it.
- The signal strength has to be high giving an illusion to the legitimate nodes that it is the nearest hop available.

But in [78] second instance is not considered. Hence the algorithm is not providing a guard towards this scenario. This reduces the security level of the nodes. [78] Also considers that the cluster heads does not compromise. The cluster heads are chosen using rectangular fashion. Hence all the nodes in the cluster may have a chance to be elected as the cluster head. To make this work, all the nodes chosen have to be non-tamper resistant. Thus the work proves to be non-economical. The proposed work provides 7.2% more security to data than [78]. Figure 3 depicts the same.

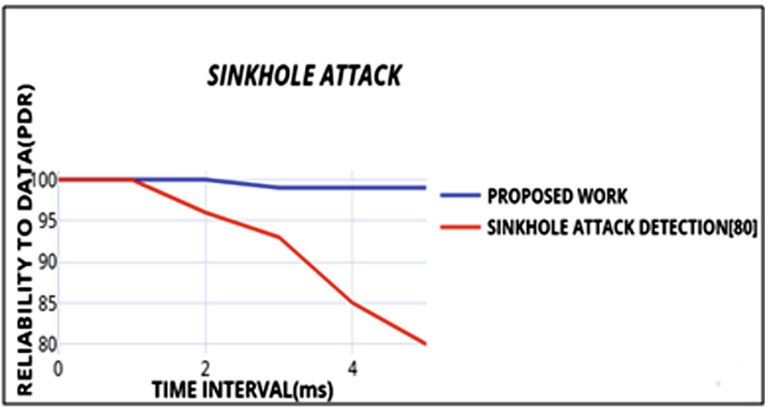


Fig. 3. Depiction of sinkhole attack

6.4 Wormhole Attack

The nodes under Wormhole attack [39, 67, 68] tunnels the packet from one part of the network to another and replays them, giving a different illusion of the network. A location key helps to minimize this kind of attack. The proposed work uses symmetric keys [18] and location keys [16] to generate hybrid keys.

The proposed work considers both the instances of the attack. It is also ensuring the check on the every node of the network. Few vital nodes are cross-verified many times. The cluster heads and auxiliary nodes are checked for their legitimacy many ways. The cluster head is checked during the following instances-

- The cluster heads are checked during mutual authentication.
- The variation in encryption key generation for every session also is a methodology to check its legitimacy.

The auxiliary nodes are checked for their legitimacy in the following ways.

- The auxiliary node is verified during mutual authentication.
- The data message dispatched from its territory is verified. The endorsement keys have to vary for every session. The node should be able to extract the keys from hash message dispatched by the authority.

The network is considered to be divided into sectors in [79]. Visiting central local algorithm is used to divide the network. The authority is considered to be point of departure. The work does not consider to formation of clusters. The source nodes aid in collecting data. This data set is sourced to the authority jointly. In this authors have considered using mobile agents. These agents are used to reject traffic intruders. The sink sends the mobile agents when it receives a message from the source nodes. These agents aid in collecting the data and returning to the authority. The disadvantage of this approach is the mobile agent if gets compromised, the procedure has to be repeated.

Hence large amount of energy is consumed if the attack increases. Hence the proposed work provides 14.7% more reliability to data transmitted with comparison to [79]. Figure 4 depicts the same.

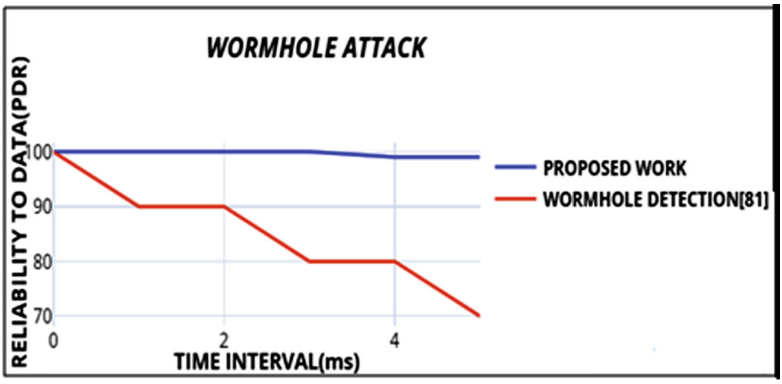


Fig. 4. Depiction of wormhole attack

7 Conclusion

Sensors are low cost devices used to monitor its environment. These unsupervised devices require security. Three kinds of attacks are considered in the work. Sybil, sinkhole and wormhole attack is minimized. The proposed work uses four methodologies to bring in better security. Usage of auxiliary nodes, mobile nodes and static nodes has aided in the approach. The auxiliary node is considered as a key distribution center. It has control over grouping the nodes into clusters and electing the head among them. Authentication is a prevention mechanism followed. The assisting node undergoes mutual authentication with the cluster head. This approach detects the malicious node very early. The node is responsible to endorse keys to the data before transmission. The approach provides more reliability to the transmitted data. Cluster heads act as monitor nodes. They monitor their members for legitimacy. The transmission rate and signal strength is considered to evaluate the same. It is also responsible to generate Hybrid encryption keys. They are generated using symmetric keys stored and location keys. The work minimizes Sybil attack by 13.6%, Sinkhole attack by and wormhole attack by 14.7%. It minimizes energy consumption by 10.6%.

References

1. Diop, A., Qi, Y., Wang, Q.: An efficient and secure session key management scheme for cluster based wireless sensors networks. In: Joint International Conference, ICPCA/SWS 2013, Vina del Mar, Chile, 5–7 December 2013, vol. 8351, pp. 33–44 (2013)
2. Ambika, N., Raju, G.T.: ECAWSN - eliminating compromised node with the help of auxiliary nodes. Wirel. Sens. Netw. **9**(2), 78–84 (2014)

3. Blom, R.: An optimal class of symmetric key generation systems. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) (1984)
4. Blundo, C., Santis, A.D., Herzberg, A., Kutten, S., Vaccaro, U., Yung, M.: Perfectly secure key distribution for dynamic conferences. In: Proceedings of the 29th International Cryptology Conference (CRYPTO) (1993)
5. Chong, C., Kumar, S.: Sensor networks: evolution, opportunities, and challenges. Proc. IEEE **91**(8), 1247–1256 (2003)
6. Çamtepe, S.A., Yener, B., Yung, M.: Expander graph based key distribution mechanisms in wireless sensor networks. In: Proceedings of IEEE International Conference on Communications (ICC) (2006)
7. Çamtepe, S.A., Yener, B.: Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Trans. Netw. **15**(2), 346–358 (2007)
8. Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P) (2003)
9. Chan, H., Perrig, A.: PIKE: peer intermediaries for key establishment in sensor networks. In: Proceedings of the 24th IEEE Conference on Computer Communications (INFOCOM) (2005)
10. Chan, S., Poovendran, R., Sun, M.: A key management scheme in distributed sensor networks using attack probabilities. In: Proceedings of the IEEE Global Communications Conference, Exhibition & Industry Forum (Globecom) (2005)
11. Chen, C., Song, M., Hsieh, G.: Intrusion detection of Sinkhole attack in large-scale wireless sensor network. In: WCNIS 2010, pp. 711–716 (2010)
12. Wu, C., Li, S., Zhang, Y.: Key management scheme based on secret sharing for wireless sensor networks. Int. J. Inf. Commun. Technol. **7**(2–3), 126 (2015)
13. Du, D., Xiong, H., Wang, H.: An efficient key management scheme for wireless sensor networks. Int. J. Distrib. Sens. Netw. **2012**, Article ID 406254, 14 (2012)
14. Deng, J., Han, Y.S.: Babel: using a common bridge node to deliver multiple keys in wireless sensor networks. In: Proceedings of IEEE Global Telecommunications Conference (GLOBECOM) (2007)
15. Damodaran, D., Singh, R., Le, P.D.: Group key management in wireless networks using session keys. In: Proceedings of the Third International Conference on Information Technology: New Generations (ITNG 2006) (2006)
16. Liu, D., Ning, P.: Location-based pairwise key establishments for static sensor networks. In: Proceedings of the ACM SASN, Fairfax, VA, October 2003, pp. 72–82 (2003)
17. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: Proceedings of the 24th IEEE Conference on Computer Communications (INFOCOM) (2004)
18. Du, W., Deng, J., Han, Y.S., Varshney, P.: A pair-wise key pre-distribution scheme for wireless sensor networks. In: Proceedings of the Annual ACM Computer and Communications Security (CCS) (2003)
19. Ngai, E.C.H., Liu, J., Lyu, M.R.: An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. J. Comput. Commun. **30**(11–12), 2353–2364 (2007)
20. Eschenauer, L., Gligor, V.: A key management scheme for distributed sensor networks. In: Proceedings of the Annual ACM Computer and Communications Security (CCS) (2002)
21. Pottie, G.J., Kaiser, W.J.: Wireless integrated network sensors. Commun. ACM **43**, 51–66 (2000)
22. Gungor, V.C., Hancke, G.P.: Industrial wireless sensor networks: challenges, design principles, and technical approaches. IEEE Trans. Ind. Electron. **56**(10), 4258–4265 (2009)

23. Hakala, I., Tikkakoski, M., Kivela, I.: Wireless sensor network in environmental monitoring - case foxhouse. In: Second International Conference on Sensor Technologies and Applications, pp. 202–208 (2008)
24. Alzaid, H., Park, D., Nieto, J.G., Boyd, C., Foo, E.: A forward and backward secure key management in wireless sensor networks for PCS/SCADA. In: Proceedings of the First International ICST Conference, S-CUBE 2009, Pisa, Italy, 7–9 September 2009, vol. 24, pp. 66–82 (2009)
25. Zhao, H., Qin, J., Shu, M., Hu, J.: A hash chains based key management scheme for wireless sensor networks. In: Proceedings of the 4th International Symposium, CSS 2012, Melbourne, Australia, 12–13 December 2012, vol. 7672, pp. 296–308 (2012)
26. Akyildiz, I., Su, W., Sankarasubramaniam, Y.: A survey on sensor networks. IEEE Commun. **40**(8), 102–114 (2002)
27. Krontiris, I., Giannetsos, T., Dimitriou, T.: Launching a sinkhole attack in wireless sensor networks: the intruder side. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2008, pp. 526–531 (2008)
28. Newsome, J., Shi, E., Song, D., Perrig, A.: The sybil attack in sensor networks: analysis & defenses, January 2004
29. Huang, J.-Y., Liao, I.-E., Tang, H.-W.: A forward authentication key management scheme for heterogeneous sensor networks. EURASIP J. Wirel. Commun. Netw. **2011**(1), 1–10 (2011)
30. Liu, J.-C., Huang, Y.-L., Leu, F.-Y., You, I., Chiang, F.-C., Yang, C.-T., Chu, W.C.-C.: A multiple-key management scheme in wireless sensor networks. In: Proceedings of the CD-ARES 2013 Workshops: MoCrySEn and SeCIHD, Regensburg, Germany, 2–6 September 2013, vol. 8128, pp. 337–344 (2013)
31. Chatterjee, K., De, A., Gupta, D.: An improved ID-based key management scheme in wireless sensor network. In: Proceedings of the Third International Conference, ICSI 2012, Shenzhen, China, 17–20 June 2012, vol. 7332, pp. 351–359 (2012)
32. Ssu, K.-F., Wang, W.-T., Chang, W.-C.: Detecting sybil attacks in wireless sensor networks using neighboring information. Int. J. Comput. Telecommun. Netw. **53**(18), 3042–3056 (2009)
33. Alagheband, M.R., Aref, M.R.: A secure key management framework for heterogeneous wireless sensor networks. In: Proceedings of the IFIP International Federation for Information Processing, vol. 7025, pp. 18–31 (2011)
34. Doraipandian, M., Rajapackiyam, E., Neelamegam, P., Rai, A.K.: An efficient and hybrid key management scheme for three tier wireless sensor networks using LU matrix. In: Proceedings of the First International Conference, ACC 2011, Kochi, India, 22–24 July 2011, vol. 192, pp. 111–121 (2011)
35. Duan, M., Xu, J.: An efficient location-based compromise-tolerant key management scheme for sensor networks. Inf. Process. Lett. **111**, 503–507 (2011)
36. Merkle, R.C.: Secure communications over insecure channels. Commun. ACM **21**(4), 294–299 (1978)
37. Mi, Q., Stankovic, J.A., Stoleru, R.: Secure walking GPS: a secure localization and key distribution scheme for wireless sensor networks. In: ACM Conference on Wireless Network Security (WiSec) (2010)
38. Messai, M.-L., Aliouat, M., Seba, H.: Tree based protocol for key management in wireless sensor networks. EURASIP J. Wirel. Commun. Netw. **2010**(1), 1–10 (2010)
39. Labraoui, N., Gueroui, M., Aliouat, M.: Secure DVHop localization scheme against wormhole attacks in wireless sensor networks. Eur. Trans. Telecommun. **23**, 303–316 (2011)
40. Dong, Q., Liu, D.: Using auxiliary sensors for pairwise key establishment in WSN. ACM Trans. Embed. Comput. Syst. **11**(2), Article no. 59 (2012)

41. Needham, R., Schroeder, M.: Using encryption for authentication in large networks of computers. Commun. ACM **21**(12), 993–999 (1978)
42. Kodali, R.K., Chougule, S.: Hybrid key management technique for WSN's. In: 9th International Conference, QShine 2013, Greader Noida, India, 11–12 January 2013, vol. 115, pp. 854–865 (2013)
43. Zhu, S., Setia, S., Jajodia, S.: LEAP: effcient security mechanisms for large-scale distributed sensor networks. In: Proceedings of the 10th ACM Conference on Computing and Communication security, Washington, DC, USA, October 2003, pp. 62–72 (2003)
44. Banihashemian, S., Ghaemi, A., Hossien, M.: Centralized key management scheme in wireless sensor networks. Wirel. Pers. Commun. **60**(3), 463–474 (2011)
45. Seo, S.-H., Won, J., Sultana, S., Bertino, E.: Effective key management in dynamic wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **10**(2), 371–383 (2015)
46. Erfani, S.H., Javadi, H.H., Rahmani, A.M.: A dynamic key management scheme for dynamic wireless sensor networks. Secur. Commun. Netw. **8**(6), 1040–1049 (2015)
47. Sharmila, S., Umamaheswari, G.: Detection of sinkhole attack in wireless sensor networks using message digest algorithms. In: International Conference on Process Automation, Control and Computing (PACC), pp. 1–6 (2011)
48. Chen, S., Liao, X., Shu, R., Shen, X., Xu, X., Zheng, X.: Dynamic key management scheme in wireless sensor networks. In: Proceedings of the Second International Conference, ICHCC 2011, Singapore, 5–6 May 2011, vol. 163, pp. 381–385 (2011)
49. Tsai, S.C., Tzeng, W.G., Zhou, K.Y.: Key establishment schemes against storage bounded adversaries in wireless sensor networks. IEEE Trans. Wirel. Commun. **8**(3), 1218–1222 (2009)
50. Qiu, W., Zhou, Y., Zhu, B., Zheng, Y., Gong, Z.: Key-insulated encryption based group key management for wireless sensor network. J. Central South Univ. **20**(5), 1277–1284 (2013)
51. Zhang, Y., Li, X., Zhen, Y., Zeng, L.: Multihop-based key management in hierarchical wireless sensor network. In: Proceedings of the 7th International Conference, GPC 2012, Hong Kong, China, 11–13 May 2012, vol. 7296, pp. 302–311 (2012)
52. Sun, Z., Wu, W., Xing, X., Li, C., Nie, Y., Cao, Y.: A hierarchical shared key algorithm in wireless sensor networks. In: Proceedings of the ICA3PP International Workshops and Symposiums, Zhangjiajie, China, 18–20 November 2015, vol. 9532, pp. 405–412 (2015)
53. Su, Z., Jiang, Y., Ren, F., Lin, C., Chu, X.: Distributed KDC-based random pairwise key establishment in wireless sensor networks. EURASIP J. Wirel. Commun. Netw. **2010**, Article no. 11 (2010)
54. Zhuang, L.Q., Goh, K.M., Zhang, J.B.: The wireless sensor networks for factory automation: issues and challenges. In: IEEE Conference on Emerging Technologies and Factory Automation, ETFA 2007, pp. 141–148 (2007)
55. Giruka, V.C., Singhal, M., Royalty, J., Varanasi, S.: Security in wireless sensor networks. Wirel. Commun. Mob. Comput. **8**, 1–24 (2008)
56. Lee, J., Park, G.L., Kang, M.J.: A message scheduling scheme in hybrid telematics network. In: Computational Science and Its Applications, ICCSA 2008. Lecture Notes in Computer Science, vol. 5072 (2008)
57. Law, C., Kwok, Y.: On efficient key redistribution in wireless sensor networks. In: IEEE International Conference of World of Wireless, Mobile and Multimedia Networks, Espoo, Finland (2007)
58. Yang, B., Zhang, J.: Physical layer secret-key generation scheme for transportation security sensor network. Sensors **17**(7), 1524 (2017)
59. Van Torre, P.: Channel-based key generation for encrypted body-worn wireless sensor networks. Sensors **16**(9), 1453 (2016)
60. Kumar, S., Singh, R.K.: Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN. Int. J. Commun. Netw. Distrib. Syst. **17**(2), 189–201 (2016)

61. Zhan, F., Yao, N., Gao, Z., Tan, G.: A novel key generation method for wireless sensor networks based on system of equations. J. Netw. Comput. Appl. **82**, 114–127 (2017)
62. Tague, P., Poovendran, R.: Modelling adaptive node capture attacks in multi-hop wireless networks. Adhoc Netw. **5**(6), 801–814 (2007)
63. Di Pietro, R., Mancini, L.V., Mei, A.: Efficient and resilient key discovery based on pseudo-random key pre-deployment. In: IEEE Parallel and Distributed Symposium, p. 217 (2004)
64. Shan, T.-H., Liu, C.-M.: Enhancing the key pre-distribution scheme on wireless sensor network. In: IEEE Asia-Pacific Services Computing Conference, pp. 1127–1131 (2008)
65. Martin, K.M., Paterson, M.B., Stinson, D.R.: Key pre-distribution for homogeneous wireless sensor networks with group deployment of nodes. ACM Trans. Sens. Netw. **7**(2), Article no. 11 (2010)
66. Xiu-Li, R., Wei, Y.: Method of detecting the Sybil attack based on ranging in wireless sensor network. In: 5th International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, September 2009, pp. 1–4 (2009)
67. Hu, Y., Perrig, A., Johnson, D.B.: Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 370–380 (2006)
68. Zhao, Z., Wei, B., Dong, X., Yao, L., Gao, F.: Detecting wormhole attacks in wireless sensor network with statistical analysis. In: International Conference on Information Engineering, pp. 251–254 (2010)
69. Xu, L., Gulliver, T.A.: Performance analysis for M2M video transmission cooperative networks using transmit antenna selection. Multimed. Tools Appl. **76**(22), 23891–23902 (2017)
70. Xu, L., Wang, J., Zhang, H., Gulliver, T.A.: Performance analysis of IAF relaying mobile D2D cooperative networks. J. Franklin Inst. **354**, 902–916 (2017)
71. Louw, J., Niezen, G., Ramotsoela, T.D., Abu-Mahfouz, A.M.: A key distribution scheme using elliptic curve cryptography in wireless sensor networks. In: 14th International Conference on Industrial Informatics (INDIN), pp. 1166–1170. IEEE, Poitiers (2016)
72. Mehmood, A., Umar, M.M., Song, H.: ICMDS: secure inter-cluster multiple-key distribution scheme for wireless sensor networks. Ad Hoc Netw. **55**, 97–106 (2017)
73. Mehmood, A., Khanan, A., Umar, M.M., Abdullah, S., Ariffin, K.A., Song, H.: Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. Secur. Anal. Intell. Cyber Phys. Syst. **6**, 5688–5694 (2017)
74. Zhao, J.: Topological properties of secure wireless sensor networks under the q-composite key predistribution scheme with unreliable links. IEEE/ACM Trans. Netw. **25**(3), 1789–1802 (2017)
75. Gandino, F., Ferrero, R., Rebaudengo, M.: A key distribution scheme for mobile wireless sensor networks: q-s-composite. IEEE Trans. Inf. Forensics Secur. **12**(1), 34–47 (2017)
76. Jan, M.A., Nanda, P., Usman, M., He, X.: PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurr. Comput.: Pract. Exp. **29**(17), 1–32 (2010)
77. Nanda, P., He, X., Liu, R.P., Jan, M.A.: A sybil attack detection scheme for a centralized clustering-based hierarchical network. In: IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, pp. 1–8 (2015)
78. Arya, I.S., Binu, G.S.: Cross layer approach for detection and prevention of sinkhole attack using a mobile agent. In: 2nd International Conference on Communication and Electronics Systems (ICCES 2017), pp. 359–365 (2017)
79. Bendjima, M., Feham, M.: Wormhole attack detection in wireless sensor networks. In: SAI Computing Conference 2016, London, UK, pp. 1319–1326 (2016)
80. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network. Communication in Computer and Information Science, vol. 958. Springer, Singapore (2019)

Diffie-Hellman Algorithm Pedestal to Authenticate Nodes in Wireless Sensor Network

N. Ambika(✉)

Faculty, Department of Computer Applications,
SSMRV College, Bangalore, India
ambika.nagaraj76@gmail.com

Abstract. Securing the network in the unsupervised environment is one of the prior issues. To address the issue authentication and encryption are adopted. The paper uses location information to generate an authentication key and bring security to the network. The Diffie-Hellman algorithm plays a key role in generating keys in the paper. Encryption keys are generated using the same. The technique adopted evaluates the nodes in communication and secures the transmitted data packets. The work minimizes the forge by 0.84% and 1.69% compared to previous work. The proposed work minimizes replay attack by 2.9% and 0.16% compared to previous work. The work conserves energy by 16.6% and 0.84% compared to the previous work. The proposal increases reliability 1.35% and 0.33% compared with previous work. The measure adheres to the forward and backward secrecy of the keys.

Keywords: Prevention and detection methodology · Security · Location keys · Authentication · Forge attack · Replay attack · Markov chain · Encryption key generation · Diffie-Hellman algorithm

1 Introduction

Sensors [1, 2] are used in many applications to lessen the human effort and adopt a low-cost setup. Applications [3] like military operations, home surveillance, monitoring hospital setups, elderly monitoring use these devices. The nodes are capable of sensing the environment and collect the data. The sensors are also used to track objects of interest. The system aid the user by providing relevant data on time.

These tiny devices are non-tamper resistant and aid in wireless transmission. The communication between the nodes happens based on their capabilities. The node will be able to transmit the data within their transmission limits. The unattended environment provides an opportunity for the adversaries to introduce different kinds of attacks. Hence the nodes should be accompanied by strong security protocols. The focus of security [4, 5] should ensure secure routing, transmission, and defense.

Authentication [6, 7] is a measure adopted to identify the communicating parties. Two kinds of identification are familiar in literature. One-way authentication happens when only the sender verifies the destination. After validation, the source transmits the

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 348–363, 2020.
https://doi.org/10.1007/978-3-030-40305-8_17

data to the same. Two-way authentication happens when both the parties involved in communication validate each other. Mutual authentication [8, 9] aids in increasing security in communication. In the study, the nodes before communication use location keys to authenticate each other.

The writing is divided into seven sections. Section 2 details working made by the various author in a similar field. Prerequisite knowledge is described in Sect. 3. The proposed work is explained in Sect. 4. The analysis of security is detailed in Sect. 5. The experiment detailing is done in Sect. 6. The writing is concluded in Sect. 7.

2 Literature Survey

Verifying the identity of the communicating party becomes essential before transmitting confidential data. The previous works suggested by different authors focus on either one-way, mutual authentication or the acknowledgment sent by the sink node. Considering the different possibilities of node compromise two-way authentication is the best available measure that can be adopted. Using only this measure does not serve the purpose if new nodes are deployed in the network [31]. A trusted entity has to certify the identity of new node before being commencing any transmission. The proposed work uses two stated measures to provide a strong security solution.

In [32] the environment is divided into different zones. Any mobile user is an authorized user to access data from the sensors. The user is to register with the gateway by its name and password before communicating with the sensors. After registration, the user is provided a time to do his queries. During the procedure, the user is supposed to be stationary, login to the sensor login-node, query them and wait for the result. The procedure has to be repeated if the user has any more queries for the sensors. The scheme fails to provide security against replay and forgery attacks.

An Energy-efficient communication paradigm is used in the work [10]. The nodes receive the broadcasted messages of the base station through its neighbors. The nodes assume this to be a reliable path and utilize the same path to transmit their data. The base station gives flexibility for the new nodes to join the network by broadcasting *interest to join* message. One of the drawbacks of the work is that the new nodes joining the cluster are not authenticated before including them into the group.

In the study [11] the nodes interested to join the cluster sends their interest to the respective cluster head. On receiving the message the cluster forwards the same to the base station. The base verifies the legitimacy and reverts with a group ticket containing the identity of the nodes. On affirmation, the nodes are allowed to join the group. After authentication, the group head issues private key and group key to the base and the cluster members. The work falls short in providing better security as it considers using one-way authentication.

The study [12] uses the sink and other nodes in the network to maintain the node neighbor list. The nodes broadcast a nonce, using which the nodes not in the list acknowledge joining the list. The sink generates an authentication key by randomly choosing a nonce. A node willing to join the group chooses one of the nonces does a part of its processing and dispatches the same to the base station. A new authentication

key is generated in case of connecting to a new sink. The work does not consider the possibility where the group head is compromised.

The study [13] provides mutual authentication and session key agreement between the user and the server. The user is to be authenticated before gaining access to the nodes. The work [14] is designed for the heterogeneous network which employs public and symmetric key cryptography approaches. The nodes of the cluster and the group head agree on a shared secret key generated by the Elliptic curve digital signature algorithm. The procedure proceeds with the registration phase where the user sends his ID encrypted with the public key. A certificate generated by the base station is transmitted to the user. The user uses this certificate to authenticate him for further communication. The user is provided with the flexibility to change his password. The user is not authenticated every time he tries to communicate. In both the suggested works the deployed node does not validate the user before transmitting the data.

The study [15] uses two new broadcast authentication schemes, a key pool scheme, and key chain scheme. Keys are stored in an access point while only a part of them are stored in the nodes. The scheme consists of 3 phases- the pre-deployment phase is where the local keys are embedded into the sensors. In the Signature phase, the second phase broadcast message and signature are generated. The last phase is known as message verification and forwarding, the node verification takes place. A Key chain scheme is where a global key pool is used to store independent key chains without any partitioning. The work does not address the validation of newly deployed nodes in the environment.

In the work [16], three phases are suggested- reliable broadcast of messages, legitimate acknowledgment from all the nodes in the network, disclosure of the message-authentication key. The server discloses the message authentication key after the server receives a positive acknowledgment from the nodes. The system specifies the number of messages to be authenticated per each of keys in the one-way key chain. Making a comparison to the proposed work, the new nodes deployed do not hassle to validate its post-neighbors before joining the cluster.

Localized encryption and authentication protocol [17] is designed to support in-network processing tasks, restricting the nodes from getting compromised. Four sets of keys are generated, an individual key is shared with the base station, and a pairwise key is generated to share it with the other node in the network, a cluster key shared with multiple neighboring nodes and a group key shared with all the nodes in the network. The study uses one-way key chains for local broadcast authentication. The work secures the network from Hello flood attack, Sybil attack, and wormhole attack but not forge attack.

The protocol [6] is a security building blocks optimized for resource- constrained environments and wireless communications. The procedure consists of two secure building blocks. The *Secure network encryption protocol* is designed to provide data confidentiality, two-party data authentication, and data freshness. The protocol adds 8 additional bytes per message giving low communication overhead, using cryptographic protocols, offers semantic security to the network. *μTESLA*, a protocol used for authenticated broadcast for severely resource-constrained environments. It is a timed, efficient, streaming, loss-tolerant authentication protocol. The protocol validates the initial packet with a digital signature using asymmetric schemes. The keys are disclosed

once per epoch. It also restricts several authenticated senders. The issue of new nodes authentication is not dealt with in this work.

The study [18] is proposed to handle the Denial-of-Service attack against broadcast authentication. The work uses a message specific puzzle to defend the network from a DOS attack. The weak authenticator is verified, used as an additional layer of protection to filter out forged broadcast packets parallel reducing resource consumption. Strawman approach is used in the one-way key chain to provide weak authentication. The broadcast message along with the message index and the broadcast authenticator is considered as a puzzle. Undisclosed key in one-way key chain is used to prevent forge attack and also at other end legitimate nodes will be able to verify the puzzling message. The work does not ensure protection against replay and forges attacks.

The combination of two kinds of sensors varying in their caliber is used in the work [19], dynamic and static nodes. When a mobile element moves to a new location, it sends a request to the base station. The sink makes a check into the revocation list, on affirmation transmits approval message with the session key to the cluster head. The head uses this message, recalculates the session key. Authenticating the cluster head is not given importance in the suggested work.

The algorithm [20] is an efficient short term public key broadcast authentication technique. Short length public/private keys are utilized, limiting the usage of keys to some minutes. There is a reduction in communication and computation, using one public key for a particular term. The work does not tackle forge and replay attacks.

The enhanced key management protocol is suggested by the authors [21]. The authentication is performed by using the Diffie-Hellman algorithm procedure. The individual key is generated using the initial key or the master key. The key is later deleted. This measure is taken to keep the master key safe from intruders. Private keys are generated using a hash algorithm. The key generated is used as the input to the process. Using the private key, the public key is generated. The prime number and integer are used in the procedure of generation. The public key is made available to the opposite party to generate the secret key. This secret key is used for authentication.

The authors [22] have used a secure key using the Diffie-Hellman key exchange algorithm and key pre-distribution scheme. The work encompasses an alarm system that aids in the isolation of compromised nodes in the network. A hardware tampering module is used to secure the network from tampering and key compromise.

Secure authentication [23] is proposed by the authors to tackle attacks in a sensor network. The authors have adopted mutual authentication to enhance security in the network. The timestamp is used to generate a new session key for every session. The work assures light computational and communicational overhead. It guarantees to secure the network against major vulnerable attacks in the network.

Elliptical curve Diffie-Hellman key exchange mechanism is proposed by the authors [24]. The TinyOS platform is used in the proposed work. A single sink-initiated broadcast message is used to bring the procedure into play. The message sets the individual keys on the nodes. The scheme assures preserving the bandwidth and energy. The authors have used a physical intrusion detection system in the office to evaluate the proposed procedure.

In [25] the data aggregator validates the received message and transmits it to the server. The proposal uses a certificateless-based aggregate signature methodology. The

elliptical curve cryptography is used to derive the signature. It also aids in verifying the signature. The elliptical curve discrete algorithm is used to bring security and privacy to the data transmitted.

[26] focuses on the impact of key connectivity on the efficiency of communication. System equations are used to establish keys. The hidden keys are produced to establish a secure connection between the nodes. The work uses the exclusion in their work.

[27] provides a suggestion for body sensor networks. The network is liable to channel variation due to shadowing and fading effects. The author has generated the encryption keys using these channel parameters. The key conciliation process employs error-free keys. The procedure is compatible with low-power microcontrollers and low-data rate transmissions.

A lightweight and resource-aware security methodology is suggested [28]. The methodology is filter-based. The received messages are filtered through the stages of aiding in filtering out malicious packets. The first stage is known as the address stage. The destination filters the message by cross-verifying against the recipient's address. A common number is generated by both the communicating parties by sharing the secret message. This methodology is used as another filter. The fourth filter verifies the MAC address [29] attached to the received data. The system also consists of a Misuse-based intrusion detection system and anomaly intrusion detection system [30] as the fifth and sixth filter.

3 Pre-requisite Knowledge

3.1 Notations Used in the Study

The below table summarizes the notations used in the study (Table 1).

Table 1. Notations used in the proposed work

Notation used	Description
N	Network under study
ID_{N_j}	Unique identification of node N_j
N_i	i^{th} node of the network
Ack	Acknowledgement
X_i	Public key generated by i^{th} node of the network
Y_i	Private key generated by i^{th} node of the network
S_k	Secret key used to generate private and public key
E_k	Encryption key
η_i	Nonce generated by node N_i

3.2 Algorithm Description

3.2.1 Diffie-Hellman Algorithm

The paper uses the Diffie-Hellman algorithm to generate authentication and encryption keys. The hash algorithm is one of the measures used to provide security in the

network. The One-way hash function consists of a sequence of hash values fulfilling some restrictions. The following properties have to be satisfied-

- Given the value of x and y, function z = H(x, y) can be calculated.
- Given the value of z, it is difficult to calculate x and y values.

The Diffie-Hellman Algorithm is a measure adopted to safeguard shared key. The algorithm works in the following-

- Consider two global parameters prime number p and integer a. a is the primitive root of p.
- Let A and B be two users willing to communicate. User A chooses a random number X_A such that $X_A < p$. This acts as a private key. The public key Y_A is calculated using the private key. The same is represented in the formula (1).

$$Y_A = a^{X_A} \bmod p \tag{1}$$

Similarly B also calculates private X_B and public key Y_B. Both the communicating parties make the public key available to the opposite party. A calculates the shared secret key using the formula (2)

$$K = Y_B^{X_A} \bmod p \tag{2}$$

The same formula is used by B to calculate the secret key. The resultant results in the same value protecting confidentiality. Formula (3) is used by B to calculate the secret key. Substituting the respective values formula (3) is equated to formula (4).

$$K = Y_B^{X_A} \bmod p \tag{3}$$

$$\begin{aligned} &= (a^{X_B} \bmod p)^{X_A} \bmod p \\ &= (a^{X_B})^{X_A} \bmod p \\ &= (a^{X_A})^{X_B} \bmod p \\ &= (a^{X_A} \bmod p)^{X_B} \bmod p \\ &= Y_A^{X_B} \bmod p \end{aligned} \tag{4}$$

3.2.2 Markov Chain Concept

The Markov chain property is where the state of the present value depends only on the previous value. The same is represented in Eq. (5).

$$P < X_{n+1} = I_{n+1} | X_n = I_n, X_{n-1} = I_{n-1}, \ldots X_1 = I_1 > \tag{5}$$

3.2.3 Assumptions Made in the Study

The following are the assumptions made in the work-

1. The base station is assumed to be trustworthy. It is responsible for generating the master key, group keys, and other key credentials.
2. All the nodes deployed fall into the same category. They have similar communication and computing capabilities.
3. The nodes deployed in the network do not follow any topology in particular.
4. The network is assumed to be free from all the attacks until the formation of the cluster.
5. The nodes deployed in the network are non-tamper resistant. It is liable to get compromised.
6. The intruder is capable of introducing a forge attack into the network. The adversary can eavesdrop on the communication, replay the messages and capable of injecting malicious packets.

4 Proposed Work

The proposed work takes care to minimize forge and replay attacks. Mutual authentication enhances security by verifying the identity of the communicating parties. The Diffie-Hellman algorithm is adopted in the study. The technique avoids disclosure of secret keys. Location information is used to generate the hash code. The hash code is used to generate a public and private key. The same is used to generate encryption keys. Markov chain concept is used to change the authentication and encryption key for every session.

4.1 Deployment of Nodes in the Environment

The base station is responsible to generate key credentials and embed them into the nodes. The nodes broadcast Hello messages to the nodes in the vicinity after self-configuring. The nodes able to receive the message send acknowledgment Ack to the sender.

$$\mathrm{N_i} \rightarrow \mathrm{N{:}Hello} \tag{6}$$

$$\mathrm{N_j} \rightarrow \mathrm{N_i} : \mathrm{Ack}, ID_{N_j} \tag{7}$$

In the notation (6), node N_i is broadcasting *Hello* message to the network N. The sensors within the transmission range r, able to hear the broadcast acknowledge with *Ack* message. In notation (7), the node N_j acknowledges with *Ack* message and its identification ID_{N_j}. The cluster is formed and a node among themselves is chosen as the cluster head. The nodes in the network are responsible to sense the environment, process and store them. They transmit the processed data to the cluster head. The cluster head is responsible to aggregate the data packets and transmit to the next available hop. The cluster head is changed with time.

4.2 Authenticating the Communicating Parties

The work adopts mutual authentication to validate the communicating parties. Location information is used to generate public and private keys. The node will be able to generate unique keys. It also aids in securing the secret key from the other. The approach aids in detecting and minimizing replay and forge attacks.

Location information is utilized as input to the Diffie-Hellman algorithm. The public key and private keys are generated. Let N_i and N_j be two nodes willing to communicate. Let N_i be the source and N_j be the destination. Let X_i be the private key and Y_i be the public key of node N_i. The nodes consider integer a and prime number p to generate the keys. Equation (8) represents the generation of private keys and Eq. (9) represents the generation of the public key.

$$X_{1i} = f(L_{N_i}) \tag{8}$$

$$Y_{1i} = a^{X_{1i}} \bmod p \tag{9}$$

Let X_j is the private key and Y_j be the public key of node N_j. Equation (10) represents the generation of private keys and Eq. (11) represents the generation of the public key.

$$X_{1j} = f(L_{N_j}) \tag{10}$$

$$Y_{1j} = a^{X_{1j}} \bmod p \tag{11}$$

Both the communication nodes N_i and N_j exchange the public keys. The same is represented in Eqs. (12) and (13).

$$N_i \rightarrow N_j : \ Y_{1i} \tag{12}$$

$$N_j \rightarrow N_i : \ Y_{1j} \tag{13}$$

The calculation of the secret key can be made by both users. The resultant has to remain the same. From Eqs. (14) and (15) the resultant results in the same value.

$$\begin{aligned} S_k &= a^{X_{1i}} \bmod p \\ &= Y_{1j}^{X_{1i}} \bmod p \\ &= (a^{X_{1j}} \bmod p)^{X_{1i}} \bmod p \\ &= (a^{X_{1j}})^{X_{1i}} \bmod p \end{aligned} \tag{14}$$

$$\begin{aligned} &= (a^{X_{1i}} \bmod p)^{X_{1j}} \bmod p \\ &= Y_{1i}^{X_{1j}} \bmod p \end{aligned} \tag{15}$$

To enhance security in the network, the Markov chain concept is utilized. For the next session, the previous private key is utilized to generate the next public and private

keys. In Eq. (16) public key is generated using the previous private key by node N_i. The same procedure is adopted by the other communicating party to enhance security in the network.

$$X_{ni} = f(Y_{ni}) \tag{16}$$

4.3 Generating the Encryption Keys

The secret key S_k is utilized to generate the encryption key for the session. The two communicating parties exchange randomly chosen nonce. In Eq. (17) node N_i is communicating nonce η_i to node N_j. in Eq. (18) node N_j is transmitting nonce η_j to node N_i.

$$N_i \rightarrow N_j : \eta_i \tag{17}$$

$$N_j \rightarrow N_i : \eta_j \tag{18}$$

$$E_k = S_k || \eta_i || \eta_j \tag{19}$$

The encryption key is generated by using the secret key and two exchanged nonce. Equation (19) represents the formation of encryption key E_k from secret key S_k, nonce η_i and η_j. The procedure enhances security by using different encryption keys for every session. The flow chart for the algorithm is given in Fig. 1. Table 2 provides the details of the generation of public and private keys in the proposed work.

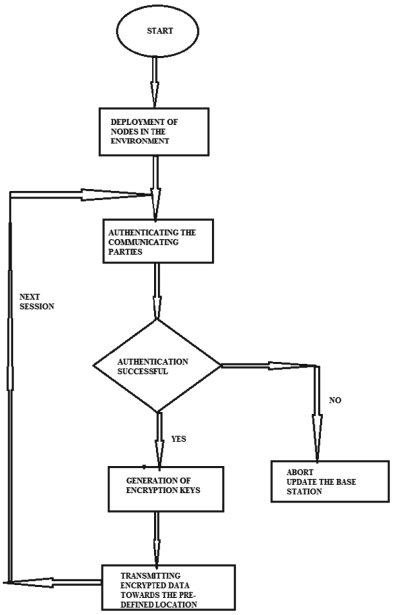


Fig. 1. Flow chart of the proposed work

Table 2. Algorithm used to private/public key (Markov chain process)

Let n be the length of the key considered (length considered in experiment is 32 bits)
Let $X_1, X_2 \ldots X_n$ be the bits in the respective positions
For p=1 to n step 2 (exchanging the positions of bits)
$X_{[p]}=X_{[p+1]}$
For p=4 to n step 4
$X_{[p]}= (X_{[p]})'$ (complement every 4 position)

5 Security Analysis

The proposed work considers the working of the Diffie-Hellman algorithm to protect the network from intruders. The location information is used to generate the private and public keys. The public key is made available to the opposite communicating party. Hence the location information is undisclosed to other party. To enhance security in the network, the keys are changed for every session. Markov chain concept is utilized to generate the new public and private keys. The proposed works protects the network from replay and forge attacks.

5.1 Forge Attack

The unattended environment is liable to get compromised and provides an opportunity for the intruder to introduce different kinds of attacks. The resources of the network are wasted shortening the lifespan of the nodes. The user will not be able to get access to the right information on time. Forge attacks are one of the kinds which duplicate the data packets. The compromised nodes under the control of the adversary try introducing different kinds of attacks into the network.

The proposed work uses location information to generate public and private keys. The keys generated remain unique from each other in all the sessions. To enhance security, the keys are generated for every session using the Markov chain concept. The opposite party is provided with only public key thus unrevealing the actual location information. If the nodes get compromised, the malicious nodes will be identified during the next authentication procedure. The same keys are used to encrypt the data packets. The procedure protects the network from forge attack by 1.69% from [21] and 0.84% compared to [25]. A graphical representation of the same is depicted in Fig. 2.

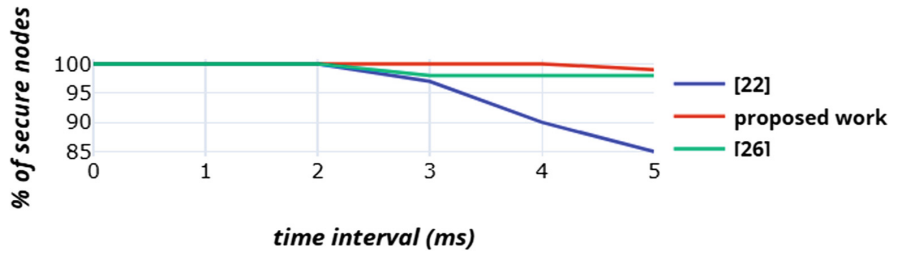


Fig. 2. Graphical representation of forge attack

5.2 Replay Attack

A Replay attack is where the compromised nodes generate a copy of the data packets and replay the same. This procedure creates a false illusion for the user. The user will not be able to act on time.

The proposed work uses the Diffie-Hellman key exchange method. Location information is used to generate public and private keys. The location information is unique by itself and hence aids in identifying the malicious node early. As the keys are changed for every session, the compromised nodes can be identified and ungrouped in an earlier stage. The location information is kept the secret which also adds safety to key credentials. A comparison between the proposed work and enhanced key management protocol [21] is made. The proposed study protects the network by 2.9% compared to [21] and 0.16% compared to [25]. A graphical representation of the attack is represented in Fig. 3.

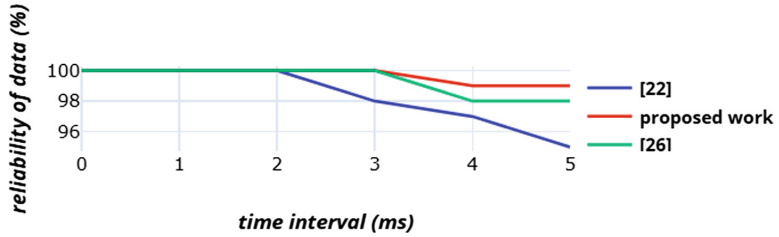


Fig. 3. Illustration of Replay attack in the network

6 Simulation Setup

The proposed work uses location information to generate public and private keys. The work uses the Diffie-Hellman key exchange algorithm aiding in unrevealing of the location information. The simulation is done using NS2. The Tinynode 584 platform is used to play the role of the static nodes. This is optimized to run TinyOS and packed as complete wireless subsystem with 19 configurable i/o pins offering up to 6 analogue inputs and two analogue outputs. It has 128B of memory and 48 KB of flash memory. The simulation setup made to evaluate the experiment is represented in Table 3.

Table 3. Representation of simulation setup used in the experiment

Parameters used	Description
Area of surveillance	200 * 200 m
Number of nodes deployed in the environment	70
Number of clusters formed	10
Private/public key length	32 bits
Secret key length	32 bits
Encryption key length	40 bits
Nonce length	4 bits
Data length	256 bits
Preamble	4 bits
Simulation time	60 s

6.1 Energy Consumption

The intruder is intended to provide inappropriate readings to the user. The adversary also tries consuming the limited resources of the network. It tries bringing the deployed nodes under its control. The compromised nodes tend to use limited resources by introducing different kinds of attacks into the network. Forge and replay attack is of the same kind. The attacks use the energy of the network by making copies of the captured data and replaying the packets.

A comparison study is made between the enhanced key management protocol [21] and the proposed work. The previous authors work [21] uses a random number to generate public and private key pairs. The protocol has some set of limitations. The same random number can be used by other communicating parties. Hence the encryption key will not differ much after using different nonce values. Using the methodology the adversary will be able to introduce forge and replay attack. To some extent, it proves successful and secure.

The proposed work uses location information to generate public and private keys. The location information is unique to any deployed node. Hence if replicated at a different location, it will come under the notice of the base station. Early detection of malicious activity is the positive side of the work. The base station and the nodes of the cluster can take appropriate action on time. The malicious node can be eliminated from the cluster. The energy can be conserved by 16.6% compared to [21] and 0.84% compared to [25]. The same is represented in Fig. 4.

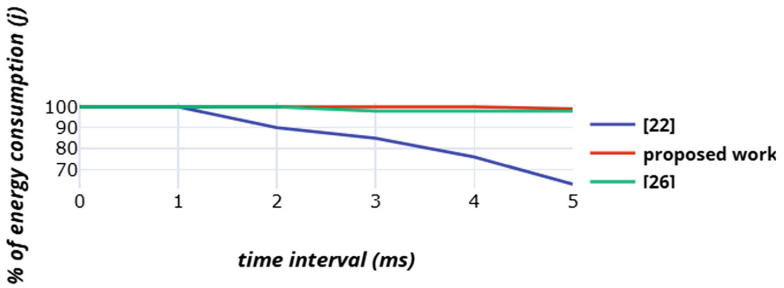


Fig. 4. Graphical representation of energy consumption in the network

6.2 Authentication Efficiency

Authentication is a methodology adopted to identify the communicating parties. The technique enhances security by recognizing the nodes in the environment before sharing any confidential information. Early detection aids in regularizing the system.

In [21] the author has proposed a methodology to randomly choose a number and authenticate each other. The adversary can compromise a node and behave normally by doing a similar methodology. But the methodology is not viable in a threatening environment. The threats like forge and replay attacks can mislead by controlling some nodes in the environment. Hence unique keys have to be used to identify the nodes in the environment. Measures need to be taken to identify the compromised nodes in the network.

The proposed work provides unique identification by using location information to authenticate the nodes. Mutual authentication is used to enhance security in the network. The proposed model uses the Markov chain concept to change its authentication keys for every session. Changing the authentication keys for every session enhances security. The methodology takes appropriate measures not to disclose the location information. For an instant of time the generated authentication keys aid in identifying the nodes. The same keys are used to encrypt data identifying the nodes transmitting data. In Fig. 5, the comparison between the proposed model and [21] is represented. The reliability of data increases by 1.35% compared to [21] and 0.33% compared to [25].

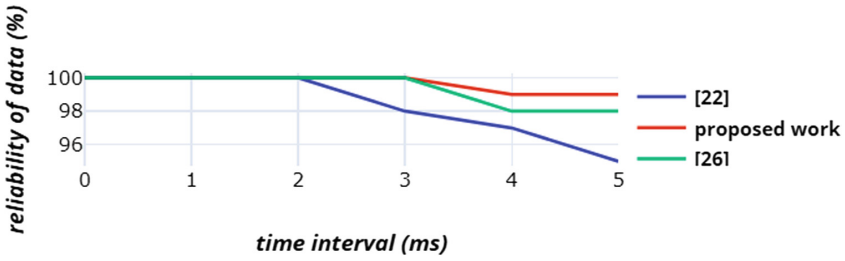


Fig. 5. Illustration of reliability to data in the network

6.3 Communication Overhead

Sensors are tiny devices deployed in an unattended environment. Bandwidth and memory availability are some of the limited resources in these devices. To support the facility in these tiny devices the resources are to be managed and utilized effectively and efficiently.

Usually, 32-64 bits of identification is attached to the transmitted data as preamble bits. The base station will be able to identify the nodes using the transmitted preamble bits. Using such a methodology can aid the adversary in accomplishing its job. The intruder can capture the transmitted data, modify the preamble bits and transmit it. The user will not be able to identify the manipulation made and take appropriate action in time of emergency.

In the proposed model, the nodes use shorter preamble bits generated using location information. The location information used to encrypt the data identifies the nodes in the network. The adversary if captures the data will not be able to misguide the user. The location information is unique to the nodes and hence protects by early detection of malicious nodes. The bandwidth of the network is increased by 0.015%–0.031% using the proposed study.

7 Conclusion

Sensors are tiny devices deployed in an unattended environment. To increase reliability, confidentiality, and privacy to data, authentication, and encryption acts as a protective methodology. The proposed work uses location information and the Diffie-Hellman methodology to generate a secret key. The public keys are made available to the opposite party to generate a secret key. The secret key is used to authenticate the communicating party. To enhance the security Markov chain concept is used. The private keys of the nodes are used to generate the keys for the next session. Hence, secret key changes for every session providing strong security against different kinds of attacks. The same is used to generate encryption keys. The work minimizes the forge by 0.84% and replay attack by 0.16%. The work conserves energy by 0.84% and increases reliability 0.33%. and bandwidth by 0.015% - 0.031%.

References

1. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)
2. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
3. Xu, N.: A survey of sensor network applications. IEEE Commun. Mag. **40**(8), 102–114 (2002)
4. Walters, J.P., Liang, Z., Shi, W., Chaudhary, V.: Wireless sensor network security: a survey. Secur. Distrib. Grid Mobile Pervasive Comput. **1**, 367 (2007)
5. Chen, X., Makki, K., Yen, K., Pissinou, N.: Sensor network security: a survey. IEEE Commun. Surv. Tutor. **11**(2), 52–73 (2009)

6. Perrig, A., et al.: SPINS: security protocols for sensor networks. Wirel. Netw. **8**(5), 521–534 (2002)
7. Bohge, M., Trappe, W.: An authentication framework for hierarchical ad hoc sensor networks. In: 2nd ACM Workshop on Wireless Security, pp. 79–87 (2003)
8. Jan, M., Nanda, P., Usman, M., He, X.: PAWN: a payload based mutual authentication scheme for wireless sensor networks. Concurr. Comput.: Pract. Exp. **29**, e3986 (2016)
9. Chen, T.-H., Shih, W.-K.: A robust mutual authentication protocol for wireless sensor networks. ETRI J. **32**(5), 704–712 (2010)
10. Abraham, J., Ramanatha, K.S.: An efficient protocol for authentication and initial shared key establishment in clustered wireless sensor networks. In: Third International Conference on Wireless and Optical Communication Networks, pp. 5–10 (2006)
11. Ibriq, J., Mahgoub, I.: A hierarchical key establishment scheme for wireless sensor networks. In: 21st International Conference on Advanced Networking and Applications, pp. 210–219 (2007)
12. Han, K., Shon, T., Kim, K.: Efficient mobile sensor authentication in smart home and WPAN. IEEE Trans. Consum. Electron. **56**(2), 591–596 (2010)
13. Cheikhrouhou, O., Koubaa, A., Boujelbenl, M., Abid, M.: A lightweight user authentication scheme for WSN. In: International Conference on Sensor Networks, Ubiquitious, and Trustworthy Computing, pp. 1–7 (2010)
14. Butun, I., Sankar, R.: Advanced two tier user authentication scheme for heterogeneous wireless sensor networks. In: IEEE Consumer Communications and Networking Conference, pp. 169–171 (2011)
15. Chuchaisri, P., Newman, R.: Fast response PKC-based broadcast authentication in wireless sensor network. In: 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 1–10 (2010)
16. Yao, T., Fukunaga, S., Nakai, T.: Reliable broadcast authentication in WSN. In: EUC 2006 Workshops, pp. 271–280 (2006)
17. Zhu, S., Setia, S., Jajodia, S.: LEAP: efficient security mechanishms in large scale distributed networks. In: 10th ACM Conference on Computer and Communications Security, pp. 62–72 (2004)
18. Ning, P., Liu, A., Du, W.: Mitigating DOS attacks against broadcast authentication in WSN. ACM Trans. Sens. Netw. **4**(1), 1 (2008)
19. Qiu, Y., Zhou, J., Baek, J., Lopez, J.: Authentication and key establishment in dynamic wireless sensor network. Sensors **10**(4), 3718–3731 (2010)
20. Du, W., Wang, R., Liu, X.: ShortPK: a short term public key scheme for broadcast authentication in WSN. ACM Trans. Sens. Netw. **4**(1), 9 (2009)
21. Cui, B., Wang, Z., Zhao, B., Liang, X., Ding, Y.: Enhanced Key Management Protocol for Wireless Sensor Network, pp. 1–10. Hindawi Publishing Corporation, London (2015)
22. Kumar, S., Singh, R.K.: Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN. Int. J. Commun. Netw. Distrib. Syst. **17**(2), 189–201 (2016)
23. Chatterjee, K., De, A., Gupta, D.: A secure and efficient authentication protocol in wireless sensor network. Wirel. Pers. Commun. **81**(1), 17–37 (2015)
24. Chung, T., Roedig, U.: DHB-KEY: an efficient key distribution scheme for wireless sensor networks. In: 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (2008)
25. Xie, Y., Li, X., Zhang, S., Li, Y.: $iCLAS$: an improved certificateless aggregate signature scheme for healthcare wireless sensor network. IEEE Access **7**, 15170–15182 (2019)
26. Zhan, F., Yao, N., Gao, Z., Tan, G.: A novel key generation method for wireless sensor networks based on system of equations. J. Netw. Comput. Appl. **82**, 114–127 (2017)

27. Van Torre, P.: Channel-based key generation for encrypted body-worn wireless sensor networks. Sensors **16**(9), 1453 (2016)
28. Heigl, M., Schramm, M., Fiala, D.: A lightweight quantum-safe security concept for wireless sensor network communication. In: IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 906–911 (2019)
29. Schurgers, C., Kulkarni, G., Srivastava, M.B.: Distributed assignment of encoded MAC address in sensor network. In: 2nd ACM International symposium on Mobile Adhoc Networking and Computing, pp. 295–298 (2001)
30. Anantvalee, T., Wu, J.: A survey on intrusion detection in mobile ad-hoc networks. J. Wirel. Netw. Secur. **4**, 159–180 (2007)
31. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication in Computer and Information Science, vol. 958. Springer, Singapore (2018)
32. Wong, K.H., Zheng, Y., Cao, J., Wang, S.: A dynamic user authentication scheme for wireless sensor networks. In: IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2006), vol. 1, pp. 8-pp. IEEE (2006)

Privacy Aware Prevention of Sybil Attack in Vehicular Ad Hoc Networks

Rajeev Kumar[1(✉)], Naveen Chauhan[1], Pushpender Kumar[1], Narottam Chand[1], and Adil Umar Khan[2]

[1] National Institute of Technology Hamirpur, Hamirpur, Himachal Pradesh, India
rajeev@nith.ac.in
[2] Qualcomm India Private Limited, Bangalore, India

Abstract. Vehicular ad hoc networks (VANETs) are prone to various threats. One type of attack is Sybil attack, where an attacker uses multiple identities to corrupt the applications of VANETs for his benefits. Vehicles exchange information in the neighborhood. Importance of such information makes privacy a major concern in VANETs. In this paper, we propose an approach that prevents Sybil attacks in privacy preserved vehicular ad hoc networks (VANETs). Proposed approach uses public key and symmetric key encryption techniques for securing the communication in VANET. RSUs distribute unique token to each vehicle which in turn are consumed to report events. It is a pseudonym-less approach that helps in preserving the privacy of vehicles. In VANET vehicles detect events and dynamically create cluster. Then they choose cluster-head for communicating with RSU about the event. Sybil attacker can use same token in different messages for misleading other vehicles. But cluster-head as well as all vehicles in the cluster collects tokens from neighbors. Then they figure out for a particular event any message includes identical token then attacker is subject to be revoked by all other vehicles in the cluster.

Keywords: Sybil attack · VANET · Privacy · Clustering · V2V

1 Introduction

Vehicular Ad Hoc Networks (VANETs) is a subcategory of Mobile Ad hoc Network (MANETs) [1–4]. It has been introduced for securing vehicles and to provide efficient transportation system by making vehicles able to communicate to each other. It promises the functionalities which include safety of vehicle, congestion avoidance, collision avoidance, securing roads and privacy preservation of vehicles. In VANETs vehicles are equipped with communication devices for communication between vehicles and among vehicles and roadside infrastructures using wireless link. There are basically two types of communication devices in VANET. One is On-Board Units (OBUs) installed at vehicles and other is Road Side Units (RSUs) installed at roadside. Vehicle to Vehicle (V2V) communication is used to exchange the message between vehicles while Vehicle to Infrastructure (V2I) communication is needed to report about events to Road Side Units (RSUs).

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 364–380, 2020.
https://doi.org/10.1007/978-3-030-40305-8_18

Vehicles act as sensors and exchange safety messages to each other about accident, traffic jams and glazes [5]. Vehicles exchange messages which include information like identity, position, speed. Attacker can receive this information easily by eavesdropping and may use this information to build a mobility pattern of vehicle. It can track the vehicle or it can misuse the identity of vehicle for its benefits. So, privacy is important in every application of VANETs.

In VANETs vehicles use wireless link for communicating to other vehicles and RSUs. Due to distributed nature of VANET, it is prone to various security threats. Security is important concern in VANETs. Sybil attack is a serious threat to ad hoc and wireless sensor network [6]. In Sybil attack an attacker can use multiple identities to forge and disrupt the functioning of VANETs. It either impersonates the identities or use fake identities to inject false information in the network. Attacker creates the illusion that there are additional vehicles on the roads. An attacker can take part of polling to create a false result or can create the illusion of traffic jam. In this way an attacker takes over the control of whole system. It impairs the efficiency of many VANETs potential applications and poses threat to even life safety [7, 8].

There are various solutions available against Sybil attack. But in these solutions, identity of vehicle is compromised. Identity privacy is important in the context of security problems [18]. Vehicles can receive the wireless signal and can get identity of the vehicles easily. Attackers can cause harm to vehicle at physical level as well as misuse the identity for its benefit. These are conflicting goals. Either defense against Sybil attack or privacy preservation can be achieved. So, it is important to create an approach that detect and prevent Sybil attack in privacy preserved VANETs.

In this paper we proposed an approach to prevent Sybil attack in privacy preserved VANETs. This scheme does not depend on infrastructure for Sybil attack prevention. Vehicles locally detect Sybil attack and inform to RSU for revocation. BRSU (Border Road Side Unit) [17] is an RSU that positioned at the overlapping area of two segments. BRSU provide a unique set of tokens to each vehicle. Each token is for a particular event that can occur in VANETs like one token for accident, one for jam etc. Vehicle uses token to report for a particular event. A token is unique for a particular event only it cannot be used for other events. Vehicles create a dynamic cluster and choose a cluster-head for transferring the information about the event to the RSUs. A vehicle can report multiple times for same event by sending different messages with different identities but it has only one token for an event. So, if vehicle do so, it identifies by other vehicles easily. It restricts attacker to use multiple identities. This mechanism prevents the vehicles for initiating Sybil attack as well as identity of vehicle is not exposed.

The rest of the chapter is organized as follow. Second section provides a review of related work on Sybil attack prevention and detection in VANET. Third section describes used system model. Fourth section presents our proposed scheme. Finally, section concludes the chapter.

2 Related Work

The Sybil attack was first described by Douceur [9] in the context of peer to peer networks. Sybil attacks affect distributed networks. VANETs are also distributed in nature. Douceur suggested that this attack can be prevented, if each vehicle has a unique identity in the network. But it lacks anonymity because vehicles use wireless link to communicate to each other. An attacker can easily get its identity by eavesdropping. Newsome et al. [10] proposed Radio Resource Testing to defend against Sybil attack. It is assumed that any physical device can have one radio at most. So, device is unable for sending and receiving simultaneously on more than one channel. But this assumption is not valid in the case of VANETs because an attacker can acquire multiple radios.

Golle et al. [11] suggested that Public Key Cryptography can be use against Sybil attack. Pal [12] uses an authentication scheme where certificate is issued to every vehicle. Certificate contains public key information and other attributes. But this approach fails due to existence of large number of vehicles and its deployment is not possible in real world due to VANET characteristics.

Most of the Sybil attack detection approach in VANETs is based on verification of position. Xiao et al. [13] introduced Receive Signal Strength based verification scheme using multi literation technique. All vehicles have same power of transmission. The distance between sending and receiving sites is calculated by receiving sites and if its position does not match to its power level. Then it is considered as Sybil node. But the accuracy of this approach is limited. So, if vehicles are very close to each other. It cannot be ensured whether they are honest node or Sybil node.

Park [14] et al. proposed an approach which is based on spatial and temporal correlation between two vehicles. A vehicle in a network will receive a series of timestamp from RSUs at regular time interval. There cannot be two vehicles in the same space at the same time. Vehicles must have different timestamps. This scheme works well in the initial deployment but fails in the situation of traffic congestion.

Kenza Mekliche et al. [15] suggested an approach in which Department of Motor Vehicle (DMV) provides vehicles a unique set of pseudonyms for hiding its unique identity. But few vehicles use these pseudonyms to launch Sybil attack. Pseudonyms assigned to particular vehicle are hashed to a common value, and the hash is stored at RSUs and DMV. By calculating the hashed values of received pseudonyms, RSU calculates if the pseudonyms came from the same pool or not. If pseudonyms are from same pool, it suspects Sybil attack. But it causes a huge load to DMV.

Zhou et al. [16] suggested an improvement to C-P2DAP [15] which is Location-Based Privacy-Preserving detection of Sybil attack (L-P2DSA). It reduces the load on DMV. In this approach detection is performed at two levels. Firstly, RSUs overhear communication between vehicles and calculate position of each vehicle. Then it calculates distinguish-ability degree. If it is over the threshold, then RSUs report about the suspicious vehicle to Department of Motor Vehicle (DMV). Then DMV perform detection at second level by calculating fine grained hashed to detect Sybil node. This scheme performs well in a small network but it is very difficult to implement in real time scenario.

Heekuck et al. [17] used pseudonym-less beaconing approach for preserving the privacy of vehicle. BRSUs are installed in the overlapping area of two consecutives domains. BRSUs distribute unique tokens to vehicle and update domain level common keys. In order to avoid Sybil attack through schedule beacons (SB), temper resistant module (TRM) is employed for performing pre-data analysis. Vehicle report for an event and use one token per event. Vehicles send event reporting message (ERM) to RSU for a particular event including its token. RSUs collect ERMs from vehicles and figure it out that any ERM contains identical tokens. If an ERM contains identical token, then that vehicle is subject to revocation. Privacy is preserved by the tokens not by pseudonyms. They can have multiple identities by stealing, forging or any other means. But they are restricted to use same token. This approach works well but attacker can have tokens of other vehicles just by having ERM of other vehicles. Then attacker can use this token further to inject wrong information. Also, this scheme is highly dependent on infrastructure (RSUs) that cannot be trusted entirely in VANET. RSUs can be compromised by attacker.

Marwane et al. [18] proposes a distributed approach, which allows the detection of Sybil attacks by making use of theory of traffic flow. The main idea of proposed approach is monitoring of their neighborhoods by each individual vehicle node to detect occurrence of Sybil attack. In [19], recent work related to network and communication technologies are given. Particularly, Kumar et al. [20] focuses on opportunistic network paradigm and proposed node activity-based protocol for opportunistic networks. Khana et al. [21] proposed traffic management system for smart cities.

3 System Model

3.1 VANET Architecture

- TA is a trusted authority that maintains records of all vehicles in the network. Every vehicle needs to perform registration to TA. After successful registration, TA distributes unique identity, certificate signed by TA, public-private key pair and other useful information to the vehicles. It acts as root of trust. This is the Certificate authority of the Vehicular Public Key Infrastructure (VPKI) and could be a Department of Motor Vehicle (DMV) or some commercial entity. To avoid single point of trust and single point of failure, multiple entities may jointly act as the authority. These entities are fixed units, dedicated only for a region.
- RSUs (Road Side Units) are wireless access point, provisioned along the road. They act as intermediate between vehicle and TA. RSUs connected to TA via wired connection. All RSUs connected to neighbor RSUs using wireless link. RSUs are considered as semi-trusted parties. It is difficult but possible to compromise RSUs. All information sent by vehicles is forwarded to neighbor RSUs after verifying the sender. RSUs can fetch information from TA to verify the identity of vehicle. RSUs are used for the coverage for the network.

- BRSUs [20] are installed in the overlapping area of two consecutives segments. Whole area is divided geographically into various fixed length segments. In a segment there can be various RSUs. The task of BRSUs is to perform initial authentication on each vehicle and after successful authentication of vehicle, it distributes group key and token to legitimate vehicles. BRSUs are also semi-trusted party. It can be compromised by attacker.
- Vehicles are semi-trusted parties. Vehicles have OBUs installed. This OBU is use for communication to other OBUs and to RSUs. Vehicles have the capabilities to generate random identity and public-private key pair to preserve its identity. Vehicles are tempering proof module (TPM). TPM is responsible for performing cryptographic operation. It is used to store secret materials like keys and certificate of OBUs. It is assumed that it is difficult to extract information from the TPM. Neither legitimate vehicles nor attacker can distort the working of its temper proof module. Vehicles sense events and communicate each other in a multi-hop manner and to RSUs using 802.11p protocol (Fig. 1).

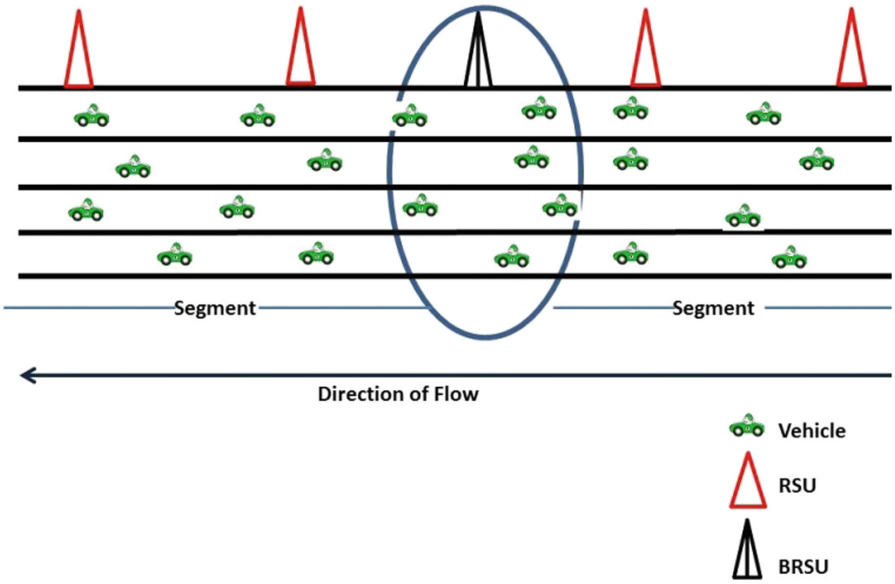


Fig. 1. Architecture of VANET containing vehicle, RSU, and BRSU

3.2 Attackers Assumption

Attackers can alter their transmission strength. Attackers have more computational resources comparing an honest vehicle. Attackers can use various identities at a same time. Attackers can impersonate other vehicles.

4 Proposed Scheme

In our proposed scheme, vehicles detect events on roads and dynamically create a cluster. Then it chose cluster-head (CH) to communicate directly to RSU to report about the detected event. This entire process carried out in a way that it prevents an attacker for launching Sybil attack in privacy preserved VANETs. The proposed scheme goes through three steps, the first is initialization step, the second is dynamic clustering among vehicles and the third step is cluster-head selection.

4.1 Initialization Step

In this step, vehicles receive group key and token from BRSUs. It is assumed that whole geographical area is divided into fixed lengths segments. At the overlapping region of segments, BRSUs are installed. In each segment a unique key is used to communicate among vehicles. That key is called group key.

In VANETs critical events on roads like accident, poor road conditions, fog, heavy rain etc. must be circulated to vehicles through RSUs for their safety. BRSUs provide unique token to each vehicle. Each event that can occur in the network has a unique code. Vehicle use token to cast their vote for a particular event. So, they can report only once for an event (Table 1).

Table 1. Notations and Description

Notations	Descriptions
RD	Relative distance
RV	Relative velocity
V_i	i^{th} vehicle
Max()	Provides max value
Min()	Provides min value
Token (V_i)	Number of token received from neighbors
Random()	It selects randomly any value.
Status_Vehicle _CRL()	It returns 1 if it is available in CRL list
NOT	Number of token

Initially BRSU authenticate each vehicle and prevent a suspicious vehicle from launching Sybil attack. Every vehicle needs to authenticate itself to BRSUs. In every segment, a unique group key required for communication. As soon as vehicle enters into a new segment, it receives beacon message from BRSUs. In the message BRSU mentions its identity (RSUID), public key (PUB_KEY) and timestamp (TS).

$$\{\text{RSUID}, \text{PUB\_KEY\_RSU}, \text{TS}\}$$

After receiving the message from BRSUs, each vehicle forwards its unique identity (VID), certificate (CERT) and public key (PUB_KEY_VECL) to BRSU and encrypt the message with the public key of BRSU (Fig. 2).

$$\{\text{VID, CERT, PUB\_KEY\_VECL, TS}\}_{\text{PUB\_KEY\_PSU}}$$

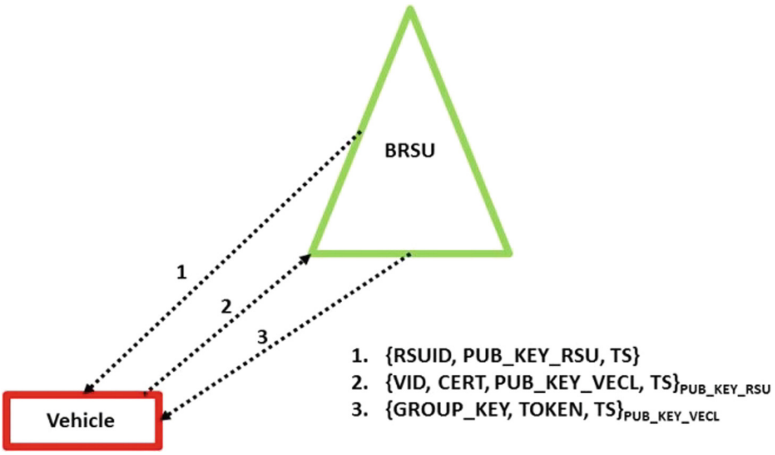


Fig. 2. Communication between vehicle and BRSU

BRSU authenticates the vehicle by checking its status in certification revocation list (CRL). If it is in CRL, BRSU will not issue any group key (GROUP_KEY) and token (TOKEN) otherwise it issues.

$$\{\text{GROUP\_KEY, TOKEN\_SET, TS}\}_{\text{PUB\_KEY\_VECL}}$$

Algorithm 1 Initial authentication and token distribution

1: BRSU periodically broadcast its ID and public key to each vehicle in its vicinity.
2: **For** each vehicle i in vicinity
Vehicle receives beacon and forward it's ID, Certificate and public key to BRSU.
End For
3: **For** each message i BRSU received
If Status_Vehicle _CRL (v_i)
Considered as Malicious node
Else
It assigns group key and token to vehicle i.
End If
End For

4.2 Dynamic Clustering

Every vehicle in the VANET has same transmission strength except the attacker. An attacker can alter its transmission strength. All vehicles in VANETs move in a particular direction. So, vehicles which are leading, will detect any event sooner. Vehicles which detects first, broadcast first the message to its neighboring vehicle. Vehicles have

a capability to generate a random identity and public-private key pair for communicating with neighboring vehicles. It uses one if its random identity (RID), random public key (RPUB_KEY), code of event (CODE), token (TOKEN), timestamp (TS) for its freshness, lane (LANE) where it is located and hop-count (HOP). They broadcast this message and encrypt with group key.

$$\{\text{RID, RPUB\_KEY, CODE, TOKEN, LANE, HOP, TS}\}_{\text{GROUP\_KEY}}$$

Vehicles are tempering proof devices. Hop-count generated by vehicles automatically. Hop-count is predefined and uses to limit the size of cluster. Every vehicle in neighborhood receives this message and waits for event to be detected by itself. Only those vehicles can decrypt the message which have group key. If it is found to be correct, it broadcast the same information with one less hop-count. When vehicles receive message and finds out that the value of hop-count is negative. Then they don't broadcast the message and all the vehicle that receives the messages as well as non-negative hop-count are the part of cluster. Every vehicle stores the information received from the neighbor.

An attacker can increase its transmission strength or inject wrong information but no vehicle in the network will believe until and unless it will not detect the event itself. An attacker can use multiple identities but it has only one token. This approach restricts attackers to send multiple messages because vehicles have only one token. If attacker sends different messages with different identities, still it has to use same token. Vehicle of the cluster collects token from neighbor and if they found identical tokens. They revoke the attacker (Fig. 3).

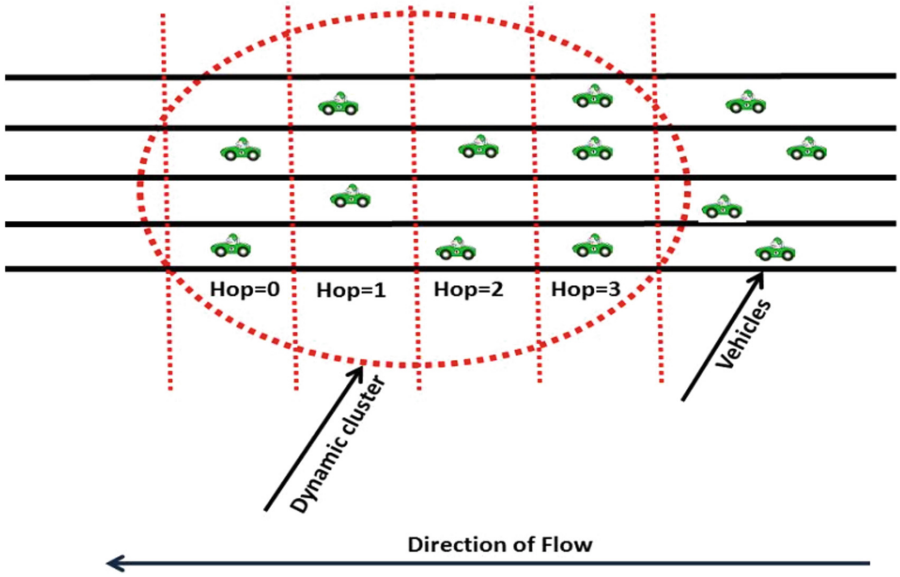


Fig. 3. Dynamic clustering

Algorithm 2 Dynamic Clustering

1: Vehicle that sensed first any event broadcast code of event, token, RID, public key, lane and hop-count.
2: **For** each vehicle that receives the token && hop-count >= 0
Broadcast its same information with one less hop-count.
End For
3: All vehicles that have non-negative hop-count are the part of cluster.

4.3 Cluster-Head Selection

In an urban scenario, if the vehicle is located on leftmost lane, it has to turn left and if it is located on right most lanes, it has to turn right [21]. So, we avoid the vehicles which are located at either leftmost or rightmost lane in the process of cluster-head selection. So, we chose vehicles from middle lanes because it will remain in the cluster for a longer period of time so that it can avoid frequent cluster head selection process.

Every vehicle has information of its neighboring vehicle and sends its coordinate and speeds to all vehicles which are located in middle lane. It sends new random identity (RID), its token (TOKEN), number of tokens received from neighbors (NOT), coordinate (CORDT), velocity (VEL) and timestamp (TS). It encrypts the message with the public key of concerned vehicle.

$$\{\text{RID, TOKEN, CORDT, VEL, NOT, TS}\}_{\text{PUB\_KEY\_VECL}}$$

Now each vehicle calculates the central location of cluster using the coordinates of neighboring vehicle and then finds out the relative distance using central location [22] for every vehicle in the table.

$$X = \frac{x_1 + x_2 + x_3 + \ldots x_n}{n}$$

$$Y = \frac{y_1 + y_2 + y_3 + \ldots y_n}{n}$$

$$RD_i = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$$

Now every vehicle sorts the velocities of every neighboring vehicle and finds out the median and then using median it finds out relative velocity for every neighboring vehicle [23].

$$\mathrm{V_m} = \text{Median}\left[\text{Sort}\left(\mathrm{v_1}, \mathrm{v_2}, \mathrm{v_3} \ldots \mathrm{v_n}\right)\right]$$
$$\mathrm{RV_i} = \left|\mathrm{v_i} - \mathrm{V_m}\right|$$

Algorithm 3 Cluster-Head Selection

1: **For** each vehicle i in a cluster
V_i forwards its velocity (v_i), location ({ x_i, y_i}) and no of token (NOT) to all the vehicle that are travelling in middle lane.
End For
2: **For** each vehicle i in a cluster, It calculates relative distance (RD).

$$X = \frac{x_1 + x_2 + x_3 + \cdots x_n}{n}$$

$$Y = \frac{y_1 + y_2 + y_3 + \cdots y_n}{n}$$

$$RD_i = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$$

End For
3: **For** each vehicle i in a cluster, It calculates relative velocity (RV).
V_m= Median [Sort (v_1, v_2, v_3 ...v_n)]
RV_i= |v_i-Vm|
End For
4: **For** each vehicle i in a cluster
If (Token (V_i) == Token (v_j))
If (RD (V_i) == RD (v_j))
If (RV (V_i) == RV (v_j))
Random (V_i ,V_j)
Else
CH= Min (RV (V_i), RV (v_j))
End If
Else
CH= Min (RD (V_i), RD (v_j))
End If
Else
CH= Max (Token (V_i), Token (v_j))
End If
End For
5: A vehicle announce itself as cluster-head if it is elected as cluster-head.

Vehicle calculates relative distance (RD) and relative velocity (RV) and maintains information locally about itself and all other vehicles. Vehicles start analysis of information received, if it has received the greatest number of token than any other vehicle. Then it announces itself as cluster head. It is possible that two vehicles received same number of tokens. Then we chose relative distance and relative velocity for resolving conflict. If two or more than two vehicles have same number of tokens received then it announces itself as cluster head only when it has lowest relative distance and if relative distance is also same then we will choose lowest relative velocity. In the case where relative velocity, relative distance and number of tokens are same then random function is use as decider. Random function provides the same result at different vehicle for same set of data. Hence, it won't cause any further conflict.

Vehicles may waste their time in the selection of cluster-head, if vehicles are moving at very high speed. That causes dynamically topology changes. Hence, that vehicle must be elected as cluster head which is close to center of cluster because then vehicle remain in a cluster for a longer period for avoiding frequent cluster head selection processes. Vehicles that are at the boundary of cluster will not have high number of tokens because they will have a smaller number of neighboring vehicle and vehicles that are close to the center of cluster will be having a greater number of tokens because of more vehicles in neighborhood. This is the reason to choose token number as a criterion for electing cluster head.

Attacker has a capability to alter its transmission strength. If attacker is not the neighbor of vehicles, still it can have tokens form other vehicle by altering its transmission strength. But other vehicles will not receive tokens from the non-neighboring vehicles or attackers because the messages sent by the attacker will be in its buffer. While vehicles wait for the event to be detected. When it detects the event, it starts analysis at the time at which messages received by the other vehicles. All the messages which received by neighboring vehicles have a small-time difference but the messages received by attacker have a large time difference. So, it drops the token which has large time difference.

The vehicle that announces itself as cluster-head must broadcast a packet containing token (TOKEN), relative distance (REL_DIST), relative velocity (REL_VEL) and neighbor tokens (LIST_OF_TOKENS).

$$\{\text{TOKEN, REL\_DIST, REL\_VEL, LIST\_OF\_TOKENS}\}_{\text{GROUP\_KEY}}$$

Legitimate vehicle chosen as cluster-head communicates to RSU and report about the event detected. This information floods from RSU to RSU and to all BRSUs. Then all RSUs and BRSUs inform vehicles about the event and vehicles can chose alternate path or can take pre-requisite measure for its safety. If attacker wrongly announces itself as cluster-head then all legitimate vehicle starts revoking against its claim for cluster-head and attacker will be fail to communicate to RSU.

4.4 Prevention from Sybil Attack

- A malicious vehicle can alter its transmission strength whenever it wants. In this approach vehicle receive information and token only form the neighboring vehicles. Suppose attacker is not the neighbor of some vehicles. Still it can transfer false information to neighboring as well as non-neighboring vehicle. But vehicles will not forward its token until or unless it detects the event by itself. When it detects the event, it found the information false that is given by attacker. So, it discards the message and report about the vehicle to the RSU using its token number. Vehicle can be identified by its token number. So, attacker will avoid transferring wrong information.
- In this approach only cluster-head communicate to the RSU. Cluster-head selection process entirely depends upon the number of tokens. The vehicle carrying the

greatest number of tokens is elected as cluster-head. An attacker can alter its transmission strength and report the actual event that took place. In this way it can distribute its token and public key to all vehicles in the cluster. Legitimate vehicle will find information right after detecting the event by itself. Then legitimate nodes transfer their tokens to attacker. In this way it can have the greatest number of tokens. But it has to broadcast the information to RSU as well as all neighboring vehicle. So, if it broadcast false information. It can be easily identified by vehicles as well as RSU because they have attacker token number. Token plays a crucial rule in this approach and restricts attacker to launch Sybil attack.

- Attacker can also have token for all neighboring vehicles without broadcasting its token. In this way all legitimate vehicles will not have the token of attacker. In the packet not only token but public key is also broadcasted. If attacker does not broadcast its token and public key. Then it will not get any further information. That will be useful at the time of announcement, because cluster-head also need to mention relative velocity and relative distance. In this way either attacker will take part fairly or it will not take part at all.
- If attacker wrongly announce itself as cluster-head by providing wrong information in term of number of token (NOT), then it will fail to show the tokens.

4.5 Token Maintenance

These tokens are distributed by BRSUs to vehicles. Vehicle use this token to not only cast their vote but also use for dynamic clustering. If a token is used by multiple times then there is a huge threat that any attacker can have that token, then attacker can use it for distorting the function of VANET by launching Sybil attack. Suppose in a scenario attacker did not behave maliciously, then it can have tokens of all neighboring or non-neighboring vehicles. Next time, attacker can have multiple tokens for multiple identities and it will be easy to launch Sybil attack. So, maintenance of token is necessary. Whenever a token is been used by vehicle, it must be replaced by another token. Vehicles send a request message to RSU. RSU authenticate the request. Then grant the vehicle a new token. Then it updates the vehicle profile.

5 Simulations and Results

We simulate this proposed methodology in MATLAB (version 7.10.0). In simulations, RSUs are placed alongside a 2-way, 3-lane-each road segment and BRSUs are placed in the overlapping region of two segments. Vehicles move at random speeds, chosen from [25, 35] m/s. A sequence of events happens over time and location. A vehicle that finds an event at its current time and location, broadcasts this event with attaching the token assigned to it during initialization. Attacker vehicles are simulated to broadcast random events using a random number of pseudonyms (a Sybil attack). As soon as vehicles detect events, they start executing this approach. Details of the simulation parameters are presented in Table 2.

Table 2. Parameters uses in Simulation

Parameters	Values
Simulation time	400 s
Communication range	150 m
Length of roads	2000 m
Number of lanes	3
Number of event types	4
Vehicle speed	20 m/s
Event interval	20 s

5.1 Performance Metrics

The performance of proposed methodology is evaluated by performing series of experiments. Following performance metrices are used: (1) Detection Rate (DR), (2) False Positive Rate (FPR) and (3) False Negative Rate (FNR).

- **Detection Rate (DR):** This is defined as per the following expression. If TPD refers to true positives (number of malicious nodes correctly identified as attacker) and TPR is the number of attacks, detection rate is determined by

$$DR = \frac{TPD}{TPR} * 100\%$$

- **False Positive Rate (FPR):** This is defined as per the following expression. If False positive (FP) refers to legitimate vehicles incorrectly identified as malicious and NB refers to the total number of messages analyzed by RSUs, then

$$FPR = \frac{FP}{NB} * 100\%$$

- **RSU Load:** This is defined as per the following expressions where FP refers to False Positive, TP refers to True Positive and NB refers to the total number of messages analyzed.

$$DL = \frac{FP + TP}{NB} * 100\%$$

5.2 Simulation Results

The experiments were performed with simulation time of 400 s. It is assumed that there are 3 lanes and length of the road is 2000 m. Communication range is of vehicle is 150 m while communication range of RSU and BRSU is 300 m and 400 m respectively. It is

assumed for simulation that there are only 20 vehicles per kilometer in a lane. In Fig. 4, it is shown the comparison of approaches on the basis of false positive rate. False positive rate defines the number of legitimate node reported as Sybil attacker. L-P2DSA and C-P2DAP entirely depends on infrastructure (Road Side Unit) and Sybil attack detection is performed by RSU only. So it increases the rate of false detection while in proposed approach detection is performed by vehicles. All vehicles help to detect Sybil attack that decreases the false positive rate. So if a vehicle wrongly declares a legitimate vehicle as adversary, still it won't increase false positive rate until or unless all vehicle in a cluster provide wrong result.

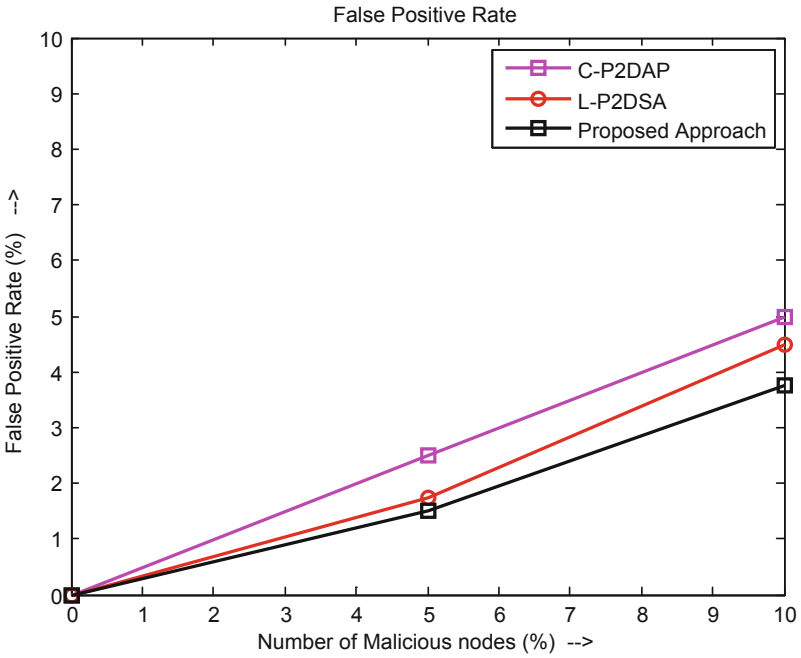


Fig. 4. False positive rate

In Fig. 5 it compares the detection rate between C-P2DAP, L-P2DSA and proposed approach. Detection rate is defined as number of attackers truly identifies as attacker. In the proposed approach, detection is performed by group of vehicles that increases the rate of detection because vehicles cooperate to one another. While in C-P2DAP and L-P2DSA, it is entirely dependent on RSUs. RSUs are semi trusted party and it can be compromised too while it is difficult to compromising all vehicles in a cluster.

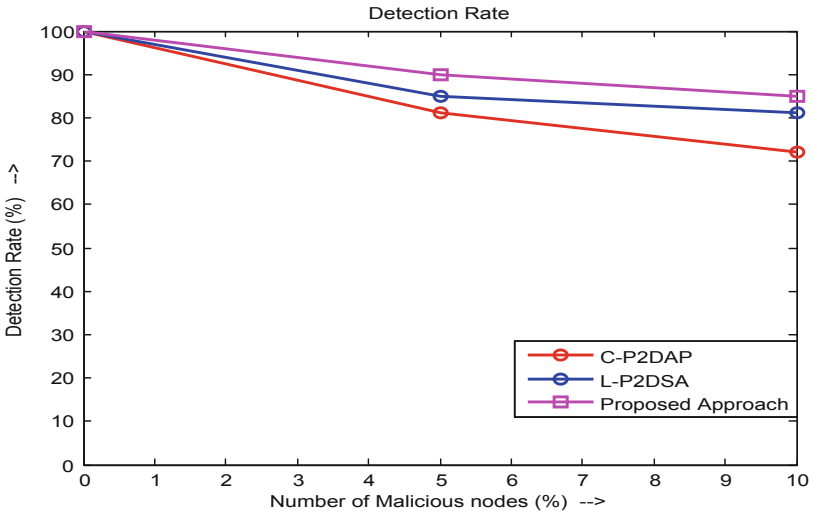


Fig. 5. Detection rate

C-P2DAP and L-P2DSA is highly dependent on infrastructure, so whole algorithm executes at RSUs. It increases the load on RSU. While in the proposed approach vehicle detects Sybil attack locally and all algorithms executed in a cluster between the vehicles that reduces the huge load on RSU. In Fig. 6, it is shown the comparison of RSU Load between above mentioned three approaches.

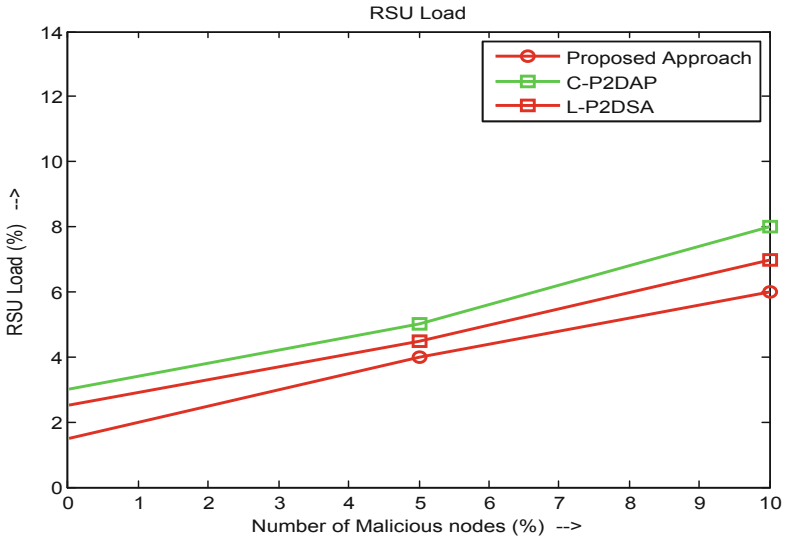


Fig. 6. Load on RSU

6 Conclusion

In Sybil attack a malicious node uses multiple identities to create an illusion about non-existing nodes. In VANETs privacy of vehicles is of primary importance. Prevention and detection of Sybil attack in privacy preserved VANETs are challenging. In this paper, we proposed a token-based pseudonym-less approach where BRSU distribute token set to all vehicles to report for events. Vehicle use this token to report for an event. A malicious vehicle can use multiple identities in different event reporting messages. But it has only one token. So, if it uses multiples messages with different identities, it will end up using same token. That will be identified by vehicles locally and subjected to revoke. This approach reduces the load on RSU by dynamically creating cluster. Vehicle chose cluster-head and only cluster-head is responsible for communicating with RSU. Cluster-head report about the event-detected to RSU and RSU floods this information to other RSUs and vehicles. So, it detects and prevents the Sybil attack. More importantly, vehicles need not to disclose its identity.

References

1. Wong, K.D., Tepe, K.E., Chen, W., Gerla, M.: Inter vehicular communications. IEEE Wirel. Commun. **13**(5), 6 (2006)
2. Muller, T.L., Daimler Chrysler, A.G., Schoch, E., Kargl, F.: Position verification approaches for vehicular ad hoc networks. IEEE Wirel. Commun. **13**(5), 16–20 (2006)
3. Raya, M., Papadimitratos, P., Hubaux, J.-P.: Seuring vehicular communications. IEEE Wirel. Commun. **13**(5), 8–13 (2006)
4. Hubaux, J.P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Secur. Priv. **4**(3), 49–55 (2006)
5. Xio, B., Yu, B., Gao, C.: Detection and localization of Sybil nodes in VANETs. In: Proceedings of Workshop Dependability Issues in Wireless Ad hoc Networks and Sensor Networks, pp. 1–8 (2006)
6. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2004), pp. 29–37 (2004)
7. Raya, M., Hubaux, J.P.: The security of vehicular networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), pp. 11–21 (2005)
8. Parno, B., Perrig, A.: Challenges in securing vehicular networks. In: Proceedings of the Fourth Workshop on Hot topics in Networks (HotNets-IV) (2005)
9. Douceur, J.: The Sybil attack. In: First International Workshop on Peer to Peer Systems (2002)
10. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor network: analysis and defenses. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, California, USA (2004)
11. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (2004)
12. Pal, S., Mukhopadhyay, A.K., Bhattacharaya, P.P.: Defending mechanisms against Sybil attack in next generation mobil ad hoc networks. IEEE Tech. Rev. **25**, 209–215 (2008)

13. Xiao, B., Yu, B., Gao, C.: Detection and localization of Sybil nodes in VANETS. In: Proceedings of Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (2006)
14. Park, S., Aslam, B., Turgut, D., Zou, C.C.: Defense against Sybil attack in vehicular ad hoc network based on roadside unit support. In: Military Communication Conference (2009)
15. Mekliche, K., Moussaoui, S.: L-P2DSA: location-based privacy-preserving detection of Sybil attacks (2013)
16. Zhou, T., Choudhury, R.R., Ning, P., Chakrabarty, K.: Privacy-preserving detection of Sybil attacks in vehicular ad hoc network. In: Proceedings of International Conference on Ubiquitous (2007)
17. Hussain, R., Oh, H.: On secure and privacy-aware Sybil attack detection in vehicular communications (2014)
18. Ayaida, M., Messai, N., Najeh, S., Ndjore, K.B.: A macroscopic traffic model-based approach for Sybil attack detection in VANETs. In: Ad Hoc Networks, vol. 90, July 2019
19. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
20. Kumar, P., Chauhan, N., Chand, N.: Node activity based routing in opportunistic networks. In: Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958, pp. 265–277. Springer, Singapore (2018)
21. Khanna, A., Goyal, R., Verma, M., Joshi, D.: Intelligent traffic management system for smart cities. In: Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958, pp. 152–164. Springer, Singapore (2018)
22. Hussain, R., Oh, H.: On secure and privacy-aware Sybil attack detection in vehicular communications. IEEE (2014)
23. Sun, J., Zhang, C., Zhang, Y., Fang, Y.: An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans. Parallel Distrib. Syst. **21**, 1227–1239 (2010)
24. Mohammad, S.A., Michele, C.W.: Using traffic flow for cluster formation in vehicular ad-hoc networks. In: IEEE Transactions on Local Computer Networks (LCN), pp. 631–636 (2010)
25. Lo, S.-C., Lin, Y.-J., Gao, J.-S.: A multi-head clustering algorithm in vehicular ad hoc networks (2013)

Key Management Schemes in Internet of Things: A Matrix Approach

Shubham Agrawal(✉) and Priyanka Ahlawat

NIT Kurukshetra, Kurukshetra, Haryana, India
shubhamagrawal66@gmail.com,
priyankaahlawat@nitkkr.ac.in

Abstract. Internet of things (IoT) as a rising technology have a great potential to be used in essential scenarios such as battlefields and industrial applications like construction, traffic monitoring, environment watching and smart homes and many other situations. One of the major challenge IoT security face today is vulnerability to various attacks. It is important to consider the inherent security challenges, like securing the communication channel between two sensor nodes to increase its performance. In order to achieve it, it is necessary to apply key management mechanisms between the nodes to shield or protect the information flow. The purpose of this chapter is to introduce different matrix based key management schemes in IoT and give a deep understanding of some security mechanisms which are used to secure the communication channel. Key establishment could be a difficult problem due to the resource constrained sensor nodes. Despite the fact, several effective solutions are proposed but none of them is practical and appropriately suitable for extremely large amount of sensor nodes. This chapter presents significant matrix based key management systems that are implemented in real world for IoT security. This chapter present some of the techniques like BLOM's, CARPY, KRONECKER PRODUCT and some other pairwise key management schemes. A comparison of different matrix based key management schemes is presented along with their merits and demerits.

1 Introduction

The Internet of Things (IoT) permits a variety of devices that are used in day to day life to communicate and connect with each other by sharing information through the Internet. IoT devices includes computers, smartphones, smart watches, and other handheld devices, which can connect to the Internet and communicate with each other. The controller of IoT devices or the IoT devices network can monitor and make smart decisions about a given task by using the information shared by the IoT devices in real time [1].

Security issues in IoT becomes important because the devices in the IoT have the capability of connecting to the internet, thus attracting privacy attacks which may lead to harmful consequences if the sensitive information is revealed [2]. We need to ensure that the communication is secure by deploying key management scheme, authentication and authorization mechanisms.

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 381–400, 2020.
https://doi.org/10.1007/978-3-030-40305-8_19

Wireless Sensor Network (WSN) is an crucial technology of IoT network, which is composed of sensor nodes that are used to sense, guide and monitor the environmental conditions, such as waste management, water management, weather temperature control and natural disaster, just to name a few. As almost everything is connected to the Internet, WSN becomes the crucial technology for IoT. Wireless sensor networks are mobile ad hoc network, which consists of sensor nodes, which are limited in resources and are capable to communicate with other sensor nodes and the central station that controls the sensor nodes to monitor the environment [3, 4]. The devices in WSN, called as sensor nodes contains inbuilt sensors, small microcontroller, wireless communication device and an energy source. Each sensor node has constrained on the resources such as memory, energy, computation speed and bandwidth due to their small size and less cost.

The applications of WSN range from small appliances at home to military and battlefield surveillance, habitat monitoring, traffic control, as well as Healthcare. These applications require a secure communication. Thus, security protocols and key management techniques become necessary for Wireless sensor networks.

1.1 Challenges in Key Management for IoT Security

This section introduces various challenges of the key management and key establishment in IoT. There must be well-established security mechanisms to provide the security and information privacy in IoT devices. There are well-defined examples of key exchange mechanisms such as Diffie-Hellman key exchange security mechanisms, etc. These mechanisms require numerous high computational operations to perform cryptographic operations for key exchange [5–7].

Lightweight key management systems are required due to the limitation of power and energy on the constrained devices. These constraints involve limited storage capabilities, very little computational power, limited battery life and network bandwidth. The problem might be solved by using symmetric algorithms, which uses same set of keys for a group of devices, but it may be more vulnerable and exposed to attacks. Once a key is revealed, the communication of the entire group of networks can be compromised.

The creation of secure channels is not enough to satisfy the security of sensor nodes and their information. Along with secure key management schemes, we must establish authentication and authorization mechanisms to avoid illegal access to the Wireless sensor network system and to avoid unauthorized access by unauthorized users.

The challenges faced by Wireless sensor networks are numerous. These challenges need to be overcome in order to ensure the safety and security of IoT network.

The wireless sensors of IoT devices can be installed in public places, which are connected by the internet. Generally, wireless communications in Internet are secured by the means of Encryption. Encryption process cannot be applied on IoT devices since they are not powerful enough to apply it. Hence, to enable Encryption in IoT devices the algorithms need to be more efficient and less energy consuming [8].

In addition to encryption, identification of a sensor node is very important in security management model. All nodes need to be uniquely identified in a sensor network. Thus, ensuring that the sensor nodes or objects are who they say are, is very essential in IoT

deployment. As almost all the objects in IoT network are traceable, there might exist a good chance of threats to personal privacy of an individual sensor node.

Along with securing the data to make sure that it does not fall into unauthorized hands, we must ensure that a user feel comfortable in participating in IoT network by addressing the issue of data ownership. The data owner must be ensured that his/her data will not be shared or used by others without his/her permission. Privacy policies can be applied to ensure the data privacy of the information. Smart objects and sensor nodes in the IoT could be equipped with privacy policies and whenever two nodes meet each other they can easily check the privacy policy of each other before communicating.

The severe security challenges are classified as follows. These are real world challenges and a key management solution must be taken to overcome these challenges.

i. The wireless links used to connect the devices are vulnerable to eavesdropping attacks.
ii. Another issue is related to the lack of a central authority for the sensor network.
iii. Many devices are highly constrained in resources such as limited battery life, low computational power, less memory capacity, etc.
iv. The sensor nodes are accessible by the other network objects via the Internet, which exposes them to several types of attacks, such as Denial-of-Service (DoS) attack.

1.2 Organization of Chapter

The chapter is organized in the following manner. In Sect. 2, the chapter presents an introduction to key management systems and why is it necessary to implement key management for securing the wireless channels in IoT. Along with this, properties of key management schemes are classified. Section 3 presents the related work in IoT security and Key management schemes used in various proposed schemes. In Sect. 4, the chapter throws light on various Matrix-based key management schemes used in previous years. Each scheme is followed by performance and security analysis. Section 5 compares the schemes with respect to computation and storage cost.

2 Key Management in Internet of Things

One major challenges while connecting an IoT network to the internet is to have a secure channel that can shield the information flowing through it. This problem is specified when the sensor nodes transfers the information with a base station. This base station acts as an interface between the users of the network and the services provided by the sensor nodes. The communication between the sensor nodes and the base station is protected using security mechanisms, such as using shared keys between the nodes and the base station [9].

Sometimes nodes require a direct channel between other nodes. Whenever such scenario occurs, it is required to apply a key management mechanism that will allow two remote devices to share the security credentials that would be used to protect the data flowing.

2.1 Role of Key Management System in IoT

More and more security problems are emerging due to the rapid growth of Internet and the devices, which are connected to the network. One of the important problems in IoT is to provide a secure communication channel between the two connecting sensor nodes. Hence, secure key management mechanisms are required to permit two remote sensing devices to negotiate some security credentials, which could be used to protect the information flow. The problem in hand is to setup the keys between communicating devices.

Key management systems are the heart of secure communication systems. The aim of key management schemes is to create a secure link between two communicating sensor nodes. The two sensor nodes establish a common key to have a secure communication between them [10].

2.2 Properties of Key Management System in IoT

Every key management system has some properties that are suitable for the creation of a secure session key between two connecting remote entities. Let us go through these properties, which will later be helpful to compare the different key management systems [11].

i. Distribution

This property indicates how the information required for the negotiation of shared secret keys is distributed. The information distributed contains him cryptographic/encryption key, public key certificates and pre-shared keys. Distribution is often considered as an offline procedure as all the information required by the nodes to create a secure communication channel is stored in the nodes before they are deployed in the sensing environment. A distribution process can also occur online whenever the information needs to be transferred during the negotiation process. In IoT communication, an online distribution is preferred over the offline distribution as any sensor node can establish a secure channel with any other node or the base station/server at any point of time, while they are in sensing environment.

ii. Authentication

This property indicates the process in which an entity or a sensor node is verified as a genuine entity of the system. This property defines whether the sensor nodes/clients/users are checked for authentication during the negotiation process or not. This is achieved by using a unique shared key or a unique signature. In IoT communication, it is desirable to use authentication on the server side, to assure that the data, which is obtained by the peer entities are obtained from the right/authenticated sensor nodes/entities, or not.

iii. Overhead

This property indicates what the communication overhead are and what the computation overhead are during the execution of negotiation process. This property is desirable to be applied on a sensor node, as they are much more resource constrained

than the server host or any other Internet host present in the network. Also, the energy that is consumed by these sensor nodes during the process of sending and receiving of data or information is very high, which is undesirable as the nodes are battery powered. In IoT communication, it is required to minimise these overheads as lol as possible.

iv. Scalability

This property indicates the amount of information that needs to be stored within a device. The information, which is stored in these devices, are used during the negotiation of secure channel between two entities. This information must enable a sensor node to negotiate with as many entities as possible within the sensing network.

An IoT network can be accessed by a huge number of devices, which needs to communicate/negotiate with other nodes to create a secure connection. In IoT communication, a key management scheme is defined to be not scalable, if the pre-loaded information within a node/client increases linearly with the increase of client nodes in the network. A key management system is defined to be scalable, if the data required to be stored within a node/client does not increases the storage overhead to the device. It is necessary to have a high scalability factor.

v. Extensibility

This property indicated the number of external nodes, which could be added into the present network, without increasing the overhead to the network. A key management system is defined to be non-extensible, if the number of external devices that could be added is limited to a certain number.

Many key management schemes are proposed in the chapter for creating a secure IoT network, which are mainly classified into two main categories: pre-shared key approaches and public key approaches. In this chapter, we primarily focus on pre-shared keys schemes, in which the secret keys are preloaded into the node's memory, and are then used to generate the shared secret key for creating the secure channel.

2.3 Pre-shared Keys

In a pre-shared key strategy, the clients and the servers, which are to evaluate a shared secret key between them, share a pre-established key material. In IoT communication, there are a number of approaches to implement this pre-shared key strategy. A collection or a set of sensor nodes can be allowed to have same pre-shared secret key, or every single sensor node can have its unique pre-shared secret key. There are four main approaches used in IoT or WSN environment.

i. 1-1: In this method, a same pre-shared secret key is shared between a group of nodes and a group of servers.
ii. 1-s: In this method, every client c is given one key per server. Every server s consists of its own pre-shared key.
iii. C-1: In this method, a pre-shared key is given to every client in the network. A server is informed in advance about the number of clients that will connect to it, and hence it needs to store a secret key per client.

iv. c-s: In this method, every individual client c and server s, shares a common pre-shared key.

The disadvantages of using pre-shared keys are as follows.

i. All useful and secret information must be preloaded into the sensor nodes in advance to share the information with other connecting nodes, which increases the overhead to a node in the sensing network.
ii. The only possibility is to securely connect the clients and servers that are known to each other; hence, no new entities could be able to communicate, which affects the extensibility of the network.
iii. Since one type of elements are allowed to store all the pre-shared keys (everyone in 1-1, clients in 1-s, servers in c-1), such elements are the weakest links in the entire network. If the adversary gains control of such elements, the entire network can be taken control of.

It is desirable in IoT communication to reuse the pre-shared key every time. It is appropriate to apply such a mechanism that will compute a session key using the pre-shared keys. Such keys have to be updated over time.

The advantages of using pre-shared keys are as follows.

i. The computational overhead is very less, since the pre-shared key is already present in a node's memory.
ii. No requirement for costly negotiation as the keys are already preloaded which are used for secret channel formation.
iii. The scalability is very high.
iv. It is easily possible to authenticate the client as well as the server.
v. The extensibility is quite high.

3 Related Work

In this section, we are going to explain some of the matrix based schemes presented by the authors in the past few years. The section covers a brief introduction about the scheme presented by the authors along with the method used, along with their advantages and disadvantages.

Padmavathi et al. [1] presented an exhaustive survey of various attacks and the various defensive mechanisms for WSNs. This paper presents a classification of various security attacks. It throws light on many security mechanisms and the core challenges in wireless sensor networks. It gives a detailed information about the security goals in Internet of Things, such as Data confidentiality, Data authentication, and Data integrity, Data availability along with some secondary goals such as Data freshness, Time synchronization and secure localization. This paper presents a number of security attacks that can compromise the sensor network. These attacks are broadly classified into Active and Passive attacks. A variety of security mechanisms is discussed to prevent the attacks. Security mechanisms are classified as low level and high level, where low-level security includes key establishment, trust setup, secrecy.

Authentication, privacy, etc. At last, the paper presents significant challenges in designing security schemes, such as a wireless medium is less secure from eavesdropping attacks, no statically structure for the network can be pre-defined as the network is always changing by addition, deletion and modification of sensor nodes, etc.

In Yu et al. [2], a Constrained Random Perturbation based pairwise Key Establishment scheme (CARPY and CARPY+), for wireless sensor, networks are presented. The scheme proposed meets all requirements such as (1) efficiency, (2) resilience to attacker's intervention, (3) guaranteed key establishment, (4) resilience to dynamic deployment of nodes and (5) resilience to network configuration. CARPY+ is the first non-interactive key management scheme proposed which has a very high resilience to a large number of compromised nodes.

In Tsai et al. [3], a scheme based on matrix key establishment is proposed, which is studied in detail in this chapter in Sect. 4. The scheme uses a Kronecker product method used in matrix key management and satisfies the following conditions. (1) it decreases the amount of data needed to be stored in a sensor node, (2) it computes the pairwise key in an efficient manner without increasing the computation cost, (3) it has no communication cost during the computation of pairwise key between a pair of nodes as it only uses the identification number of another node to generate the secret key. Thus, this scheme is better in terms of computation cost, communication cost and storage cost, which are thoroughly discussed in this chapter. Different trends in IoT security are given in [4] by Whitemore. Zhang et al. presented different KMS based on different performance parameters for WSN [5]. KMSs for IoT is given Roman et al. in [6]. Li et al. survey different aspects of IoT in [7]. Nafi et al. [8] presented a lightweight key management scheme for IoT security, which provides more scalability, resilient to several attacks as well as flexible. It is shown that it has reduced the amount of information to be exchanged and stored during a key establishment. They focus on optimizing all the performance criteria without neglecting any. It is shown that this scheme can protect usr's privacy as well as saves energy, which is very necessary for resource-limited network. Another scheme presented by Rahman et al. [10], improves the initial Blom's scheme, to make it more suitable for using in an environment, which is full of resource-constrained nodes. In this scheme, a pair of sensor nodes are capable of producing/generating a common shared key without even exchanging any information between them. The identification number of the node to which a sensor node is trying to communicate achieves this. A node in this scheme does not need to exchange any part of the public column of matrix G. a node generates the required information by using the node's identification number. This helps in reducing the storage and communication overhead. This scheme also provides a mechanism for key updation and addition of new nodes after the deployment along with removing the compromised nodes. This makes the scheme more flexible. The disadvantage is that, a node has to generate the public matrix G itself. This increases the computation overhead on the sensor node and make it more vulnerable to several attacks. When an attacker gets control over a single node, he is able to compute all its shared keys and the secret matrix.

Initially the matrix-based design for creating secure channel using pairwise keys was proposed by Blom [11]. It allows a pair of sensor nodes to compute a common pairwise key, which is calculated on the basis of set of matrices. The matrices are initially preloaded into the memory of a sensor node before its deployment. Three types of matrices are used in sensor node network to compute the secret keys and create a secure channel between any pair of sensor nodes. First, a public matrix, called G is used which is known to anyone present in the network including the adversary, second a random symmetric key, called as D and a secret symmetric matrix, called as A. this chapter will explain the procedure of key sharing in detail in Sect. 4.1. It has been shown in [11] that the scheme is λ-secure, which means after λ nodes have been captured by the adversary, the network can be compromised. It means when the number of compromised nodes are more than λ (threshold), the entire secret key matrix could be calculated and the entire network can be compromised.

Another scheme proposed by Du et al. [12] defined a new pre-distributed scheme which achieves better resilience by using multi-space key and prevents the network from node capture attack. In this scheme, every node is preloaded with a row vector of λ + 1 elements. It is more efficient with communication cost, but is not better in terms of computation and storage cost. In this scheme, nodes need not have to share or exchange their public column, which in turn minimize the communication overhead, but increases the computation overhead as the column needs to be regenerated by the node itself.

Yu and Guan in [13], presented a key management scheme which uses the deployment technique based on Blom's scheme. The network area is partitioned into hexagons, squares or triangles, and the sensor nodes are arranges in groups depending upon the number of grids. This scheme shows that the hexagon grids are best for memory requirements and security purposes. All groups share the same public global matrix G and each sensor node is preloaded with a unique secret matrix A and a set of B matrices, this happens during the keys predistribution phase. Each node stored one row of matrix A, one column of matrix G and at most w rows of matrices B. If more than λ nodes are compromised, it is very easy to break the matrix A and B matrices. This scheme provides higher connectivity with a very less memory requirements. It is also more resilient to node capture attack.

4 Matrix-Based Key Management Schemes in IoT

This section discusses some significant matrix-based key management schemes. Starting with the oldest technique that is Blom's approach, this chapter will explain various advantages and disadvantages of proposed schemes along with the new schemes that are proposed to overcome the disadvantages of the previous schemes. We have chosen the following techniques, as they are easy to understand and does not require very complex computation to generate the keys. Blom's scheme is the first scheme that uses matrix based key distribution. Other schemes like Carpy are extension of Blom's scheme. Kronecker product is a different operation, which is used to generate the session keys between the nodes.

4.1 Blom's Scheme

In 1985, Blom proposed a matrix-based key distribution scheme. In this scheme, a symmetric matrix K stores all the possible pair wise keys which could be calculated by the sensor node and is a valid entry. Suppose there are N sensor nodes present in the network and for a matrix G we denote the elements in the i-th row of G by $G_{i,-}$ and j-th column by $G_{-,j}$.

Blom's idea states that for each node i, the row vector $A_{i,-}$ and column vector $G_{-,i}$ are stored into the node i. A is the secret matrix, or the private matrix and G is the public matrix.

When node i and j would like to have a key, they exchange their columns of G and use the private A to calculate the key. Thus, after the deployment of these nodes into an environment, each pair of nodes i and j can uniquely calculate a pair wise key $K_{ij} = K_{ji}$, by only exchanging their column.

The key is calculated by performing the product of node i row and the column of another node to which it is connecting with. Here it is noted that the rows of each node are kept secret from the network.

It cannot be applied to WSNs due to the storage overhead, as it grows rapidly when the network size is large. The scheme has the λ- security, which means that if more than λ rows of secret matrix A are compromised, then the entire secret matrix A can be broken by the adversary.

$$\begin{matrix} & \text{A} & & & & \text{G} & & & & & \text{K} & & \\ \begin{bmatrix} 34 & 40 & 42 & 36 \\ 21 & 27 & 25 & 19 \\ 18 & 18 & 16 & 12 \\ 19 & 20 & 19 & 16 \end{bmatrix} & \cdot & \begin{bmatrix} 4 & 1 & 1 & 2 \\ 4 & 2 & 1 & 1 \\ 2 & 4 & 1 & 1 \\ 4 & 1 & 3 & 3 \end{bmatrix} & = & \begin{bmatrix} - & - & 224 & - \\ - & - & - & - \\ 224 & - & - & - \\ - & - & - & - \end{bmatrix} \end{matrix}$$

$$K_{1,3} = 34 * 1 + 40 * 1 + 42 * 1 + 36 * 3 = 224$$

$$K_{3,1} = 18 * 4 + 18 * 4 + 16 * 2 + 12 * 4 = 224$$

$$K_{1,3} = K_{3,1}$$

4.1.1 Performance Metrics

i. *Computation cost*: It is the cost incurred during the key establishment between two adjacent sensor nodes. The computation cost turns out to be O(N), where N equals to the number of nodes in the network.
ii. *Storage cost*: The space needed to store the keying credentials constitute its storage cost. The Storage cost also turns out to be O(N), where N denotes the number of nodes present in the network.

Figure 1 depicts the variation in communication overhead of Blom scheme with number of sensor nodes. As we see that if we increase the number of nodes, the communication cost of setting a pairwise key increases in a network.

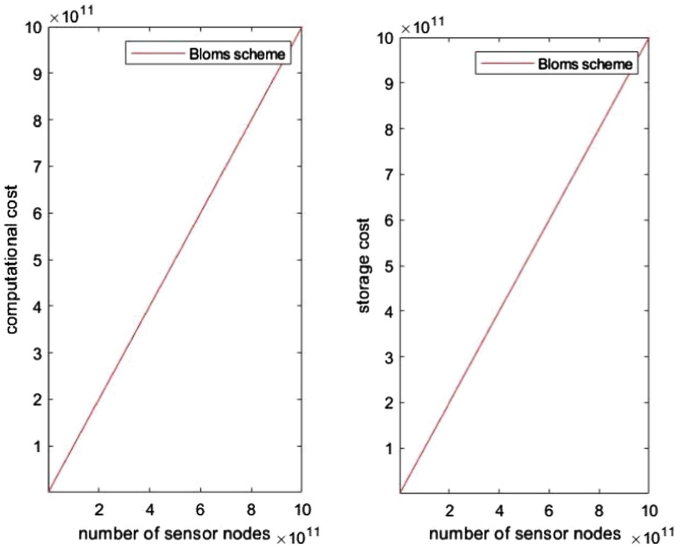


Fig. 1. Analysis of communication overhead and storage overhead of Blom scheme with number of sensor nodes

4.2 Kronecker Product Scheme

Given two matrices such that, A is an (m × n) matrix and B is a (p × q) matrix, then the Kronecker product of the two matrices A and B (denoted by A ⊗ B) is an mp × nq block matrix. The Kronecker product and the common matrix multiplication are very dis-similar operations. Matrix multiplication is more complex and more time consuming than Kronecker product [3] a_{11}.

$$\mathrm{A} \otimes \mathrm{B} = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

It is written as $(A \otimes B)_{p(r-1)+v,q(s-1)+w} = a_{rs}b_{vw}$.

Example:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} = \begin{bmatrix} 1\times0 & 1\times5 & 2\times0 & 2\times5 \\ 1\times6 & 1\times7 & 2\times6 & 2\times7 \\ 3\times0 & 3\times5 & 4\times0 & 4\times5 \\ 3\times6 & 3\times7 & 4\times6 & 4\times7 \end{bmatrix} = \begin{bmatrix} 0 & 5 & 0 & 10 \\ 6 & 7 & 12 & 14 \\ 0 & 15 & 0 & 20 \\ 18 & 21 & 24 & 28 \end{bmatrix}$$

This scheme is entirely dependent on the creation of symmetric matrices, so let's quickly have a look at the symmetric property defined for the Kronecker product.

If $\mathrm{A} \in \mathbf{R}^{\sqrt{m}\times\sqrt{m}}$ and $\mathrm{G} \in \mathbf{R}^{\sqrt{n}\times\sqrt{n}}$ are symmetric, then $A \otimes G$ is also symmetric.

4.2.1 Algorithm

The matrix that is used to calculate the keys for various pairs of nodes need to be symmetric according to Blom's scheme [3].

STEP 1. Kronecker Product

Let $\mathrm{A} \in \mathbf{R}^{\sqrt{m}\times\sqrt{m}}$ and $\mathrm{G} \in \mathbf{R}^{\sqrt{n}\times\sqrt{n}}$, where A and G are symmetric matrices, the Kronecker product of A and G is given by:

$$A \otimes B = \mathrm{K}$$

Where $\mathrm{K} \in \mathbf{R}^{\sqrt{m}\sqrt{n}\times\sqrt{m\sqrt{n}}}$ is also a symmetric matrix and $K_{i,j} = A_{\left\lceil \frac{i}{\sqrt{n}} \right\rceil, \left\lceil \frac{j}{\sqrt{n}} \right\rceil} \times K_{i\%\sqrt{n}, j\%\sqrt{n}}$.

Example:

Let $A^{4\times4}$ and $G^{4\times4}$ be the two matrices used for this scheme.

$\mathrm{A} = \mathrm{B} \cdot \mathrm{D} = \begin{bmatrix} 5 & 25 \\ 25 & 105 \end{bmatrix}$, $\mathrm{G} = \mathrm{C} \cdot \mathrm{F} = \begin{bmatrix} 292 & 134 \\ 134 & 30 \end{bmatrix}$, then the Kronecker product of matrix A and G is evaluated to K.

$$A \otimes G = \mathrm{K} : \begin{bmatrix} 5 & 25 \\ 25 & 105 \end{bmatrix} \otimes \begin{bmatrix} 292 & 134 \\ 134 & 30 \end{bmatrix}$$

$$= \begin{bmatrix} 5 \times 292 & 5 \times 134 & 25 \times 292 & 25 \times 134 \\ 5 \times 134 & 5 \times 30 & 25 \times 134 & 25 \times 30 \\ 25 \times 292 & 25 \times 134 & 105 \times 292 & 105 \times 134 \\ 25 \times 134 & 25 \times 30 & 105 \times 134 & 105 \times 30 \end{bmatrix}$$

STEP 2. Matrix Decomposition

The symmetric matrices A and G are broken down into multiplication of two other matrices by using matrix decomposition method.

Let A = B · D and G = C · F, where the symbol (·) denotes the normal matrix multiplication.

Example:

$$A \otimes G = \mathrm{B} \cdot \mathrm{D} \otimes \mathrm{C} \cdot \mathrm{F} = \mathrm{K} : \begin{bmatrix} 3 & 4 \\ 11 & 18 \end{bmatrix} \cdot \begin{bmatrix} -1 & 3 \\ 2 & 4 \end{bmatrix} \otimes \begin{bmatrix} 10 & 42 \\ -4 & 25 \end{bmatrix} \cdot \begin{bmatrix} 4 & 5 \\ 6 & 2 \end{bmatrix}$$

$$K = \begin{bmatrix} 5 \times 292 & 5 \times 134 & 25 \times 292 & 25 \times 134 \\ 5 \times 134 & 5 \times 30 & 25 \times 134 & 25 \times 30 \\ 25 \times 292 & 25 \times 134 & 105 \times 292 & 105 \times 134 \\ 25 \times 134 & 25 \times 30 & 105 \times 134 & 105 \times 30 \end{bmatrix}$$

$$K = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cc} 1 & 2 \end{array} \\ \begin{bmatrix} B_{1,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,2} \\ B_{1,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,2} \end{bmatrix} \\ \begin{array}{cc} 3 & 4 \end{array} \\ \begin{bmatrix} B_{1,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,2} \\ B_{1,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,2} \end{bmatrix} \end{array}$$

Where $B_{1,-}$ represents first row of B, and $D_{-,1}$ represents first column of D.

STEP 3. Assign data to sensor nodes

When the Kronecker matrix is generated, the next task is to assign each sensor node in the network with the significant rows from matrix B and matrix C. Matrix D and matrix F are public.

Example:

Node 1 stores $B_{1,-}$and $C_{1,-}$, that is equal to [3 4], [10 42].
Node 2 stores $B_{1,-}$and $C_{2,-}$, that is equal to [3 4], [−4 25].
Node 3 stores $B_{2,-}$and $C_{1,-}$, that is equal to [11 18], [10 42].
Node 4 stores $B_{2,-}$and $C_{2,-}$, that is equal to [11 18], [−4 25].

STEP 4. Sensor node communication

If two nodes N_i and N_j wish to connect and exchange data, they first need to calculate the according index number of the column from matrix D and matrix F.

N_i Computes the indexes $\lceil j/\sqrt{n} \rceil$ and j$\%\sqrt{n}$, and N_j computes the indexes $\lceil i/\sqrt{n} \rceil$ and i$\%\sqrt{n}$.

After computing the indexes,

N_i Computes $B_{\lceil i/\sqrt{n} \rceil,-} \cdot D_{-,\lceil j/\sqrt{n} \rceil} \times C_{\mathrm{i}\%\sqrt{n},-} \cdot F_{\mathrm{j}\%\sqrt{n}}$ and

N_j Computes $B_{\lceil j/\sqrt{n} \rceil,-} \cdot D_{-,\lceil i/\sqrt{n} \rceil} \times C_{\mathrm{j}\%\sqrt{n},-} \cdot F_{\mathrm{i}\%\sqrt{n}}$.

N_i and N_j must get the similar result for the computation since matrix K is symmetric. The resultant becomes the secret key between N_i and N_j. This way no extra information is required to compute the common key.

Example:

Let node 1 and node 3 wish to communicate, they just need to compute the indexes number of the column vectors for matrix D and F and after than find the value of N_1 and N_3.

Node 1 will compute indexes numbers $\lceil j/\sqrt{n} \rceil$ and j%$\sqrt{n}$, which is, $\lceil 3/\sqrt{4} \rceil = 2$ and $3\%\sqrt{4} = 1$.

Node 3 will compute indexes numbers $\lceil i/\sqrt{n} \rceil$ and i%$\sqrt{n}$, which is, $\lceil 1/\sqrt{4} \rceil = 1$ and $1\%\sqrt{4} = 1$.

N_1 Calculates $B_{1,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,1} = [3\,4] \cdot \begin{bmatrix} 3 \\ 4 \end{bmatrix} \times [10\,42] \cdot \begin{bmatrix} 4 \\ 6 \end{bmatrix} = 25 \times 292 = 7300.$

N_3 Calculates $B_{2,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,1} = [11\,18] \cdot \begin{bmatrix} -1 \\ 2 \end{bmatrix} \times [10\,42] \cdot \begin{bmatrix} 4 \\ 6 \end{bmatrix} = 25 \times 292 = 7300.$

After the evaluation, node 1 and 3 will evaluate the common key, i.e 7300. Hence, each pair of sensor nodes in the network will have a uniquely shared key.

4.2.2 Performance Metrics

a. *Computation cost*: considering the cost of multiplications used to generate the key, to analyse the computation cost.
   The number of multiplications used to compute the key between node I and node j, depends on the size of matrix B and C.
   The computation cost turns out to be $O(\sqrt{N})$, where N is the total number of nodes in the network.
b. *Storage cost*: It directly depends on the size of matrices B and C.
   The storage cost also turns out to be $O(\sqrt{N})$.

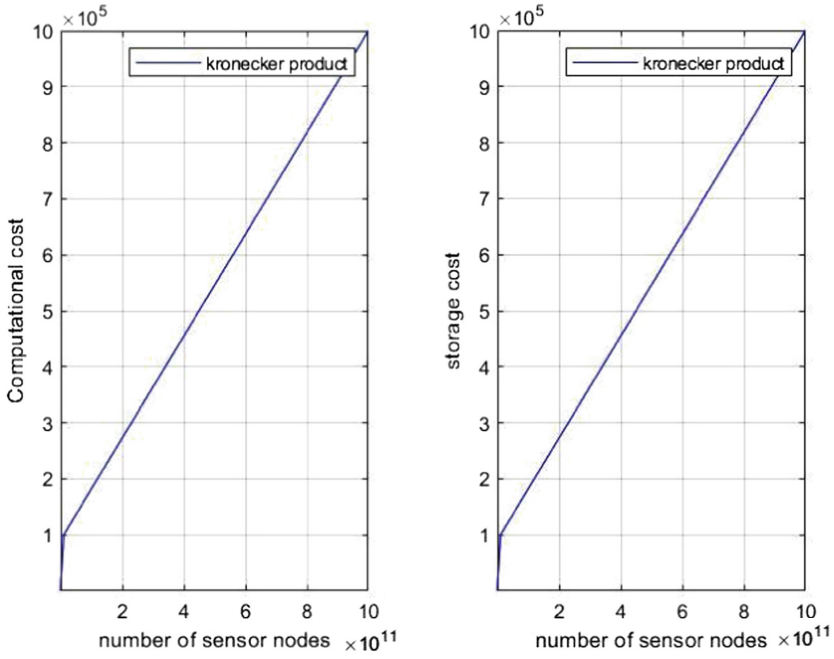


Fig. 2. Analysis of communication overhead and storage overhead of Kronecker Product based KMS with number of sensor nodes

Figure 2 depicts the variation in communication overhead of Kronecker Product based KMS with number of sensor nodes. It is observed that it also increases with the number of nodes. It is due to the communication cost of setting a pairwise key increases in a network.

4.3 CARPY Scheme

The Blom's scheme is extended by adding a random noise to the matrix such that the corresponding keys are not symmetric in nature and thus adding a security feature to it. In Blom's scheme, communications become insecure after more than λ sensor nodes are compromised. The reason for this is that the row vector Ai, in the sensor node i is directly related to the private matrix D. Hence, after collecting a sufficient number of row vectors of A, the adversary is able to construct the private matrix D by solving a system of linear equations since G is publicly known.

$$\begin{matrix} & \text{W} & & & & \text{G} & & & & \text{K} \\ \begin{bmatrix} \mathbf{35} & \mathbf{41} & \mathbf{41} & \mathbf{37} \\ 21 & 27 & 25 & 19 \\ \mathbf{17} & \mathbf{17} & \mathbf{15} & \mathbf{13} \\ 19 & 20 & 19 & 16 \end{bmatrix} & \cdot & \begin{bmatrix} 4 & 1 & 1 & 2 \\ 4 & 2 & 1 & 1 \\ 2 & 4 & 1 & 1 \\ 4 & 1 & 3 & 3 \end{bmatrix} & = & \begin{bmatrix} & & & 228 \\ & & & \\ 218 & & & \end{bmatrix} \end{matrix}$$

$$W_{1,-} = [35\ 41\ 41\ 37] = A_{1,-} + \phi_{1=[34\ 40\ 42\ 36]} + [1\ 1\ -1\ 1]$$

$$W_{3,-} = [17\ 17\ 15\ 13] = A_{3,-} + \phi_{3=[18\ 18\ 16\ 12]} + [-1\ -1\ -1\ 1]$$

4.4 Matrix Based Key Management Scheme by Nafi, Samia and Omar

4.4.1 Introduction

A lightweight key management scheme is proposed by the authors for securing IoT network. The scheme is matrix-based and the motive of this scheme is to make it more flexible than previously defined schemes, more scalable, resilient to several types of attacks and to limit the amount of information needed to be shared and processed at constraint nodes. Few contributions of this schemes are as follows:

i. The number of keys that are needed to store in a very constrain node's memory is extremely limited, as a node is allowed to store only the pairwise keys of the neighbours which are at 1-hop distance, along with the group key.
ii. It provides a negligible communication burden, since the keys are accomplished in a very shared manner.
iii. It offers less computation overhead since no advanced operation is needed to create the secret keys.
iv. It is flexible as new devices can easily be added to the network even after the deployment of sensor nodes.
v. Security goals are guaranteed, which includes integrity, secrecy and authentication.
vi. It is resistant to various security attacks like eavesdropping, compromising of nodes, forward and backward attacks along with replay attacks.

4.4.2 Overview of Proposed Scheme

The Nafi et al. key management scheme, that is based on matrix aims to reduce the computation cost, communication cost and storage overhead. The network architecture assumed to consist three main network components: constrained nodes, gateway nodes and remote server nodes which are also called as command nodes.

4.4.2.1 Constrained Nodes

These nodes are very constrained in resources such as memory, energy and computation power. These nodes can be carried by the humans and the role of these nodes/devices is to monitor and sense the environment to gather the data and transmit it to gateway nodes via Bluetooth or Wi-Fi networks. These nodes include sensors, RFID tags, and wearable devices such as watches.

In healthcare environment, the sensors could be planted inside a human body with a task to collect health related issues like blood pressure, body temperature, glucose level, etc.

4.4.2.2 Gateway Nodes

These are the nodes, which have somewhat higher energy resources and consists of high performance processors and a larger memory than constrained nodes, but the memory is less compared to next level remote server nodes. These nodes process and sends the data collected by constrained nodes to the remote server node. This communication between the next level remote sensor nodes and gateway nodes is done through mobile communication (3G or 4G) or Wi-Fi technologies.

4.4.2.3 Remote Sensor Nodes (Command Nodes)

These nodes are assumed to have very high power, high computation rate and sufficiently large storage than the constrained nodes and Gateway nodes.

4.4.3 Notations Used in the Scheme

The notations and their symbolic meaning is given in Table 1.

Table 1. Notation used in Nafi, Samia and Omar scheme

Notation	Description
Idi	Unique ID number given to node Ni
M	n × n Square matrix, where n is the number of nodes in the network
Mi	node Ni matrix
Vi	Neighbour vector of node Ni
a ‖ b	Information a is concatenated with b's one
Hash (Msg, k)	1-way hash function
|x|	x's absolute value
Det(M)	Determinant of matrix M

4.4.4 Phases of Scheme

The Nafi et al. scheme works in six phases:

(a) Initialization Phase
(b) Pairwise Key Establishment Phase
(c) Group Key Establishment Phase
(d) New Node Addition Phase
(e) Key Revocation Phase
(f) Key Refresh Phase

4.4.4.1 Initialization Phase

During the initialization phase, the nodes are pre-loaded with the following information:

1. A unique identification number Idi.
2. A square matrix M of order n, where n is the number of nodes present in the network. The elements in the matrix is generated randomly and are positive integers.
3. A one-way Hash (msg, k) function, which takes *msg* and *k*, as an input where k is the secret key.

Given the Hash() function and the matrix M, each node Ni is capable of computing a symmetric key Kij which is shared with its 1-hop neighbour Nj.

4.4.4.2 Pairwise Key Establishment Phase

It consists of two parts. Neighbour discovery phase and Pairwise key computation phase. In neighbour detection phase, each node Ni discovers neighbours, which are at 1-hop distance and adds them in their respective direct neighbours' vector. After this stage, each node Ni has its neighbours' vector updated and the neighbours are sorted in ascending order. In pairwise key computation phase, every node calculates its square matrix Mi, along with a secret key value Sij, that is the absolute value of the determinant.

$$\mathrm{Sij} = |\det(\mathrm{Mij})|$$

4.4.4.3 Group Key Establishment Phase

When nodes try to send or broadcast a same set of data to multiple nodes in a very secure manner, it is necessary to use one common key, called as group key. The group communication improves the performance and efficiency of the network. All the nodes in the group share and use the common secret key so as to secure the communications within the group. The common group keys are created and shared by gateway nodes as the resources are more than the constrain nodes.

4.4.4.4 New Node Addition Phase

When a new node Nn tries to enter the network, the gateway node closer to this new node will randomly generate a secret value Si and forwards it to its neighbouring nodes. Each node that receives the broadcast message, saves the secret value and transmit to its 1-hop neighbouring nodes. At the end of this repeated process, all the nodes will have this new value.

4.4.4.5 Key Revocation Phase

A node may be removed from the network in two cases. Case 1: The node is kicked out of the network after it is reported to be compromised by the attacker or Case 2: The node leaves with its own will.

In case 1, if a gateway node detects any suspicious behaviour from any of its neighbouring node, it performs the following task:

i. Remove the compromised node from its memory and the pairwise key which is shared between them.
ii. Modify its n × n matrix by removing the row and column corresponding to the compromised node.
iii. Modify its neighbour vector by deleting the id of that node.
iv. Informs the close nodes by forwarding them an encrypted message.

In case 2, the node that willingly leaves the network, forwards a Leave message to its 1-hop neighbours. A node that receives this Leave message responds with an acknowledge message Ack and performs i, ii and iii operation stated in case 1.

4.4.4.6 Key Refresh Phase

When the same set of keys are used for a longer period in the network, the adversary could get control over these keys by using network analysis, hence new keys are required. Key refresh improve the security of the network as new set of keys will be completely different from the previous keys, which will make the cryptanalytic attack difficult. Therefore, all the keys need to be updated periodically. The gateway nodes update these keys when the old keys expiration time is reached.

4.4.5 Security Analysis

The scheme provides the following properties:

i. *Extensibility*: Since the scheme allows the new nodes to be added even after deployment phase which is achieved by using the node addition phase, the scheme allows flexibility and dynamism.
ii. *Scalability*: Every node saves one group key per network and only the pairwise keys of the neighbours, the sensors are assigned with a small number of keys to save the memory. Hence the number of keys stored in a node's memory does not increase linearly or exponentially even after adding several new nodes.
iii. *Resilience*: The compromise of one node has a very little consequence on the entire system. An adversary who compromises a node will have control over to the keys that are stored in its memory, hence it will have a very little influence on the system.

5 Comparison of Matrix Based Key Management Protocols

The number of multiplications performed to compute the key calculates the computation cost of any scheme. In Kronecker product, the multiplication number depends on the size of matrices B and C with size $\sqrt{M} \times \sqrt{M}$ and $\sqrt{N} \times \sqrt{N}$ respectively. The

total multiplications are $\sqrt{M}+\sqrt{N}$. The analysis is done by assuming the size of matrices B and C to be same, which is equal to $\sqrt{N}$, with N being the number of total nodes in the network. Hence, when the size of both the matrices are assumed to be same, the computation cost is $O(\sqrt{N})$. In Blom's scheme, each node is supposed to store an entire row and an entire column of secret symmetric matrices A and B; hence the storage overhead increases rapidly with the number of nodes. Therefore, in Blom's scheme the computation as well as storage cost grows linearly O(N) with the increase in number of nodes in the network, as for computing the key for a pairwise connection with another node, N number of multiplications are required to be performed, which depends on the entire size of the network. Whereas, in Kronecker product scheme, the storage cost depends on the size of matrices B and C, which again turns out to be $O(\sqrt{N})$ (Table 2).

Table 2. Comparative analysis of different schemes

Performance metric	Blom's scheme	Kronecker product	CARPY	Nafi et al.
Computation cost	O(N)	$O(\sqrt{N})$	–	Constant multiplications
Storage cost	O(N)	$O(\sqrt{N})$	O ($\xi \cdot \lambda$)	d(d + 1)

ξ is the number of rounds performed by CARPY. Let ξ = 64
λ is the security parameter and is independent of N. Let λ = 32
d is the number of neighbours for which a node stores square matrix.

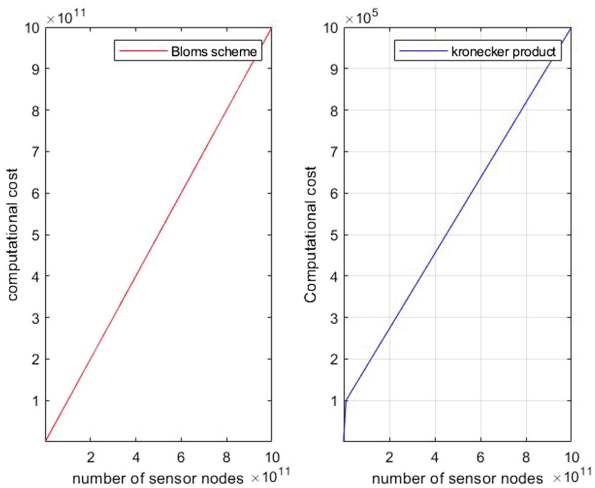


Fig. 3. Analysis of computation cost of Blom scheme with Kronecker Product based KMS with number of sensor nodes

Figure 3 depicts the variation in computation cost of Kronecker Product based KMS with Blom scheme with number of sensor nodes. It is observed that it also increases with the number of nodes in both scheme.

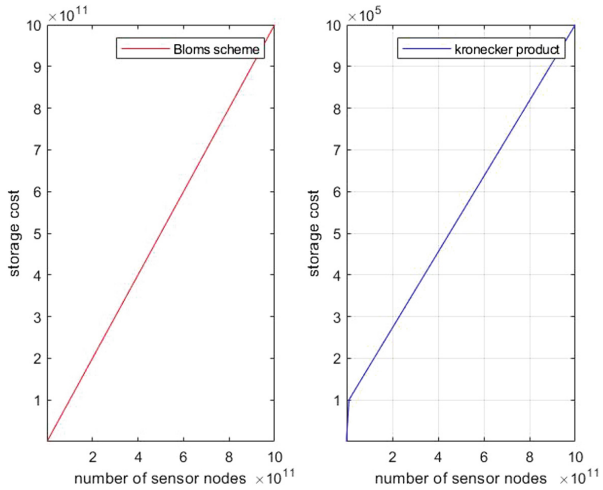


Fig. 4. Analysis of storage cost of Blom scheme with Kronecker Product based KMS with number of sensor nodes

Figure 4 depicts the variation in storage cost of Kronecker Product based KMS with Blom scheme with number of sensor nodes. It is observed that it also increases with the number of nodes in both scheme. It is also observed that Kronecker product based scheme lesser storage overhead as compared to Blom scheme for a given number of node.

6 Conclusion and Future Work

Internet of things is a rapidly growing technology in the area of Wireless sensor network (WSN). Security issues in IoT development has become an important factor as if the security is not fully guaranteed, then sensitive data and secret information of IoT system may be stolen by an adversary. In order to provide security, a key agreement protocol is designed which will help the nodes in IoT to have a secure channel to share information. We have presented practically possible key management schemes like Blom's, Kronecker product scheme, Carpy scheme etc. for the problem of establishing a secure key between the devices. The purpose of this chapter is to explain the basic concept of security in IoT and survey of various key management schemes along with their performance parameters. We evaluate and compared the proposed schemes on storage overhead, communication overhead, computation overhead and resilience against various attacks against node-compromised attacks.

Future work consists of various advancements in the security area like, optimising the computation cost of proposed algorithms, testing the real IoT nodes for the performance of various proposed scheme and developing a lightweight secure key management scheme.

References

1. Padmavathi, G., Shanmugapriya, D.: A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576 (2009)
2. Yu, C.-M., Lu, C.-S., Kuo, S.-Y.: A simple non-interactive pairwise key establishment scheme in sensor networks. In: 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. IEEE (2009)
3. Tsai, I.-C., Yu, C.-M., Yokota, H., Kuo, S.-Y.: Key management in Internet of Things via Kronecker product. In: 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 118–124. IEEE (2017)
4. Whitmore, A., Agarwal, A., Da Xu, L.: The Internet of Things—a survey of topics and trends. Inf. Syst. Front. **17**(2), 261–274 (2015)
5. Zhang, J., Varadharajan, V.: Wireless sensor network key management survey and taxonomy. J. Netw. Comput. Appl. **33**(2), 63–75 (2010)
6. Roman, R., et al.: Key management systems for sensor networks in the context of the Internet of Things. Comput. Electr. Eng. **37**(2), 147–159 (2011)
7. Li, S., Da Xu, L., Zhao, S.: The internet of things: a survey. Inf. Syst. Front. **17**(2), 243–259 (2015)
8. Nafi, M., Bouzefrane, S., Omar, M.: Matrix-based key management scheme for IoT networks. Ad Hoc Netw. **97**, 102003 (2019)
9. Rahman, M., Sampalli, S.: An efficient pairwise and group key management protocol for wireless sensor network. Wirel. Pers. Commun. **84**, 2035–2053 (2015)
10. Blom, R.: An optimal class of symmetric key generation systems. In: Workshop on the Theory and Application of Cryptographic Techniques, pp. 335–338. Springer (1984)
11. Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A.: A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur. (TISSEC) **8**, 228–258 (2005)
12. Yu, Z., Guan, Y.: A key management scheme using deployment knowledge for wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **19**, 1411–1425 (2008)
13. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT (2018)
14. Shukla, A.S., Tripathi, S.: A matrix-based pair-wise key establishment for secure and energy efficient WSN-assisted IoT. Int. J. Inf. Secur. Priv. (IJISP) **13**(3), 91–105 (2019)
15. Akhbarifar, S., et al.: Hybrid key pre-distribution scheme based on symmetric design. Iran. J. Sci. Technol. Trans. A: Sci. **43**, 2399–2406 (2019)

Black Hole Attack and Its Security Measure in Wireless Sensors Networks

Ila Kaushik and Nikhil Sharma(✉)

Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India
ila.kaushik.8.10@gmail.com,
nikhilsharma1694@gmail.com

Abstract. Computers are being reasonably important part of our daily lives. Different solutions were introduced for its connectivity such as wired approach which existed for longer duration of time. But due to advancement in field of technology wireless connectivity came into picture for connectivity to internet, exchanging information etc. One of suited network based on wireless standard is wireless sensor network (WSN). WSN comprises of a number of small motes that are distributed in random manner in any environment. The motes communicate with one another in their resource domain using low power communication medium. WSN possesses many characteristics but difficulty arises in its energy management, security aspect and deployment. Communication take place over radio environment and are prone to various attacks. Some of the attacks include Black hole attack, Gray hole attack, sinkhole attack etc. In this paper we are discussing network layer Black hole attack along with its security measure to decrease its effect in the network.

Keywords: Wireless Sensor Network · Black hole attack · Motes · Security issues

1 Introduction

WSN comprises of self-organizing motes which are distributed in random fashion. The network is set up with small size, low power motes which are connected via single or multiple sinks [1]. Some of the applications include environmental or habitat monitoring, seismic detection, military surveillance, inventory tracking, medical monitoring, smart spaces, process monitoring etc. Sensor network falls under low power and lossy networks (LLNs). These embedded devices can be connected by number of wired links, Bluetooth, IEEE802.15.4, low power Wi-Fi, other low power communication links [2]. Some of the difficulties in the network include limited memory and power battery, processing capability and a restricted field of sensing [3]. Wireless communication network is implemented using radio communication. Different types of wireless network include wireless personal area network (WPAN), wireless local area network (WLAN), wireless ad-hoc network, wireless metropolitan area (WMAN), wireless wide area network (WWAN), cellular network, space network etc. A wireless sensor mote comprises of five major components–sensing unit, battery, transmitter or

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 401–416, 2020.
https://doi.org/10.1007/978-3-030-40305-8_20

receiver, processor. Major factors which are to be taken into consideration while designing a sensor network are power consumption, scalability and fault tolerance. Sensor network is formed by two basic architecture-layered and clustered. Layered architecture uses single base station (BS). Clustered architecture maps sensor motes into clusters. Each cluster has its own cluster head. Motes within each cluster exchange messages within their cluster heads. WSN uses star, tree and mesh topologies [4] (Fig. 1).

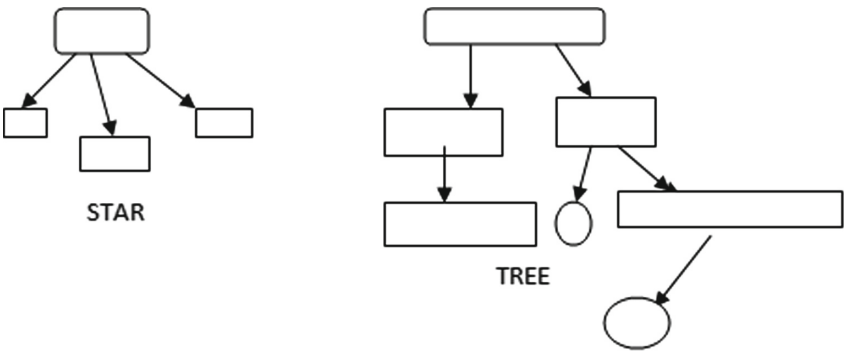


Fig. 1. Star and tree topology

Sensors node used without security measures decreases the quality of services in the network topology. Wireless sensors are linked via radio frequency links. Efficient working of nodes is characterized by compression and equal distribution of information in the network. Data obtained from the nodes in the network must reached the destination safely.

While transferring data, network may be interrupted by a number of attacks. In order to eliminate impact of these attacks in the networks, security principles such as Integrity, Availability, non-repudiation and Confidentiality have been developed. Sensors are devices having tendency to detect and communicate with other nodes.

Broadcast messages are vulnerable to various attacks. In order to have safe transmission between nodes, sensors nodes must be incorporated with authentication mechanism and key management. Wireless sensors nodes are based on the phenomenon of transferring sensors data to the Centre by multi-hop routing. Sink node is the last node that communicates with base stations. The neighboring node is transferred after processing of sensors nodes from sensed data. Then, the data is forwarded to sink node via base station.

To have an efficient functionality of the network, links must be maintained in good condition mainly in safety critical applications. With increase in use of sensor network they are prone to many attacks in order to breach the security of the network. In this paper, we present literature survey of various attacks along with their security mechanism. Simulation is performed on Contiki MAC which is one of the MAC protocols implemented in Contiki Operating System. Variation of power with attack in the

network and with security mechanism has been discussed. In wireless sensors networks there are different types of attacks which affects the normal functioning of the network [5] (Fig. 2).

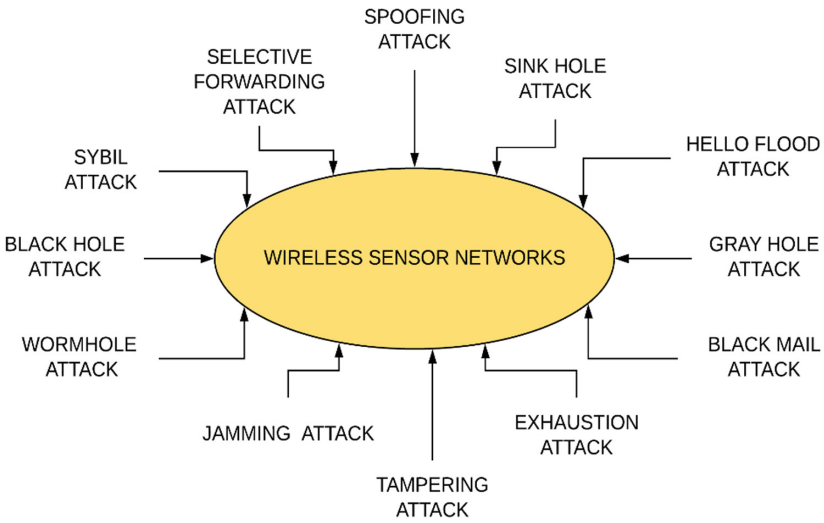


Fig. 2. Various attacks on WSNs

In order to breach the information, Wireless Sensor networks are more prone to attacks. There are various types of attacks such as

- Jamming: Jamming is a type of WSN attack in which by transferring purposeless or impractical information the attacker disturbs the radio channel. This type of attack can be irregular, short-term or permanent.
- Exhaustion: In Exhaustion all the resources energy of the fatality node gets consumed. By doing this the intruder can receive the data, send useless data, and can perform some calculation using actual data.
- Wormhole attack: In Wormhole attack, the intruder is placed at both the network's end. The intruder used to receive the actual information or data and tunnels them to another place and retransfer that data to the network. It is the type of attack which receives messages from neighboring nodes via low latency connection. This type of attack consists of two nodes which want to reduces their distance. Attackers convinces that both the nodes are neighbors. From the two nodes, one node acts as neighbor of base station and another node as neighbor of target node.
- Blackmail attack: In blackmail attack, the true node gets identified as malicious node by the attacker. In WSNs, the true nodes always keep the records of malicious nodes in a blacklist. So, the attacker threatens the true node and ask other nodes to add this node into the blacklist so that it cannot be restricted by that node.

- Tampering: In Tampering, without authorization the intruder accesses the node and extract all the details such as key of the cryptographic material which can be used for ciphering the data.
- Blackhole attack: Blackhole attack is network layer attack in which malicious node drops the pack in the e network. The empty slots being created in the network when the packet is dropped in the network.
- Spoofing: alteration results in the networks when an attacker makes changes in the routing table by entering false values in the routing table and generate false messages in network topology, maximizing delay from one end to another end in the networks to gain felonious benefits.
- Selective forwarding: the type of attack in which malicious nodes drops the incoming packets in the networks. This malicious node also blocks the data flow in the networks.
- Sink Hole Attack: In this type of attack, node that leaks in the network act as a sink hole, that keeps all data packets. It makes malicious node attractive to its neighboring nodes in order to receive data from nearby nodes. It is the type of selective forwarding attack.
- Sybil Attack: this attack contains several Intrusion detection systems. An attacker can be at a number of places at the same time. Impact of sybil attack reduces the effectiveness of fault tolerance systems. As a node is assigned with number of intrusion detection systems, information at different locations can be changed. It reduces effect of authenticity, multipath routing and topology maintenance [6].
- Hello Flood Attack: in this attack, the attackers try to convince that it is a neighboring node. Using high transmission power, information can be transmitted. Many other nodes assume themselves as neighbor and broadcast HELLO message in the network. Other receiving nodes assumes sender node is in their range. The aim of this attack is to slow down the transmission process by sending numbers of Hello message in the network.
- Acknowledgement Spoofed Attack: Another type of attack that tells that a dead node is still alive in the network. This results in capturing packet sent via dead node. Attackers also listens to packets sent in the network and determines which nodes are weakly or deadly connected in network topology [7].

2 Literature Survey

Black hole attack is a kind of attack which operates on network layer of the OSI network model. There are two types of mechanism which work-REQ and REPLY. Whenever a node wants to transmit the data, it sends REQ command in the entire network. Node which wants its data sends a REPLY command in response. On receiving the command, node now sends the data in the network. Neighboring nodes updates their table according to transfer of data packet from source to destination node. The node which has to transmit the data searches shortest path in the entire network and then transfers the data packet along the shortest path. In between the network some malicious nodes are also present which disturbs the functioning of the packet by

dropping packet in between or absorbing packets due to which empty spaces are created in between the network [8].

In Wireless Sensor Network, each layer is prone to various attacks. Blackhole attack is one of the dangerous attacks on the network layer. The microcontrollers play important role as a transducer in WSNs. According to Kaur [9], a bridge is created by the microcontroller in WSNs between initial source node & destination nodes so that, the receiver can receive signal from initial source node & transmitted the message to the destination nodes. Instead of using ethernet sensors networks, the WSNs is widely employed because of its easy installations & the on-demand network features [10]. In runtime process, no human (third party) gets involve in WSNs. Presently, there are various types of attacks in WSN's. Black hole attack is a network layer attack which disturbs the normal functioning of the network. The name Blackhole has been described as vacant space or empty holes are created in the network topology due to packet drop by the compromised node in the network. The malicious node drops the packet in between transmission of packet from one node to another. False entries in the routing table are done by malicious node which results in sending and exchange of false messages in the network. Various security mechanisms are provided to decrease the effect of attack in the network. Some preventive measures can be inbuilt in the network before transmitting the data so that no malicious node can interrupt in the network while transmission. This helps in reducing the effect of attack in the network. Mobile WSN based on ad-hoc network without any base station on communication. In ad-hoc network, at regular interval of time devices may connect or disconnect into the network. Packet loss and efficiency describe about the better communication between networks.

According to Saikia [11], for secure connection between nodes we use cryptographic techniques on it. Due to this technique only particular nodes work on that time or sensor node receive only that message which is send by sink node. Cryptographic techniques called key pre-distribution scheme is used. By that technique of cryptography, resource node is not working on installation. Key pre-distribution works on two schemes:- (a) Location Independent (b) location Dependent. In location independent, all destination nodes are connected to sources node in asynchronous ways while on location dependent, these were connected at regular interval time or simultaneous. Every node set or called by particular key which is used for less data saving on the time of installation. On connectivity time (in between source and destination) on single node connection Pr1 is probability of single node connect at single time which is gives better response as compared to more than one connection. Resilience (fails) is that terms which is used for testing connectivity is better or not between any damaging links. It is the ratio between better connectivity to non-better connectivity of the nodes. If fails = 0 means each node are connected to source node. Every node has unique and single key on pairing and deployment respectively. If Pr1 = 1 on all pairs of nodes then all pairs communicate safe and secure. For perfect resilience and better connectivity Pr1 = 1 on all nodes.

Wazid et al. [12] proposed cluster-based technique for prevention of attack. Coordinator is selected based on efficiency and all nodes in the network are analyzed by the coordinator. Only authenticated packets are being sent and a table is maintained

when packets are received by assigning unique number to all nodes. Nodes which act as a malicious node drop the packet in between the transmission.

Ahmed and Ko [13] used two processes-local decision and global verification neighbors. A node in local decision process identifies malicious node based on behavior of its neighboring nodes. Verification messages are forwarded by an alternate path. This increases data delivery rate and reduces end to end delivery of packets.

Karakehayov [14] proposed a mechanism receive, watch, and redirect (REWARD) which is based on power control performed by a transmitting node to multiple nodes in direction of base station. Black hole node is identified as a node which does not forward packets. Identification of such a node is done by material for intersection of suspicious sets. This scheme is expensive for a network with n black hole nodes.

Yu et al. [15] gives a detailed review of various methodologies for secure routing in trust-based schemes. Less suited in WSN as the complexity is high, which take resources and with complexity of trust-based structure. It also requires diverse roles in order to meet flexibility of trust evaluation approaches.

Casado and Tsigas [16] presented ContikiSec, a configurable secure network layer designed and introduced in Contiki architecture for providing security in three modes-confidentiality, integrity, authentication.

Mathur et al. [17] provides a solution using cryptographic hashing. The nodes collectively pick a cluster head (CH) to transmit data. The nodes CH combines encrypted data and transmits it to nearest access point. Access point using mesh routing, routes the data towards base station. Random numbers generated by Contiki are assigned by base station to access points by routing phase where request and reply packets are reversed. The defense mechanism used provides suitable way to deal with single and multiple attacks in medical sensor networks.

In [18], a light weight one-way cryptographic hash algorithm is proposed as a security mechanism. Short fixed size length of 96 bits are produced by applying low operations like modulus, swap. Light weight proves more efficient in terms of communication, storage, computational overhead and energy than other cryptographic algorithms. It is suitable for energy starved sensor motes and can be used for message authentication to prevent malicious activities in the network.

3 Common Attacks on Various Layers

In WSN, the different types of attacks on various layers are as described below:

- Physical Layer: One of the well-known attacks on physical layer is jamming. Radio frequencies are being used by sensors network where this attack interferes with the frequencies used by the nodes. As energy is the main constraints in this type of network, this attack results in large scale energy consumption by injecting false packets in network topology [19].
- Data Link Layer: in this layer, attackers violate the communications model by sending repeatedly number of packets in order to cause collision in the network. By this, a node can be easily consumed energy of another node [20].

- Network Layer: Network layer attack comprises of blackhole attack in which the intruder sends false data packets in the network or drops the packet in between transmission. When the packets are dropped in between the transmission, vacant space is being created in the network. In order to maintain authenticity and integrity of data, several encryption techniques and hash functions are being used [21].
- Transport Layer: transport layer is vulnerable to common attacks called flooding. In this type of attack, intruder sends many requests to one of the nodes in the network. Receiving number of requests at a same time decreases the resources and efficiency of the node [22] (Tables 1 and 2).

Table 1. Different layers attacks [23, 24]

S. No.	Layers	Attacks
1	Application Layer	Application layer is responsible for application services like http, ftp, smtp etc. For all these services header is added. Some of the attacks of this layer includes-Message Forwarding, Buffer Overflow, Data Aggregation Distortion
2	Network Layer	Network layer is responsible for routing, traffic shaping, fragmentation etc. Some of the attacks of this layer includes-Worm hole Attack, Black hole Attack, Sybil Attack, Byzantine Attack, Packet Replication, Modification, Fabrication
3	MAC Layer	MAC layer is responsible for flow control, error control, access control etc. Some of the attacks of this layer includes-Identity spook, Traffic manipulation
4	Physical Layer	Physical layer is mainly responsible for electrical properties of wire. Some of the attacks of this layer includes-Eavesdropping, Jamming, Device tempering

Table 2. Comparative analysis of security mechanisms [25, 26]

S. No.	Security mechanism	Advantages	Disadvantages
1	Authentication Packet Exchanges	Easy detection and removal of Black hole node	Only cluster-based topology used
2	Trust Based Monitoring	Efficient and Reliable identification of Black hole nodes	Complex Schemes
3	Multi sink nodes	Efficient delivery of data packets in presence of attack	Attack nodes not identified
4	Contiki Sec Layer	Provides all key elements of security-confidentiality, integrity, authentication	High level of energy consumption
5	Cryptographic Hashing	Less Computational Time	Requirement of external batteries to increase lifetime of motes in the network

4 Different Security Mechanism

The two different types of security measures have been discussed below.

A. Security using AES (Advanced Encryption Standard) Encryption Techniques

Wireless sensors networks are rapidly growing networks based on small sixed nodes exchanging large amount of information. Major challenges faced by wireless network is its size, energy, quality of services, battery power, security, etc. Security is the main concern amongst all these parameters. These types of networks are more vulnerable to threats as unguided medium is more prone to attacks [27].

Cryptography is one of the suited security techniques. There are two types of key which can be used in the cryptography algorithm: Public Key and Private key. In private key, same key is used for both encryption and decryption while in public key, two different keys are used for encryption and decryption processes [28] (Fig. 3).

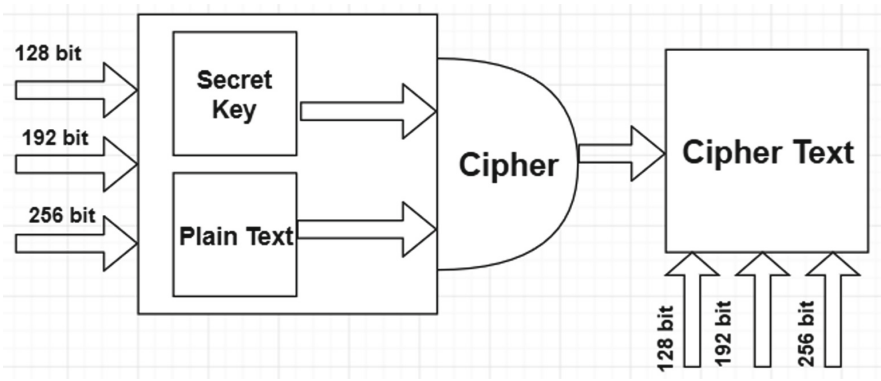


Fig. 3. AES design

AES Encryption techniques operates over 128 bits plain text where initial round key is added to starting state. After initial and final rounds of computations, the final resulting message is in encrypted form. For decryption process, same process is followed in reverse form [29]. On the basis of key size, rounds are being defined. For example, if key size is of 128 bits 10 rounds are being used. For byte-by-byte substitution of blocks, S-Box is being used. After this process, shift rows operations are being performed which shifts one bit. In add round key, key is bitwise XORed to plain text to get new text. This algorithm can further extend to images. For more complex ciphers, ECC algorithms can also be used [30] (Fig. 4).

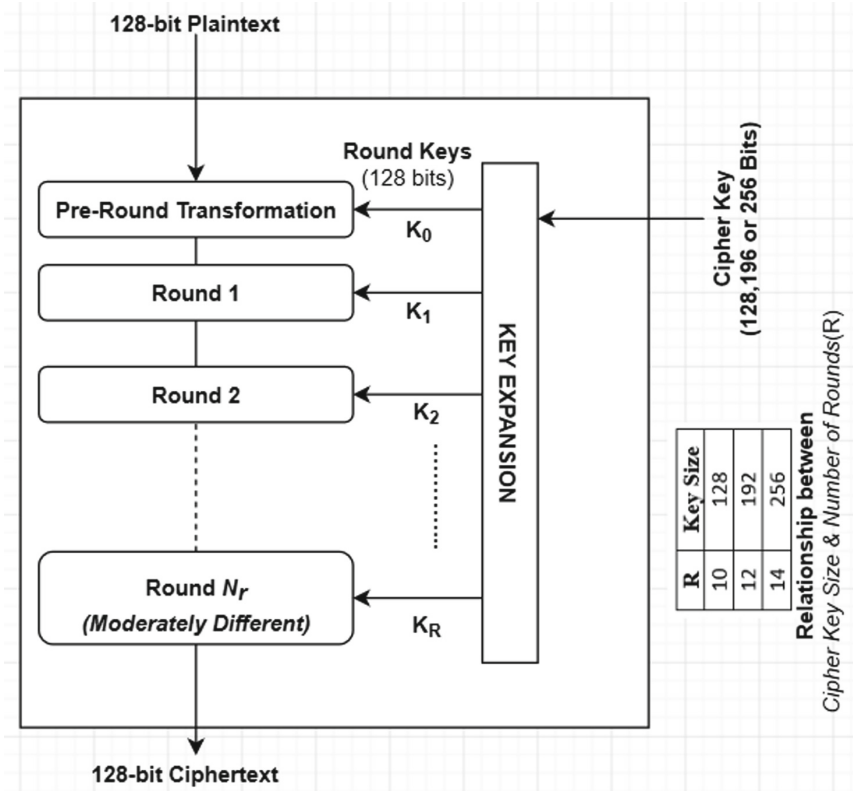


Fig. 4. Depict of AES encryption cipher

There are different Operations in AES. Following transformations are performed during encrypting and decrypting message.

- Substitution: AES performs substitution using only one table. If two bytes are same transformation of bytes is also same in that case. Substitute byte and inverse substitute byte falls under this category. Substitute byte is first step of transformation in encryption process. Input is organized in 4*4 matrix. There are 16 different byte transformation. Inverse substitution byte is used in decryption process and is reverse of substitute byte process.
- Permutation: AES uses byte level permutation. Shift rows and inverse shift rows are used. Shift rows are used in encryption process. Bytes to be shifted depends on row number. Example row 3 is shifted 3 bytes. Inverse shift rows are used in decryption process which is reverse of encryption process [31].

- Mixing: It is an interbyte transformation in which bits inside bytes are changed. Mixing uses matrix multiplication. Mix columns are used in encrypting side. One column of input is transformed into new column. For transforming constant square matrix is used. Square matrix is multiplied by each column resulting in new column value. Inverse mix columns are used in decrypting process which is reverse of encryption process [32].
- Key Adding: It is considered as important transformation as it uses add round key. Add round key uses matrix addition operation. Each column is XORed with key word to produce new column. This process is used for both encryption as well as decryption [33].
- *B. Security of Nodes Joining in & quitting from Wireless sensors networks*

Many protocols focus on energy consumption but security features lack when nodes join in the network [34]. In order to overcome this problem, nodes joining and quitting safely algorithm has been introduced. Whenever a new node wants to join in the network, it sends request and locations to the base station in the network. After receiving the request, it searches its neighbors cluster head node [35].

Cluster head which sends information, must have node I'd and key. After receiving the I'd of the node, it will be marked as join. Both the nodes communicate with one another using key. Cluster head now checks the communication of node. If the communication is abnormal node is removed and feedback is sent to the base station. If the communication is normal, node's information is sent to cluster members and sends feedback to base station to allow the node to join the network.

For node quitting, if the cluster time is greater than or equal to regular interval time, then it will check for cluster transmission anomalies. If there are any anomalies are found, then it will be removing the cluster head and sends the information to base stations. This message is being propagated in the entire network and the node is deleted from entire communication process [36].

5 Implementation

To evaluate the impact of black hole attack in the network, we first studied the network with the attack and then by introducing security parameter. Experiment has been performed on Contiki Operating System which is an open source software developed above Ubuntu as base operating system. It connects tiny low cost, low power controller to the internet [37]. COOJA is a simulation tool provided by Contiki Operating System. It allows simulation of all small and large network motes. Contiki forms a wireless network with help of a routing protocol for low power and lossy network (LLNs). It forms acyclic graph from root node called Destination Oriented Directed Acyclic Graph (DODAG). DODAG Information Object (DIO) messages are broadcasted by all nodes starting from initial node. It comprises of nodes rank, directed acyclic graph version number etc. [38].

Algorithm 1: *Black Hole Attack*

1. Create sensor motes which h are assigned value as $\boldsymbol{M}$.
2. Selection of first mote as $\boldsymbol{M_1}$ assigning rank as 1.
3. Start the process for route establishment
4. First mote transmits multicasts DIO messages
5. if a node doesn't receive DIO after waiting for few seconds {
6. Parent node replies using DIO messages
7. Go to step 10
8. }
9. else {
10. do {
11. Based on objective function value, neighboring motes calculate rank
12. Mote having minimum path value becomes parent mote and transmits the packet Neighbor mote which has minimum path becomes parent node and multicasts message.
13. }
14. Until all motes join DODAG
15. }
16. do {
17. For each leaf mote
18. Send DAO to its parent
19. }
20. Until prefix information reaches $\boldsymbol{M_1}$
21. Traffic Movement
22. {
23. do {
24. if (mote is Black hole)
25. Drop the packet
26. else send the packet
27. }

Algorithm 2: *Key Exchange Algorithm*

1. For any two motes choose any two random numbers.
2. Mote1 performs scalar multiplication and keep it as secret.
3. Similarly, mote2 performs scalar multiplication and keep it as secret.
4. Mote1 computes $(K_a + X).Pub$ and sends it to another mote.
5. Mote2 multiplies it with inverse of private key of it.
6. Packet is sent when keys are valid.

6 Performance Evaluation

Performance of network is studied by introducing the network with malicious mote along with security measure. Power is measured using Contiki Cooja simulation platform. We ran the simulation on network comprising of 50–100 motes. Network was formed on area of $100 \times 100\,m^2$ with simulation time of 10 min. Simulation parameters have been described in the Table 3.

Table 3. Simulation parameters

S.No.	Parameters	Values
1.	Number of Motes	50–100
2.	Simulation Time	10 min
3.	Deployment Area	$100 * 100$
4.	Radio Medium Model	UDGM
5.	Physical Layer	IEEE802.15.4
6.	Routing Layer	Contiki RPL
7.	Transport Layer	UDP
8.	Mote Type	Sky Mote

In this experiment two scenarios were evaluated. In first scenario, power was evaluated with the introduction of attack in the network. In the second scenario, security mechanism was introduced. Power was evaluated for each sensor mote within the specified time interval. Motes consist of Transmission Range (TX), Receiving Range (RX), and sleep mode.

$$\text{Total Energy Consumed} = \sum n \times (c_p + l_p + l_t + l_r) \tag{1}$$

Where,

c_p = CPU energy
l_r = listening energy
l_p = low power mode energy
l_t = transmit energy

Consumption range for each state is described in table.

Table 4 describes the following parameters. Transmission Range is defined as transmission area where the nodes send the packet in the network topology. Receiving Range defines the area where the packet is to be received by the sending node in the transmitting area. CPU energy is defined as the energy consumed by the CPU during transfer of packets in the network. Low energy Power Mode is used in wireless network as energy is one of the major constraints in wireless network and to save power consumption low energy power mode is used.

Table 4. Consumption parameters

S.No.	States	Consumption
1.	Transmission Range (TX)	17.7 mA
2.	Receiving Range (RX)	20 mA
3.	CPU Energy	1.8 mA
4.	Low Power Mode	0.0545 mA

7 Results

Graph has been plotted between number of motes and power consumption of motes with the attack and with security mechanism. Figure 5 shows power variation with the involvement of attack in the network. Figure 6 shows power variation by introducing security parameter in the network. From the graph, it can be inferred that there is a gradual decrease in average power consumption of the network with an increase in number of motes. It is observed that the average power consumption decreases when the proposed security mechanism is employed in the network. It has been observed that by introducing security parameter in the network, there is less wastage of power as compared to when network was exposed to an attack. Power is major issue in sensor network as the motes are restricted by low power batteries. So, our major concern is to save the power of the batteries.

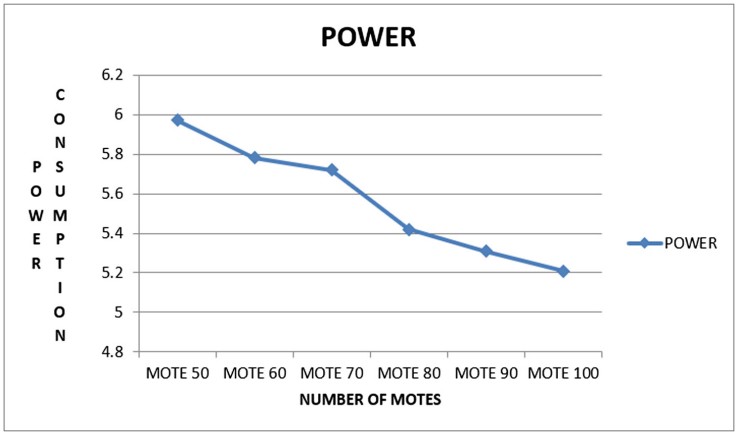


Fig. 5. Power variation with attack in the network

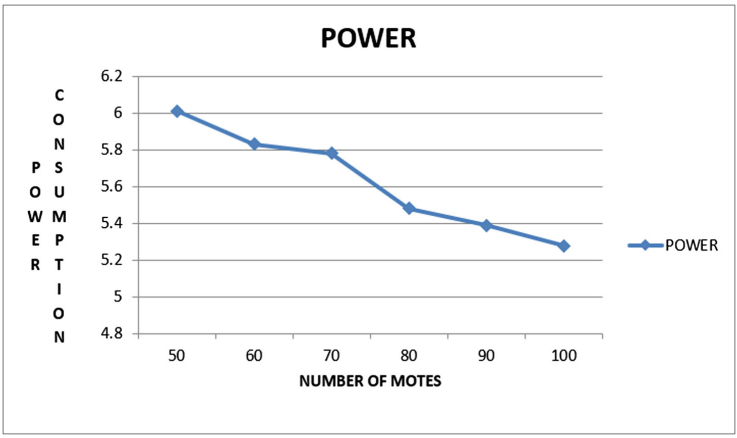


Fig. 6. Power variation with security mechanism in the network

8 Conclusions

In this paper, we discussed importance of Wireless Sensor Networks. These networks are becoming popular because of autonomous nature, self-organization of motes, ease of mobility etc. It follows layered architecture where brief introduction of various types of attacks resulting at different layers has been discussed. Power evaluation of Black hole attack along with its security mechanism has been discussed. Simulation has been performed on Contiki and variation of results has been addressed. Simulation has been performed on Contiki and variation of results has been addressed. It has been observed that with introduction of security mechanism in the network, it results in low power consumption by the motes. Our main focus is to decrease the wastage of power as the motes are powered by low energy resources. Further the work can be extended by measuring the energy using different security measures, its impact on the network with minimum wastage of energy resources as energy is the main constraint in wireless network.

References

1. Akyildiz, I.F., et al.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. Algora, C.M., Reguera, V.A., Fernandez, E.M., Steenhaut, K.: Parallel rendezvous-based association for IEEE 802.15.4 TSCH networks. IEEE Sensors J. **18**(21), 9005–9020 (2018). https://doi.org/10.1109/jsen.2018.2868410
3. Bhushan, B., Sahoo, G., Rai, A.K.: Man-in-the-middle attack in wireless and computer networking—a review. In: 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall) (2017). https://doi.org/10.1109/icaccaf.2017.8344724

4. Khan, M., Misic, J.: Security in IEEE 802.15.4 cluster-based networks. Security in Wireless Mesh Networks, vol. 6 (2008)
5. Kumar, A., Prashar, D.: A novel approach for node localization in wireless sensor networks. In: Intelligent Communication, Control and Devices, pp. 419–428. Springer, Singapore (2018)
6. Bhushan, B., Sahoo, G.: Routing protocols in wireless sensor networks. In: Computational Intelligence in Sensor Networks Studies in Computational Intelligence, pp. 215–248 (2018). https://doi.org/10.1007/978-3-662-57277-1_10
7. Elmahdi, E., Yoo, S., Sharshembiev, K.: Securing data forwarding against blackhole attacks in mobile ad hoc networks. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (2018). https://doi.org/10.1109/ccwc.2018.8301683
8. Mishra, B.K., Nikam, M.C., Lakkadwala, P.: Security against black hole attack in wireless sensor network-a review. In: 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT). IEEE (2014)
9. Kaur, H., Singh, A.: Identification and mitigation of black hole attack in wireless sensor networks. In: 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE). IEEE (2016)
10. Prashar, D., Jyoti, K., Kumar, D.: Design and analysis of distance error correction–based localization algorithm for wireless sensor networks. Trans. Emerg. Telecommun. Technol. **29**, e3547 (2018)
11. Saikia, M., Hussain, Md.A.: Improving the performance of key pre-distribution scheme in sensor network using clustering of combinatorics. In: 2016 International Conference on Computing, Communication and Automation (ICCCA). IEEE (2016)
12. Wazid, M., et al.: Detection and prevention mechanism for blackhole attack in wireless sensor network. In: 2013 International Conference on Communications and Signal Processing (ICCSP). IEEE (2013)
13. Ahmed, F., Ko, Y.: Mitigation of black hole attacks in routing protocol for low power and lossy networks. Secur. Commun. Netw. **9**(18), 5143–5154 (2016)
14. Karakehayov, Z.: Using REWARD to detect team black-hole attacks in wireless sensor networks. In: Workshop on Real-World Wireless Sensor Networks, pp. 20–21 (2005)
15. Yu, Y., et al.: Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. J. Netw. Comput. Appl. **35**(3), 867–880 (2012)
16. Casado, L., Tsigas, P.: Contikisec: a secure network layer for wireless sensor networks under the contiki operating system. In: Identity and Privacy in the Internet Age, pp. 133–147 (2009)
17. Mathur, A., Newe, T., Rao, M.: Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. Sensors **16**(1), 118 (2016)
18. Chowdhury, A.R., Chatterjee, T., DasBit, S.: LOCHA: a light-weight one-way cryptographic hash algorithm for wireless sensor network. Procedia Comput. Sci. **32**, 497–504 (2014)
19. Jaitly, S., Malhotra, H., Bhushan, B.: Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: a survey. In: 2017 International Conference on Computer, Communications and Electronics (Comptelix) (2017). https://doi.org/10.1109/comptelix.2017.8004033
20. Bhushan, B., Sahoo, G.: Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wirel. Pers. Commun. **98**(2), 2037–2077 (2017). https://doi.org/10.1007/s11277-017-4962-0
21. Sinha, P., Jha, V.K., Rai, A.K., Bhushan, B.: Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey. In: 2017 International Conference on Signal Processing and Communication (ICSPC) (2017). https://doi.org/10.1109/cspc.2017.8305855

22. Bhushan, B., Sahoo, G.: A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. In: 2017 International Conference on Signal Processing and Communication (ICSPC) (2017). https://doi.org/10.1109/cspc.2017.8305856
23. Kumar, A., Matam, R., Shukla, S.: Impact of packet dropping attacks on RPL. In: 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC) (2016). https://doi.org/10.1109/pdgc.2016.7913211
24. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies, FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
25. Goyal, S., Chand, T.: Improved trickle algorithm for routing protocol for low power and lossy networks. IEEE Sens. J. **18**(5), 2178–2183 (2018). https://doi.org/10.1109/jsen.2017.2787584
26. Li, G., Yan, Z., Fu, Y.: A study and simulation research of blackhole attack on mobile adhoc network. In: 2018 IEEE Conference on Communications and Network Security (CNS) (2018). https://doi.org/10.1109/cns.2018.8433148
27. Panda, M.: Data security in wireless sensor networks via AES algorithm. In: 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO) (2015). https://doi.org/10.1109/isco.2015.7282377
28. Shreenath, K.N., Manasa, V.M.: Black hole attack detection in zone based WSN. Int. J. Recent. Innov. Trends Comput. Commun. **5**(4), 148–151 (2017)
29. Kaurav, A., Kumar, K.A.: Detection and prevention of black hole attack in wireless sensor network using Ns-2.35 simulator. IJSR CSEIT **2**(3), 717–722 (2017)
30. Gupta, P.K., Madhu, M.: Improving security and detecting black hole attack in wireless sensing networks. Int. J. Prof. Eng. Stud. **VIII**(5), 260–265 (2017)
31. Liu, Y., Dong, M., Ota, K., Liu, A.: ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **11**(9), 2013–2027 (2016)
32. Alajmi, N.M., Elleithy, K.: A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks. In: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, pp. 1–6 (2016)
33. John, C., Wahi, C.: Security analysis of routing protocols for wireless sensor networks. Int. J. Appl. Eng. Res. **11**(6), 4235–4242 (2016)
34. Hu, X., Zhang, Y.: Research on security mechanism of nodes joining in and quitting from WSN. In: 2011 Third Pacific-Asia Conference on Circuits, Communications and System (PACCS) (2011). https://doi.org/10.1109/paccs.2011.5990233
35. Alrajei, N., Fu, H., Zhu, Y.: Information theory based intrusion detection in wireless sensor networks. J. Commun. Technol. Electron. Comput. Sci. **5**, 11–21 (2016)
36. Chaubey, N., Aggarwal, A., Gandhi, S., Jani, K.A.: Performance analysis of TSDRP and AODV routing protocol under black hole attacks in MANETs by varying network size. In: 2015 Fifth International Conference on Advanced Computing & Communication Technologies, pp. 320–324, 21–22 February 2015
37. Cai, J., Yi, P., Chen, J., Wang, Z., Liu, N.: An adaptive approach to detecting black and gray hole attacks in ad hoc network. In: 4th IEEE International Conference on Advanced Information networking and Applications. IEEE Computer Society, pp. 775–780 (2010)
38. Jhaveri, R.H., Patel, S.J., Jinwala, D.: A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. In: Second International Conference on Advanced Computing and Communication Technologies, pp. 556– 560. IEEE Computer Society (2012)

Detection and Tracking of Mobile Intruder in Harsh Geographical Terrains Using Surveillance Wireless Sensor Networks

Anamika Sharma(✉) and Siddhartha Chauhan

Computer Science and Engineering Department,
National Institute of Technology Hamirpur,
Hamirpur 177005, Himachal Pradesh, India
anamika@nith.ac.in

Abstract. The physical threat is a critical issue for the security of the sensitive regions. The sensitive regions are very much prone to unauthorized access. Likewise, the border area of a country is the sensitive region because it is the place where most of the intrusion has been taking place. Most of the border areas comprise harsh geographical terrains. The human-being cannot surveil such terrains. Therefore, the characteristics of a sensor node such as miniaturization, low-cost, ease of deployment, self-configuration, and stealthiness in harsh environmental conditions make them eligible to surveil harsh border terrains. A set of sensor nodes with sensing, coordination and communication capability, form a wireless sensor network (WSN). The prime challenge for deployed WSN is to detect and track the intruder with maximum detection probability and minimum false alarm-rate. The reliable and in-time transmission of detection and tracking results to the base-station is another issue for intruder detection and tracking application. Along with this, random deployment, coverage, network lifetime, energy conservation and network partitioning are other challenges that disrupt the performance of WSN. This chapter presents various intruder detection and tracking attributes and protocols for mobile intruder detection and tracking application. This chapter also presents the various challenges that emerge for WSNs in intruder detection and tracking application.

Keywords: Coverage · Mobile intruder · Node activity scheduling · Detection probability · Tracking

1 Introduction

Mobile intruder detection and tracking (IDT) is one of the crucial applications of wireless sensor networks [1–3]. It is very advantageous in military applications [2, 3]. An intruder can also be synonym as target, object or event in many research articles on IDT applications. Intruder detection is defined as identifying and detect the mobile intruder once it starts intruding on the sensitive region. After intrusion, the mobile intruder starts traversing the region and forms a random trajectory. Intruder tracking is defined as to locate the mobile intruder at various points inside the sensitive region. The prime objective of WSNs for this application is to detect and track the mobile intruder

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 417–437, 2020.
https://doi.org/10.1007/978-3-030-40305-8_21

with maximum detection probability (high precision) and minimum average detection delay. The mobile intruder detection and tracking depend upon sensor node's coverage and connectivity model [4], collaborative sensing and information fusion for intruder detection [5, 6] and intruder tracking [7, 8]. Figure 1 shows the flow chart for the designing of the IDT application protocol. IDT application emphasizes on intruder detection and intruder tracking. The decision or inference about the intruder detection is made with the help of statistical detection theory and track results are generated with the help of estimation theory.

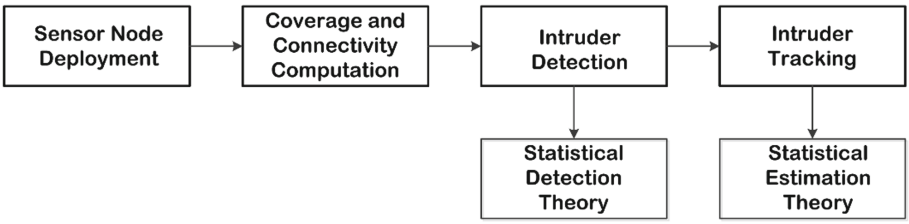


Fig. 1. Intruder detection and tracking protocol

1.1 Mobile Intruder Detection

An intruder is called a passive or non-cooperative intruder and the signals generated by such intruder are known as passive signals. An intruder is detected when the sensor nodes sense some malicious signals [5, 9]. These malicious signals can be radio, seismic or acoustic signals. Based on the received signals at k (where, $k \geq 1$) sensor nodes, a decision is made about the presence of the intruder. The final decision is made by the fusion center where the detection information from k sensor nodes is fused to generate the valuable results. This process is known as information fusion in WSNs. In WSNs, either sink node or cluster head acts as a fusion center. Figure 2 represents the flowchart for intruder detection and tracking application.

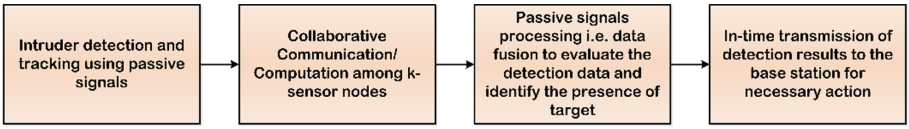


Fig. 2. Structural outline of intruder detection algorithm

For an intrusion detection scenario, a proper trade-off between accuracy, energy efficiency and latency are required. As soon as, event is detected in particular sub-region, base station is notified about the existence of intruder through sensor nodes. The sensor nodes store this information in its local memory. The base station broadcast queries into the network, to know about the existence and current position of the intruder. The discrete nature or irregularity in the existence of event makes query-based

protocol highly advantageous in intrusion detection system as compare to the continuous data delivery protocols [10].

The pictorial representation of Fig. 2 is shown in Fig. 3. The N number of sensor nodes having index S_i (i = 1, 2, 3,……,N) are deployed over sensitive region of area A_s. Generally, the border area of any country is of very large area. It becomes complex to handle the intruder detection and tracking computations. Therefore, the sensing region is subdivided into grids to get maximum detection probability and minimum false alarm rate. Each sensor node can be aware of its location inside sensitive region using predefined localization algorithm [11–13]. Sensor nodes detect an intruder on the basis of received signal strength (RSS) of passive signals. Intruder may enter inside the sensitive region from any grid and the existence of intruder is discrete. An intruder is considered as detected if the malicious passive signals are received by at least k ($k \geq 1$) sensor nodes. The RSS of these signals must be greater than the predefined threshold value. These nodes send the information about the existence of intruder to the fusion center (FC). The fusion centers are more powerful as compare to the deployed sensor nodes in terms of battery, computation and transceiver power. The information comprises all signal measurement values. Fusion center computes the location of intruder and transmits reliable detection information to the base station through wireless communication links. The base station estimates the intruder trajectory on the basis of received measurements. Intruder trajectory is the next plausible random locations which intruder might traverse or visit.

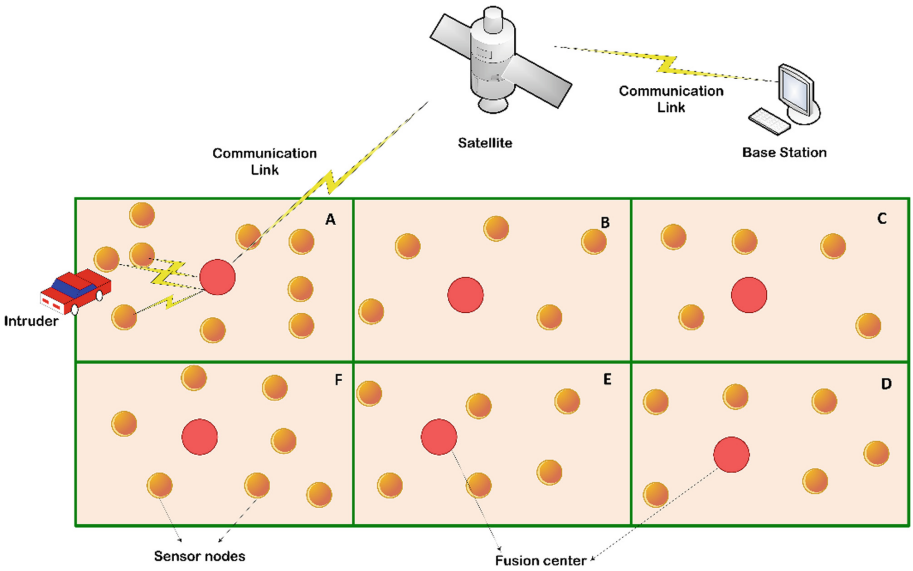


Fig. 3. The pictorial representation of intruder detection and its detection data fusion

1.2 Mobile Intruder Tracking

Mobile intruder tracking is an emerging research area and a distributed tracking algorithm. This algorithm develops accurate path trajectory of an intruder. While performing tracking, nodes works in collaborative manner. In existing research, there are several intruder tracking algorithms based upon either prediction [7] or state estimation approach [8]. These algorithms follow tree, face tracks or cluster network structure [14]. The prediction algorithm predicts next appropriate position of intruder, in accordance to the information extracted from current position. But it suffers from track lost problem and tracking algorithms are vulnerable to loss of tracks due to coverage holes. Occlusion effect, scarcity of sensor nodes, localization error or energy constraints are the main cause of coverage hole and it affects the performance of tracking algorithm. So, estimation algorithm is the best technique to build a track path for such kind of problems. This algorithm generates most optimum set of points, according to the current variables of mobile intruder at any particular time period 't'. For mobile intruder position, velocity, time, acceleration and direction are the current variables. The generated points are the next possible positions of mobile intruder.

Though the results are noisy and there is uncertain set of information as compare to prediction algorithm, but it gives a clear view of next possible positions. Kalman filter [15] also known as linear filter for dynamic system is a technique to overcome this drawback. Kalman filter is used to compute the track path by incorporating external influence like harsh region and uncertainty like acceleration. The performance of tracking algorithm, using filters relies on the accuracy of estimated values.

2 WSN Parameters for Intruder Detection and Tracking

The design of intruder detection and tracking algorithm incorporates the various parameters of WSN. This section has discussed the prime parameters of WSN along with their constraints for intruder detection and tracking application.

2.1 Number of Sensor Nodes

It is defined as the optimum number of sensor nodes require to cover a geographical region. The metrics that are relevant for deriving the optimum number of sensor nodes are sensor node density, a total area of sensitive region A_s and their distribution type. The required number of sensor nodes per unit area is known as sensor node density. Sensor node density provides an insight into the required optimum number of sensor nodes. Wang [4] has computed the node densities for three different tessellations i.e. triangle, square, and hexagon. According to his computation, the hexagon tessellation requires a maximum number of sensor nodes as compared to triangle and square. In harsh geographical regions, the maximum number of sensor nodes are the optimum sensor nodes because of the random deployment and the deployment area have a rough surface. These constraints lead to an asymmetrical density of sensor nodes. According

to Wang [4], the sensor node density and optimum number of sensor nodes N_{opt} for hexagonal tessellation is computed as:

$$\delta = \left(\frac{4\sqrt{3}}{9R_s^2}\right) \tag{1}$$

$$N_{opt} \geq (\text{ceil}(\delta A_s)) \tag{2}$$

where, R_s is the sensing range of the sensor nodes. The distribution of these N_{opt} sensor nodes is modeled by using the distributions of probability theory such as Poisson distribution or Normal distribution. Abdollahzadeh et al. [16] have presented a comprehensive review on the deployment strategies of WSN. The authors have reviewed various deployment optimization algorithms of sensor nodes in terms of coverage and connectivity maximization, energy efficiency and network lifetime optimization. Sharma et al. [17] have reviewed various deployment strategies to provide blanket coverage to large scale area. The authors have presented the concise review of random deployment algorithms for both static and mobile sensor nodes.

2.2 Coverage Model

The network designer of WSN consider any one of the coverage models to acquire the intruder detection results. These coverage models are: (1) Binary coverage model, (2) Exponential coverage model [18] and (3) Probabilistic coverage model [19, 20]. The binary coverage model produces the detection results in the form of binary values i.e. 0 or 1. The binary value 1 depicts the existence and successful detection of a mobile intruder, whereas, 0 depicts no detection of the intruder inside the sensing range of a sensor node. In this model, the sensing area of a sensor node is considered as a circle as shown in Fig. 3. The detection decision is made on the basis of binary results from k sensor nodes. If the maximum number of results from k sensor node is 1 then intruder detection is inferenced else, there is no existence of the intruder. It can be represented as:

$$I_D = \max(\text{Number of 0s}, \text{Number of 1s}) \tag{3}$$

The passive signals always attenuated with respect to the distance between the sensor node and intruder. Therefore, exponential coverage model is used to model the signal attenuation. According to this model, the received signal strength is considered up to the threshold value τ. Beyond that value an intruder is considered as not detected. It can be represented as:

$$I_D = e^{-\gamma y} \geq \tau \tag{4}$$

where, y is the estimated distance between the sensor node and source of the signal and γ is the decay parameter. The sensitive region is the rough surface and comprises obstacles inside the region. It causes irregularity in the sensing range of a sensor node and also creates coverage hole inside the sensing region [21] and coverage area

overlapping [22]. The intruder detection results are imprecise without considering these irregularities. Therefore, the probabilistic coverage model is applied to incorporate all of these irregularities. Along with this, the probabilistic coverage model also incorporates attenuation in received signals.

2.3 Network Connectivity

The network connectivity is also defined as broadcast reachability. In IDT, the successful transmission of detection result to the fusion center is of prime importance. For successful transmission there must be at least m ($m \geq 1$) communication links between the sensor nodes and fusion center. The communication range R_c must be twice to that of the sensing range for complete network connectivity ($R_c = 2*R_s$) [23, 24]. This analysis holds good for uniform deployment of sensor nodes and if there are no obstacles presents inside the sensing range. Most of the research work done on intruder detection and tracking have applied this analysis for network connectivity [24–26]. For complete network connectivity or broadcast reachability for harsh geographical regions an optimum or close to optimum solution is required. Along with this the solution must also incorporate network partitioning constraint. Network partitioning occurs either due to the sparse deployment, node failure or obstacle inside the sensing region.

2.4 Energy Expenditure Model

The energy used by a sensor node for sensing, computation and communication task directly represent the lifetime of a sensor node. Therefore, energy expenditure optimization is the important metric for intruder detection and tracking. Because, there is wastage of energy either due to the redundant sensing or idle listening [27]. A lot of protocols to solve these problems have been devised in the literature to optimize the energy expenditure. These protocols are based on sensor node activity scheduling. According to these protocols, out of N sensor nodes only a subset of sensor node must be in active state. These active sensor nodes provide full coverage and complete network connectivity. But in case of IDT in harsh geographical region the concept of full coverage is replaced by partial coverage. The partial coverage means the coverage provided by the sensor nodes must be up to some threshold level. Pantazis et al. [28] have reviewed the energy efficient protocols in terms of network structure, topology, communication model and reliable routing. This paper has also provided solution for energy expenditure model for wireless sensor nodes. The energy expenditure model's components are: sensing module, processing or computation module and wireless communication module. Yadav et al. [29] have reviewed various energy efficient protocols in WSN in terms of data aggregation protocols for flat and hierarchical network.

2.5 Duty Cycle

Duty cycle is the working schedule time of the sensor node [30]. The sensor node is in working state intermittently rather than continuously. In WSN, the duty cycle can be

either centralized duty cycle or distributed duty cycle. If the duty cycle is handled by either cluster head or base station, then it is known as centralized duty cycle. On the other hand, if each deployed node handles its own duty cycle then it is known as distributed duty cycle. The nodes go to active or inactive state according to their duty cycle.

3 Intruder Detection and Tracking Attributes

Intruder detection and tracking (IDT) is a real time application of wireless sensor networks. Detection is defined as to identify the existence of an intruder and relay that information to the base station. In contrast to detection, tracking objective is to estimate a path trajectory for that intruder, over specific time period. The path trajectory is the set of next possible positions or locations of the intruder, from where it is going to traverse inside the sensitive region.

An intruder may follow either straight path or random trajectory while intercepting the sensing region. Figure 4 shows the intruder interception in the sensing region of a sensor node in two-dimensional plane. The intruder makes a trajectory i.e. known as path, while intercepting the sensitive region. When a mobile intruder is intersecting the sensing region having sensing range R_s of a particular sensor in 2D plane, then it is detected.

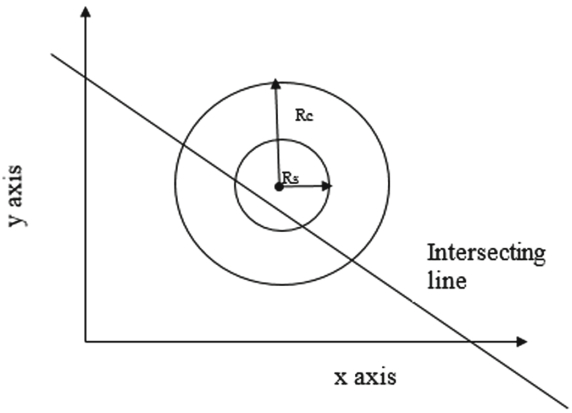


Fig. 4. Interception path in 2D plane

The attributes discussed in this section are helpful in designing intruder detection and tracking protocol. These attributes also impose many challenges for the designing of the protocols. For the complete designing of the IDT protocol, at first, these attributes need to be computed. The prime objective of an IDT protocol is to successfully detect an intruder when it tries to intercept the sensing region of a sensor node.

3.1 Threshold Value (τ)

The threshold value is the value that define limit for the computation of the attributes of IDT protocol. This value helps the fusion center to infer the presence of the intruder. It is an important attribute for IDT protocol because of the randomness in the deployment of sensor node and presence of an intruder. Moreover, the analysis and accuracy of IDT protocol in harsh geographical region can be validated with the help of threshold value. The threshold value is decided after performing number of experiments on the simulated network.

3.2 Detection Probability (P_d)

It is defined as the chances of detection of an intruder while intercepting the sensitive region. The intruder must be detected with detection probability i.e. equals to or greater than the threshold value ($P_d \geq \tau$). The detection probability of an intruder, below threshold value is considered as the false alarm. In IDT, the detection probability result of k ($k \geq 1$) sensor nodes are aggregated to identify the presence of the intruder. Assad et al. [31] have evaluated the detection probability using Poisson distribution. The intruder is considered to be detected by at least k sensor nodes. The detection probability is evaluated as:

$$P_d = 1 - \sum_{i=0}^{k-1} \frac{(A_s \delta)^i}{i!} e^{-A_s \delta} \geq \tau \tag{5}$$

3.3 Average Detection Delay (T_d)

It is defined as the time required by the sensor nodes to detect the intruder after it has intercepted the sensitive region. If the intruder is not detected immediately after intercepting the sensitive region, then it is known as detection delay. It is represented as:

$$T_d = T_f - T_i \tag{6}$$

where, T_f is the time when intruder is detected by the sensor nodes and T_i is the time when intruder has started intercepting the sensitive region.

3.4 Estimated Distance (E_d)

It is defined as the distance between the sensor node and the mobile intruder. This attribute is the prime metric for the signal attenuation modeling. The larger is the distance between the sensor node and intruder the more is the attenuation in the signal. Therefore, a threshold value is decided for the estimated distance, so that only received

signals from threshold distance is considered for identifying the detection of an intruder. It can be represented as:

$$E_d = \sqrt{(S_x - I_x)^2 + (S_y - I_y)^2} \leq \tau \tag{7}$$

where, (S_x, S_y) and (I_x, I_y) are the (x, y) coordinates of sensor node and intruder in two-dimensional plane.

3.5 False Alarm Probability

The sensor nodes sense some passive signals of an intruder which does not exist in actual inside the sensitive region. These sensor nodes generate the detection data about the presence of the intruder and transmit the results to the fusion center. This type of detection data is known as false alarm. An IDT protocol can tolerate false alarm rate up to threshold value to preserve the integrity and reliability of the protocol. Wang et al. [32] have evaluated the global false alarm probability for N sensor nodes as:

$$P_F = 1 - \prod_{i=1}^{N} (1 - p_{f_i}) \tag{8}$$

where, P_F represents the global false alarm probability and p_{f_i} represents the false alarm probability of S_i (i = 1, 2, 3, …, N) sensor nodes.

3.6 Miss Probability

The sensor nodes fail to identify the passive signals when an intruder is actually present inside the sensing region then it is known as intruder miss. An IDT protocol can tolerate the intruder miss up to permissible threshold value. This threshold value is defined in terms of miss probability. Wang et al. [32] have evaluated the global miss probability for N sensor nodes deployed inside a sensing region having area A_s:

$$P_M = \max_{A_s} \left\{ \prod_{i=1}^{N} p_{m_i} \right\} \leq \max_{A_s} \{ \min \{ p_{m_i} \} \} \tag{9}$$

where, P_M represents global miss probability and p_{m_i} represents the miss probability of S_i (i = 1, 2, 3, …, N) sensor nodes. Every point inside the sensing region must be sensed by at least one sensor node having miss probability P_M.

3.7 Data Size

Data size is defined as the total amount of detection data generated by the k sensor nodes after receiving the passive signals about the presence of an intruder. The generated data is processed and fused using collaborative signal processing (CSP) in one of the two ways: Data fusion and Decision fusion [33]. Data fusion exchanges low dimension features mean the sensed data is transmitted to the fusion center without

being processed. This increases the communication cost of the WSN. On the other hand, decision fusion transmits likelihood values to the fusion center. In decision fusion processing at first the sensed data is processed by individual sensor nodes and then the valid results are transmitted to the fusion center. Hence, this approach minimizes the communication cost by transmitting a limited amount of data.

3.8 Data Fusion

The detection data from k-sensor nodes is more reliable for processing as compare to the single sensor node. The total number of detection results are then test on the hypothesis to derive out the necessary conclusion [34]. The main aim of sensor nodes is to generate an inference about the presence or absence of the intruder. Sensor nodes generate inference on the basis of received signals from the intruder. The received signals may attenuate due to the distance between the sensor node and intruder and obstacles inside the sensing region. Moreover, the received signals also consist some amount of noise η or sometimes noise only η. Assume that RSS is the received signal strength at node S_i then the node S_i generates a set of n (where, n = 1, 2, 3, …, n − 1) data results as x[n] = x[0], x [1], x [2], …, x[n − 1]. The value of RSS must be equal to or greater than the threshold value. The two detection hypotheses are generated as:

$$\begin{aligned} H_0 &: x[n] = \eta_n \\ H_1 &: x[n] = RSS_n + \eta_n \end{aligned} \tag{10}$$

If RSS is evaluated using binary results i.e. 1 for successful signal detection and 0 for no signal detection. The 0 value represents that sensor node has received only noise and represented by the hypothesis H_0. The 1 value represents that the received signal also comprises noise and represented by hypothesis H_1. The actual signals must be extracted from the noise to derive out the actual signal strength. After implementing binary detection results the Eq. 10 can be represented as:

$$\begin{aligned} H_0 &: x[n] = \eta_n \\ H_1 &: x[n] = 1 + \eta_n \end{aligned} \tag{11}$$

Therefore, the raw detection data from two or more sensor nodes is processed to interpret the precise detection results so that necessary actions can be taken place. The various data fusion rules applied on the detection data of wireless sensor nodes are:

- Binary data-based decision fusion rule [34]
- K out of N fusion rule [34]
- Distance based decision fusion rule [35]
- Local data fusion rule [36]
- Threshold OR-fusion rule [37]
- Neyman Pearson detector [38]
- Generalized likelihood ratio test (GLRT) [47].

3.9 Signal Attenuation Model

Signal attenuation model plays an important role in locating the intruders. A sensor node sense radio, seismic or audio signals to infer the location of an intruder. In real-time, the received signal strength at sensor nodes is not equivalent to the source signal strength [9]. This happened because of attenuation in propagated signals due to the large distance between the sensor node and intruder, interference and obstacles inside the sensing region. The attenuation in signals is better modeled by using signal attenuation model or path-loss model [39]. In this model, distance between the source and destination signal is an important metric that require prior estimation. The distance can be estimated by applying the following methods on received signals: (1) Received Signal Strength Indicator (RSSI) [9]; (2) Angle of Arrival (AoA) [40]; (3) Direction of Arrival [41]; and (4) Time Difference of Arrival (TDoA) [42]. After estimating the distance and location of an intruder the quantized data is transmitted to fusion center. However, these techniques sometimes suffer from localization errors.

To overcome this limitation, Liu et al. [43] have proposed intruder localization algorithm based on energy measurement model. The energy level (e.g. sound energy emitted by vehicle) decreases as the distance between the sensor node and mobile intruder increases. The fusion center estimates the location of an intruder based on the relationship between received energy level and distance. The signal intensity of sound signal is analyzed by Liu et al. [43] is based on isotropic signal attenuation model presented by Niu et al. [44] and represented as:

$$RSS_i = \sqrt{\frac{P_o}{1 + \alpha E_{di}^m}} + \omega_i \tag{12}$$

where, RSS is received signal strength measured at S_i sensor node, P_0 is the signal power emitted by the intruder at zero distance, α is the adjustable constant, the large value of α the faster signal power decay, m is a constant that represent the signal power decay, E_{di} is the estimated distance between the sensor node S_i and intruder and ω_i is the noise present inside the received signal at node S_i. Deng et al. [45] have proposed a low power sound localization algorithm. This algorithm is applicable in battlefields where, sound signals are the prominent signals to locate the enemies. The authors have done their analysis on traditional acoustic energy attenuation model presented by Li et al. [46]. The sound signal attenuation model at any time t is defined as:

$$RSS_i = \xi_i \frac{S(I)}{|r_i - r(I)|^{\alpha}} + \omega_i \tag{13}$$

where, RSS_i received sound signal strength at sensor node S_i, ξ_i is the gain factor of the S_i sensor node, S(I) is the emitted sound energy at 1 m distance from sound source, $|r_i - r(I)|$ is the distance between the S_i sensor node and intruder, α is the path loss exponent and ω_i is the noise inside the signal. The RSS displayed in Eqs. 12 and 13 holds good when the source power of received signal is already known. But in real time scenario most of the time the source power of received signal is unknown. Ciuonzo et al. [47] have designed a non-cooperative intruder detection algorithm where the

source power of the received signal is unknown. The power law attenuation model based on Amplitude Attenuation Function (AAF) is adopted from [36, 48] and represented as:

$$RSS_i = \frac{1}{\sqrt{1 + \left(\frac{E_d}{\lambda}\right)^{\alpha}}} \tag{14}$$

where, E_d is the estimated Euclidean distance between sensor node and unknown intruder, α represents signal decay value and λ approximates the spatial signature. The exponential attenuation model is represented as:

$$RSS_i = \sqrt{e^{-\left(\frac{E_d^2}{\lambda^2}\right)}} \tag{15}$$

3.10 Signal to Noise Ratio (SNR)

It is defined as the actual strength of the received passive signal (radio, seismic or acoustic signal) to that of the presence of the noise inside received signal. It is an important parameter to detect the presence of an intruder. Köse et al. [49] have estimated and calculated the signal to noise ratio in dB as:

$$SNR = 10 \log_{10}\left(\frac{E_{RSS}}{E\eta} - 1\right) \tag{16}$$

where, E_{RSS} represents the average energy of received signal and E_η represents the average energy of noise signals. There are many real-time applications of signal to noise ratio. The Link Quality Indicator (LQI) in IEEE 802.15.4 protocol is estimated by using signal to noise ratio (SNR) [50]. SNR is an important metric to design an estimate for successful intruder detection and tracking [35, 36].

4 Intruder Detection Protocols

The intruder detection protocols have been designed for two types of intruders i.e. static intruder (such as: to monitor the precious items) and mobile intruder (such as: to detect a mobile vehicle or human being). The protocols for this category have been subdivided into three parts as shown in Fig. 5. This section presents a brief description about these protocols.

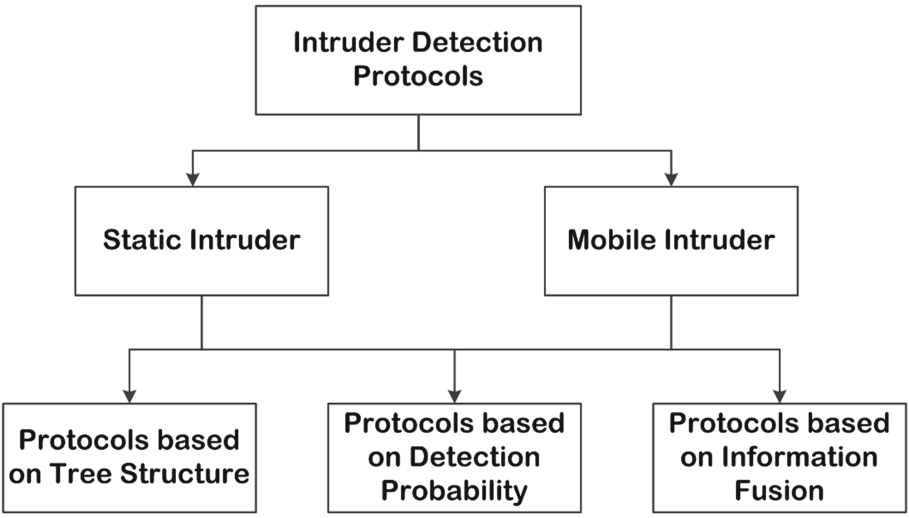


Fig. 5. Classification of intruder detection protocols

4.1 Protocols Based on Tree Structure

This type of protocols uses dynamic tree structure to collaborate with each other for successful intruder detection. Zhang et al. [51] have proposed DCTC (Dynamic Convoy Tree-based Collaboration) protocol for intruder detection and tracking. As the intruder intercepts the sensitive region the sensor nodes collaborate with each other to select a root node which aggregate the detection results. As the intruder moves away from the sensing range of some of the sensor nodes, these nodes are removed from the tree. Dynamic Object Tracking (DOT) [52] is another protocol which uses the concept of planar graph for the construction of face structure so that the intruder can be detected successfully. DOT is a query-based object detection and tracking protocol.

4.2 Protocol Based on Detection Probability

In this category of the protocols, the intruder detection is analyzed and validated on the basis of detection probability and false alarm probability. Cao et al. [53] have analyzed and computed detection probability for both stationary and mobile intruders using various geometrical structures for sensing range and intruder's path. Along with this the nodes' duty cycle is also generated to prolong the network's lifetime. Wang et al. [54] have computed the intruder detection probability for homogeneous and heterogeneous WSN. The authors have used the geometrical structure to represent sensing range and intruder's path for the computation of detection probability. The detection probability is computed for two cases i.e. single sensing detections and multiple sensing detections.

Donmez et al. [55] have computed the detection probability using integral geometry and geometric probability. The intruder's path is considered as a straight line and mapped with line set intersection problem. According to the protocol, if intruder intercept the sensing region, it is definitely detected by at least one sensor node. Coverage area and coverage holes are also considered for the computation of detection probability. Komar et al. [3] have also devised a protocol for the computation of intruder detection probability in accordance to the intruder's favorite path. The intruder detection probability is computed using the deployment strategy of the sensor nodes. The sensor nodes are considered to be randomly deployed and follows Poisson distribution. This paper has proposed the k-sensing model for complete coverage and network connectivity.

4.3 Protocol Based on Information Fusion

This category of protocol senses the signal generated by an intruder. The signal can be seismic, acoustic or electromagnetic signals. The detected signals are used to generate detection probability and false alarm probability [56]. The detected signals can be generated from two type of intruders i.e. active or cooperative intruder and passive or non-cooperative intruder. In case of active intruder, the actual signal power is known and the received signal strength can be analyzed using Eqs. 12 and 13 [45, 46]. On the other there is no knowledge of actual signal power in case of passive intruder detection [47]. The received signal strength can be analyzed using Eqs. 14 and 15. Based on the received signals the hypotheses are generated as represented in Eqs. 10 and 11. The results of the hypothesis related to each sensor node is fused together using various information fusion rules represented in Sect. 3.8 The detection protocols under this category are also generated for multimedia sensors [57]. Al-Jarrah et al. [58] have proposed intruder detection protocol for cooperative wireless sensor networks using decision fusion. The decision fusion rule is based on Neyman-Pearson detector (NP-detector) and Likelihood ratio test (LRT). Ciuonzo et al. [47] have proposed a distributed detection algorithm for non-cooperative intruders using Neyman-Pearson detector and Generalized likelihood ratio test (GLRT).

5 Intruder Tracking Protocols

Intruder tacking is defined as to estimate the trajectory or future path of the intruder which intruder is going to traverse. The intruder tracking protocols are divided into three categories as shown in Fig. 6. This section explains the brief description about these three categories of intruder tracking protocols.

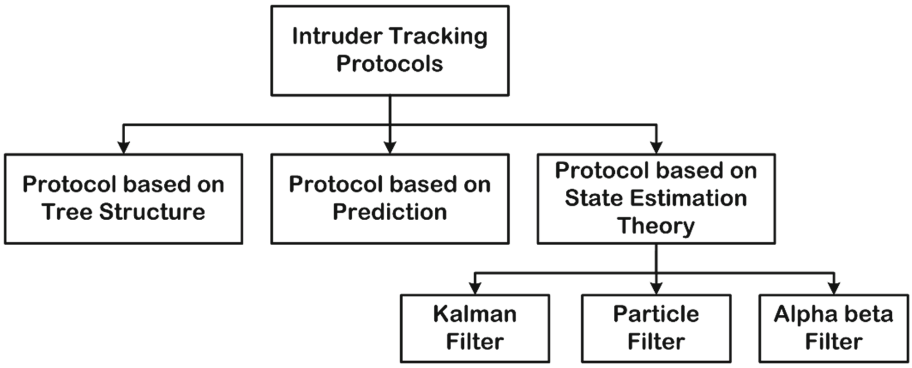


Fig. 6. Classification of intruder tracking protocols

5.1 Protocols Based on Tree Structure

The sensor nodes communicate and collaborate among each other using tree structure to track the mobile intruder. The various protocols in this category are: DCTC (Dynamic Convoy Tree-based Collaboration) protocol [51], DOT (Dynamic Object Tracking) protocol [52], DSTA (Distributed Spanning Tree Algorithm) protocol [59] and FaceTrack protocol [60]. DCTC and DSTA uses tree structure for dynamic construction of network whereas DOT and FaceTrack uses planar graph to construct the network for intruder tracking.

5.2 Protocol Based on Prediction

The intruder tracks are predicted on the basis of available or current values such as intruder signature, moving direction, velocity and acceleration. Xue et al. [61] have designed EDPT (Exponential Distributed Predictive Tracking) protocol for remote tracking of mobile intruders. This protocol also provides recovery mechanism to recover from lost intruder tracks. Similarly, Hsu et al. [62] have proposed POOT (Prediction-based Optimistic Object Tracking strategy) protocol. The accuracy of POOT protocol is 97.5% and can save energy up to 23% by scheduling the duty cycle of the sensor nodes. PPSS (Probability-based Prediction and Sleep Scheduling) protocol is energy efficient mobile intruder tracking protocol [63]. Based on the intruder detection and mobility probability the nodes inside the particular region are remain awaken, where the probability of traversing is maximum. PRATIQUE is a prediction-based clustering protocol for intruder tracking [64]. Ahmadi et al. [65] have designed a mobile intruder tracking protocol based on RSSI (Received Signal Strength Indicator).

5.3 Protocol Based on State Estimation Theory

This category of protocols used the algorithms of estimation theory to estimate the trajectory of intruder. The various algorithms of estimation theory are: Kalman filter, Particle filter and Alpha-beta filter. Misra et al. [66] have designed a localized policy-

based intruder tracking algorithm. At first the intruder's location is identified using received signal strength and then intruder trajectory is estimated using Kalman Filter. The Markov Decision Process (MDP) is used to get an actual estimate about the intruder trajectory. Kalman filter uses intruder's location and velocity to estimate the next plausible locations of the intruder that form trajectory. Mahfouz et al. [67] have also estimated the intruder trajectory using received signal strength and Kalman Filter and maintained a database about the received values. Further the machine learning algorithm is used to estimate the trajectory of future intruders. Machine learning algorithm implements already available knowledge to develop an inference about the application domain.

The above briefly explained intruder detection and tracking protocols in Sects. 4 and 5 provides an outlet about the various categories of the protocols. The new researchers in this field can have a brief idea about various parameters, attributes and protocols of IDT in wireless sensor networks.

6 Challenges and Future Scope for Intruder Detection and Tracking

There are various challenges listed below for information fusion in WSNs because of its resource-constrained nature. These challenges need to be considered while designing the algorithm for IDT application.

- The sensitive region may have an asymmetrical density of sensor nodes due to the random deployment and rough surface. Some of the sub regions may have more than enough sensor nodes causes coverage area overlapping, while others may have sparse senor node causes coverage holes or sensing voids.
- The heterogeneity among sensor nodes cause compatibility issues in terms of sensing and transceiver power. Therefore, heterogeneity creates coverage and connectivity constraints.
- Network connectivity is the main constraint because the prior research work on WSN network connectivity is done for uniform deployment of sensor nodes in uniform and plain surface. There is no optimum solution for the problem of network connectivity in harsh geographical regions.
- There is a huge noise in the information that means noise in the received signals. This happens due to the harsh geographical region, obstacles inside the region and large distance between the sensor node and intruder. The noise statistics should be modeled before the WSN deployment.
- The limited battery power of sensor nodes causes a scarcity of energy. A proper energy expenditure modeling is required to prolong the WSN lifetime.
- The rough surface and wireless communication channel restrict the sensor node from utilizing their appropriate bandwidth.
- Sensor nodes failure either due to the physical damage or early depletion of battery power.
- The data generated by the sensor nodes is sometimes incomplete and imprecise. This category of data is known as corrupted data.

- There must be accurate in the intruder location estimation.
- The recovery from missed and lost intruder tracks.
- The deployment of sensor nodes in geographical harsh regions is susceptible to attacks. Therefore, to design a secure data transmission mechanism for deployed sensor nodes.
- To implement computational intelligence for smart intruder detection and tracking.

7 Conclusion

Wireless sensor networks are adapted to evolving technologies that are more precise and intelligent. This makes sensor networks to surveil the harsh geographical regions without any intervention of human being. WSN network has increased its aptness towards surveillance of the sensitive regions to identify the malicious activities successfully. It encompasses detection and tracking of mobile intruders at a particular region, where sensor nodes are deployed. WSN is used for intrusion detection at hostile border areas, where nodes are deployed randomly and the existence of event is in a random manner. This chapter has discussed various WSN parameters and IDT attributes that help in designing intruder detection and tracking protocols. This chapter has also briefly explained the various categories of IDT protocols and presented various challenges that emerge while designing the IDT protocols.

References

1. Sharma, A., Chauhan, S.: Target coverage computation protocols in wireless sensor networks: a comprehensive review. Int. J. Comput. Appl., 1–23 (2019). https://doi.org/10.1080/1206212x.2019.1663382
2. Sun, Z., Wang, P., Vuran, M.C., Al-Rodhaan, M.A., Al-Dhelaan, A.M., Akyildiz, I.F.: BorderSense: border patrol through advanced wireless sensor networks. Ad Hoc Netw. **9**, 468–477 (2011). https://doi.org/10.1016/j.adhoc.2010.09.008
3. Komar, C., Donmez, M.Y., Ersoy, C.: Detection quality of border surveillance wireless sensor networks in the existence of trespassers' favorite paths. Comput. Commun. **35**, 1185–1199 (2012). https://doi.org/10.1016/j.comcom.2012.03.002
4. Wang, B.: Coverage problems in sensor networks: a survey. ACM Comput. Surv. (CSUR) **43**, 32 (2011). https://doi.org/10.1145/1978802.1978811
5. Li, Y., Jha, D.K., Ray, A., Wettergren, T.A.: Information fusion of passive sensors for detection of moving targets in dynamic environments. IEEE Trans. Cybern. **47**, 93–104 (2016). https://doi.org/10.1109/TCYB.2015.2508024
6. Yang, X., Zhang, W.A., Yu, L., Xing, K.: Multi-rate distributed fusion estimation for sensor network-based target tracking. IEEE Sens. J. **16**, 1233–1242 (2015). https://doi.org/10.1109/JSEN.2015.2497464
7. Bhuiyan, M.Z.A., Wang, G., Vasilakos, A.V.: Local area prediction-based mobile target tracking in wireless sensor networks. IEEE Trans. Comput. **64**, 1968–1982 (2014). https://doi.org/10.1109/TC.2014.2346209

8. Wang, X., Fu, M., Zhang, H.: Target tracking in wireless sensor networks based on the combination of KF and MLE using distance measurements. IEEE Trans. Mob. Comput. **11**, 567–576 (2011). https://doi.org/10.1109/TMC.2011.59
9. Liu, C., Fang, D., Yang, Z., Jiang, H., Chen, X., Wang, W., Xing, T., Cai, L.: RSS distribution-based passive localization and its application in sensor networks. IEEE Trans. Wirel. Commun. **15**, 2883–2895 (2015). https://doi.org/10.1109/TWC.2015.2512861
10. Jain, S., Pattanaik, K.K., Shukla, A.: QWRP: query-driven virtual wheel based routing protocol for wireless sensor networks with mobile sink. J. Netw. Comput. Appl. **147**, 102430 (2019). https://doi.org/10.1016/j.jnca.2019.102430
11. He, J., Yu, Y., Wang, Q.: RSS assisted TOA-based indoor geolocation. Int. J. Wirel. Inf. Netw. **20**, 157–165. https://doi.org/10.1007/s10776-012-0198-9
12. Lee, J., Cho, K., Lee, S., Kwon, T., Choi, Y.: Distributed and energy-efficient target localization and tracking in wireless sensor networks. Comput. Commun. **29**, 2494–2505 (2006). https://doi.org/10.1016/j.comcom.2006.02.004
13. Tomic, S., Beko, M., Dinis, R.: RSS-based localization in wireless sensor networks using convex relaxation: noncooperative and cooperative schemes. IEEE Trans. Veh. Technol. **64**, 2037–2050 (2014). https://doi.org/10.1109/TVT.2014.2334397
14. Souza, É.L., Nakamura, E.F., Pazzi, R.W.: Target tracking for sensor networks: a survey. ACM Comput. Surv. (CSUR) **49**, 30 (2016). https://doi.org/10.1145/2938639
15. Ribeiro, A., Schizas, I.D., Roumeliotis, S.I., Giannakis, G.: Kalman filtering in wireless sensor networks. IEEE Control Syst. Mag. **30**, 66–86 (2010). https://doi.org/10.1109/MCS.2009.935569
16. Abdollahzadeh, S., Navimipour, N.J.: Deployment strategies in the wireless sensor network: a comprehensive review. Comput. Commun. **91**, 1–16 (2016). https://doi.org/10.1016/j.comcom.2016.06.003
17. Sharma, V., Patel, R.B., Bhadauria, H.S., Prasad, D.: Deployment schemes in wireless sensor network to achieve blanket coverage in large-scale open area: a review. Egypt. Inform. J. **17**, 45–56 (2016). https://doi.org/10.1016/j.eij.2015.08.003
18. Altınel, İ.K., Aras, N., Güney, E., Ersoy, C.: Binary integer programming formulation and heuristics for differentiated coverage in heterogeneous sensor networks. Comput. Netw. **52**, 2419–2431 (2008). https://doi.org/10.1016/j.comnet.2008.05.002
19. Onur, E., Ersoy, C., Deliç, H., Akarun, L.: Surveillance wireless sensor networks: deployment quality analysis. IEEE Netw. **21**, 48–53 (2007). https://doi.org/10.1109/MNET.2007.4395110
20. Hefeeda, M., Ahmadi, H.: Energy-efficient protocol for deterministic and probabilistic coverage in sensor networks. IEEE Trans. Parallel Distrib. Syst. **21**, 579–593 (2009). https://doi.org/10.1109/TPDS.2009.112
21. Kashi, S.S., Sharifi, M.: Coverage rate calculation in wireless sensor networks. Computing **94**, 833–856 (2012). https://doi.org/10.1007/s00607-012-0192-1
22. Sharma, A., Chauhan, S.: Optimal threshold coverage area (OTCA) algorithm for random deployment of sensor nodes in large asymmetrical terrain. In: Singh, M., Gupta, P., Tyagi, V., Flusser, J., Ören, T. (eds) Advances in Computing and Data Sciences. ICACDS 2018. Communications in Computer and Information Science, vol. 906. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-1813-9_4
23. Zhang, H., Hou, J.C.: Maintaining sensing coverage and connectivity in large sensor networks. Ad Hoc Sens. Wirel. Netw. **1**, 89–124 (2005)
24. Akram, V.K., Dagdeviren, O.: DECK: a distributed, asynchronous and exact k-connectivity detection algorithm for wireless sensor networks. Comput. Commun. **116**, 9–20 (2018). https://doi.org/10.1016/j.comcom.2017.11.005

25. Biswas, S., Das, R., Chatterjee, P.: Energy-efficient connected target coverage in multi-hop wireless sensor networks. In: Bhattacharyya, S., Sen, S., Dutta, M., Biswas, P., Chattopadhyay, H. (eds.) Industry Interactive Innovations in Science, Engineering and Technology. Lecture Notes in Networks and Systems, vol. 11. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-3953-9_40
26. Wang, H., Roman, H.E., Yuan, L., Huang, Y., Wang, R.: Connectivity, coverage and power consumption in large-scale wireless sensor networks. Comput. Netw. **75**, 212–225 (2014). https://doi.org/10.1016/j.comnet.2014.10.008
27. Abo-Zahhad, M., Amin, O., Farrag, M., Ali, A.: Survey on energy consumption models in wireless sensor networks. Open Trans. Wirel. Sens. Netw. **1**, 63–79 (2014)
28. Pantazis, N.A., Nikolidakis, S.A., Vergados, D.D.: Energy-efficient routing protocols in wireless sensor networks: a survey. IEEE Commun. Surv. Tutor. **15**, 551–591 (2012). https://doi.org/10.1109/SURV.2012.062612.00084
29. Yadav, S., Yadav, R.S.: A review on energy efficient protocols in wireless sensor networks. Wirel. Netw. **22**, 335–350 (2016). https://doi.org/10.1007/s11276-015-1025-x
30. Liu, K.S., Gao, J., Lin, S., Huang, H., Schiller, B.: Joint sensor duty cycle scheduling with coverage guarantee. In: Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 11–20. ACM (2016). https://doi.org/10.1145/2942358.2942379
31. Assad, N., Elbhiri, B., Faqihi, M.A., Ouadou, M., Aboutajdine, D.: Efficient deployment quality analysis for intrusion detection in wireless sensor networks. Wirel. Netw. **22**, 991–1006 (2016). https://doi.org/10.1007/s11276-015-1015-z
32. Wang, W., Srinivasan, V., Chua, K.C., Wang, B.: Energy-efficient coverage for target detection in wireless sensor networks. In: Proceedings of the 6th International Conference on Information Processing in Sensor Networks, pp. 313–322. ACM (2007). https://doi.org/10.1145/1236360.1236401
33. D'Costa, A., Sayeed, A.M.: Data versus decision fusion in wireless sensor networks. In: 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 4, pp. IV-832–835. IEEE (2003). https://doi.org/10.1109/icassp.2003.1202772
34. Varshney, P.K.: Distributed Detection and Data Fusion. Springer, Heidelberg (2012)
35. Duarte, M., Hu, Y.H.: Distance-based decision fusion in a distributed wireless sensor network. Telecommun. Syst. **26**, 339–350 (2004). https://doi.org/10.1023/B:TELS.0000029045.03170.e9
36. Katenka, N., Levina, E., Michailidis, G.: Local vote decision fusion for target detection in wireless sensor networks. IEEE Trans. Signal Process. **56**, 329–338 (2007). https://doi.org/10.1109/TSP.2007.900165
37. Zhu, M., Ding, S., Wu, Q., Brooks, R.R., Rao, N.S., Iyengar, S.S.: Fusion of threshold rules for target detection in wireless sensor networks. ACM Trans. Sens. Netw. (TOSN) **6**, 18 (2010). https://doi.org/10.1145/1689239.1689248
38. Zhao, H., Chen, L., Feng, W.: A signal detection scheme for wireless sensor networks based on convex optimization. In: 2016 IEEE SENSORS, pp. 1–3. IEEE (2016). https://doi.org/10.1109/icsens.2016.7808713
39. Kurt, S., Tavli, B.: Path-loss modeling for wireless sensor networks: a review of models and comparative evaluations. IEEE Antennas Propag. Mag. **59**, 18–37 (2017). https://doi.org/10.1109/MAP.2016.2630035
40. Niculescu, D., Nath, B.: Ad hoc positioning system (APS) using AOA. In: IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 1734–1743. IEEE (2003). https://doi.org/10.1109/infcom.2003.1209196

41. Hassani, A., Bertrand, A., Moonen, M.: Distributed node-specific direction-of-arrival estimation in wireless acoustic sensor networks. In: 21st European Signal Processing Conference, pp. 1–5. IEEE (2013)
42. Girod, L., Estrin, D.: Robust range estimation using acoustic and multimodal sensing. In: Proceedings 2001 IEEE/RSJ International Conference on Intelligent Robots and Systems. Expanding the Societal Role of Robotics in the Next Millennium, pp. 1312–1320. IEEE (2001). https://doi.org/10.1109/iros.2001.977164
43. Liu, G., Liu, H., Chen, H., Zhou, C., Shu, L.: Position-based adaptive quantization for target location estimation in wireless sensor networks using one-bit data. Wirel. Commun. Mob. Comput. **16**, 929–941 (2016). https://doi.org/10.1002/wcm.2576
44. Niu, R., Varshney, P.K.: Distributed detection and fusion in a large wireless sensor network of random size. EURASIP J. Wirel. Commun. Netw. **2005**, 462–472 (2005). https://doi.org/10.1155/WCN.2005.462
45. Deng, F., Guan, S., Yue, X., Gu, X., Chen, J., Lv, J., Li, J.: Energy-based sound source localization with low power consumption in wireless sensor networks. IEEE Trans. Ind. Electron. **64**, 4894–4902 (2017). https://doi.org/10.1109/TIE.2017.2652394
46. Li, D., Hu, Y.H.: Energy-based collaborative source localization using acoustic microsensor array. EURASIP J. Adv. Signal Process. **2003**, 985029 (2003). https://doi.org/10.1155/S1110865703212075
47. Ciuonzo, D., Rossi, P.S.: Distributed detection of a non-cooperative target via generalized locally-optimum approaches. Inf. Fusion **36**, 261–274 (2017). https://doi.org/10.1016/j.inffus.2016.12.006
48. Guerriero, M., Svensson, L., Willett, P.: Bayesian data fusion for distributed target detection in sensor networks. IEEE Trans. Signal Process. **58**, 3417–3421 (2010). https://doi.org/10.1109/TSP.2010.2046042
49. Köse, M., Taşcioğlu, S., Telatar, Z.: Signal-to-noise ratio estimation of noisy transient signals. Commun. Fac. Sci. Univ. Ankara Ser. A2-A3 **57**, 11–19 (2015). https://doi.org/10.1501/commua1-2_0000000084
50. Qin, F., Dai, X., Mitchell, J.E.: Effective-SNR estimation for wireless sensor network using Kalman filter. Ad Hoc Netw. **11**, 944–958 (2013). https://doi.org/10.1016/j.adhoc.2012.11.002
51. Zhang, W., Cao, G.: DCTC: dynamic convoy tree-based collaboration for target tracking in sensor networks. IEEE Trans. Wirel. Commun. **3**, 1689–1701 (2004). https://doi.org/10.1109/TWC.2004.833443
52. Tsai, H.W., Chu, C.P., Chen, T.S.: Mobile object tracking in wireless sensor networks. Comput. Commun. **30**(8), 1811–1825 (2007). https://doi.org/10.1016/j.comcom.2007.02.018
53. Cao, Q., Yan, T., Stankovic, J., Abdelzaher, T.: Analysis of target detection performance for wireless sensor networks. In: International Conference on Distributed Computing in Sensor Systems, pp. 276–292. Springer, Heidelberg (2005). https://doi.org/10.1007/11502593_22
54. Wang, Y., Wang, X., Xie, B., Wang, D., Agrawal, D.P.: Intrusion detection in homogeneous and heterogeneous wireless sensor networks. IEEE Trans. Mob. Comput. **7**, 698–711 (2008). https://doi.org/10.1109/TMC.2008.19
55. Donmez, M.Y., Kosar, R., Ersoy, C.: An analytical approach to the deployment quality of surveillance wireless sensor networks considering the effect of jammers and coverage holes. Comput. Netw. **54**, 3449–3466 (2010). https://doi.org/10.1016/j.comnet.2010.07.007

56. Rumyantsev, K., Zikiy, A., Zlaman, P.: Detection of signals by the frequency-time contrast method. In: Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-3804-5_7
57. Boulanouar, I., Lohier, S., Rachedi, A., Roussel, G.: DTA: deployment and tracking algorithm in wireless multimedia sensor networks. Ad Hoc Sens. Wirel. Netw. **28**, 115–135 (2015)
58. Al-Jarrah, M.A., Al-Dweik, A., Kalil, M., Ikki, S.S.: Decision fusion in distributed cooperative wireless sensor networks. IEEE Trans. Veh. Technol. **68**, 797–811 (2018). https://doi.org/10.1109/TVT.2018.2879413
59. Alaybeyoglu, A., Dagdeviren, O., Kantarci, A., Erciyes, K.: A distributed wakening based target tracking protocol for wireless sensor networks. In: 2010 Ninth International Symposium on Parallel and Distributed Computing, pp. 165–172. IEEE (2010). https://doi.org/10.1109/ispdc.2010.33
60. Wang, G., Bhuiyan, M.Z.A., Cao, J., Wu, J.: Detecting movements of a target using face tracking in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **25**, 939–949 (2013). https://doi.org/10.1109/TPDS.2013.91
61. Xue, L., Liu, Z., Guan, X.: Prediction-based protocol for mobile target tracking in wireless sensor networks. J. Syst. Eng. Electron. **22**, 347–352 (2011). https://doi.org/10.3969/j.issn.1004-4132.2011.02.024
62. Hsu, J.M., Chen, C.C., Li, C.C.: POOT: an efficient object tracking strategy based on short-term optimistic predictions for face-structured sensor networks. Comput. Math. Appl. **63**, 391–406 (2012). https://doi.org/10.1016/j.camwa.2011.07.034
63. Jiang, B., Ravindran, B., Cho, H.: Probability-based prediction and sleep scheduling for energy-efficient target tracking in sensor networks. IEEE Trans. Mob. Comput. **12**, 735–747 (2012). https://doi.org/10.1109/TMC.2012.44
64. Souza, É.L., Pazzi, R.W., Nakamura, E.F.: A prediction-based clustering algorithm for tracking targets in quantized areas for wireless sensor networks. Wirel. Netw. **21**, 2263–2278 (2015). https://doi.org/10.1007/s11276-015-0914-3
65. Ahmadi, H., Viani, F., Bouallegue, R.: An accurate prediction method for moving target localization and tracking in wireless sensor networks. Ad Hoc Netw. **70**, 14–22 (2018). https://doi.org/10.1016/j.adhoc.2017.11.008
66. Misra, S., Singh, S.: Localized policy-based target tracking using wireless sensor networks. ACM Trans. Sens. Netw. (TOSN) **8**, 27 (2012). https://doi.org/10.1145/2240092.2240101
67. Mahfouz, S., Mourad-Chehade, F., Honeine, P., Farah, J., Snoussi, H.: Target tracking using machine learning and Kalman filter in wireless sensor networks. IEEE Sens. J. **14**, 3715–3725 (2014). https://doi.org/10.1109/JSEN.2014.2332098

Applications of Wireless Sensor Networks

Opportunities and Challenges with WSN's in Smart Technologies: A Smart Agriculture Perspective

Nagesh Kumar(✉) and Brijbhushan Sharma(✉)

School of Electrical and Computer Science,
Shoolini University of Biotechnology and Management Sciences, Solan,
Himachal Pradesh, India
engg.nagesh2@gmail.com, bsharmavik@gmail.com

Abstract. Study of a smart environment is very common these days. The techniques for building smart applications, consist of manufacturing devices and sensors, which can communicate with each other to monitor their surrounding conditions. These conditions may be environmental conditions like pollutant gases, radiations, noise and waste etc. Basically, useful information is generated by the sensor nodes deployed in the environment and decision implementation is done by the controller to control the conditions according to requirement of the users or applications. Wireless sensor networks are able to accumulate the information from the environment. This may be done with the help of tiny sensors nodes which can communicate with the other sensor nodes wirelessly and are not harmful to the environment. These tiny sensor nodes operate on low power to perform various operations like sensing and any type of calculations. The communication process between the sensor nodes also consumes low power which will ensure the long life of the networks. The architecture of the sensor nodes gives the advantage to program the micro-controllers associated with these, depending upon the applications. There are numerous of applications of wireless sensor networks which include applications in healthcare, defense, smart cities, event detection and underwater monitoring applications. Also in the field of smart agriculture, sensors play a vital role in different applications like soil quality checking, precision agriculture and irrigation control. In this chapter, a study of wireless sensor networks for smart applications is conducted. The main focus of the chapter is on smart applications in agriculture. The chapter answers questions like how to design and develop smart techniques for agriculture, how can the wireless sensor networks help in precision agriculture.

Keywords: WSN · Sensor · Smart environments · Smart agriculture · Smart applications

1 Introduction

To monitor physical or environmental conditions, such as sound, temperature, vibrations, pollutants or motion and pressure autonomous sensor nodes have been used by wireless sensor networks. All the data collected by the sensor nodes is transmitted to

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 441–463, 2020.
https://doi.org/10.1007/978-3-030-40305-8_22

the main base station with the help of network. With the use of these inexpensive, tiny and smarter devices more and more area can easily be covered for the investigation, all measuring environment parameters can be covered. It has enabled the continuous timed monitoring. Now collection of data can be done in real-time. Sensor nodes are used to gather data, store and then sharing the same data on network. As wireless sensor network has a very wide range of applications in almost each and every sector in this article smart agriculture has been focused.

In smart agriculture, precision farming is a technique to manage very large fields. More sophisticated sensor nodes with sensing abilities to biological and chemical parameters are required. This may increase the productivity in the fields and will be helpful for the farmers to achieve more with less efforts [1]. Precision farming is the capacity to deal with so many varieties in the productivity of crops within the fields and to increase it, so that it can help in maximizing the financial properties. This technique is also used to minimize the wastage, environmental impacts by using the automatic data gathering with sensor nodes deployed with in the fields. The gathered information is helpful in managing the fields and decision-making capability also increases. Researchers have introduced so many new and smart technologies in precision farming, few of them are GPS, Remote Sensing and GIS [2]. Whereas to make precision farming more effective characteristics of soil is required. Characteristics' values may be recorded using sensor nodes which are deployed in the fields. These sensor nodes consist of Sensing unit, Controlling unit and the actuator unit. These sensor nodes are deployed very densely [3] so that the exact and effective data can be collected to address various issues. Sensor nodes do not require any special care, these can be deployed randomly, which means no predetermined position is required. These sensor nodes can easily communicate with each other and are able to transmit the gathered data to the end user or base station. Routing capabilities of the sensor nodes make WSN so important. In wireless sensor networks base station is where user collect the processed and aggregated information. Communication in between sensor nodes and base station can take place using WIFI, Bluetooth and internet connectivity.

This chapter will discuss the possible applications of WSN in smart precision farming which will help the readers to enhance research in this field. The issues and challenges will be discussed and last five to six years of literature will be elaborated to find out current state of art in this research area.

1.1 Wireless Sensor Networks (WSN)

Number of sensor nodes in WSN is much larger than any of traditional wireless networks. A major difference between WSN and other traditional networks computing devices including PC's, PDA's and other embedded devices is that in WSN main emphasize is on power management. WSN is a data centric approach but traditional wireless networks are address centric because of large number of nodes in WSN. Sensor nodes are much cheaper than nodes in other wireless networks. WSN uses broadcast communication approach but traditional wireless networks use point-to-point communication. Traditional wireless network like Mobile Ad hoc Networks are designed for distributed computing while WSN are designed to gather information. A unique characteristic of WSN is that data collected by adjacent nodes and some

consecutive readings sensed by sensors are highly correlated which gives opportunity to develop efficient protocols. 802.11-like MAC in traditional wireless networks consumes two to six times more energy than S-MAC for traffic load with messages sent every 1–10 s (Fig. 1).

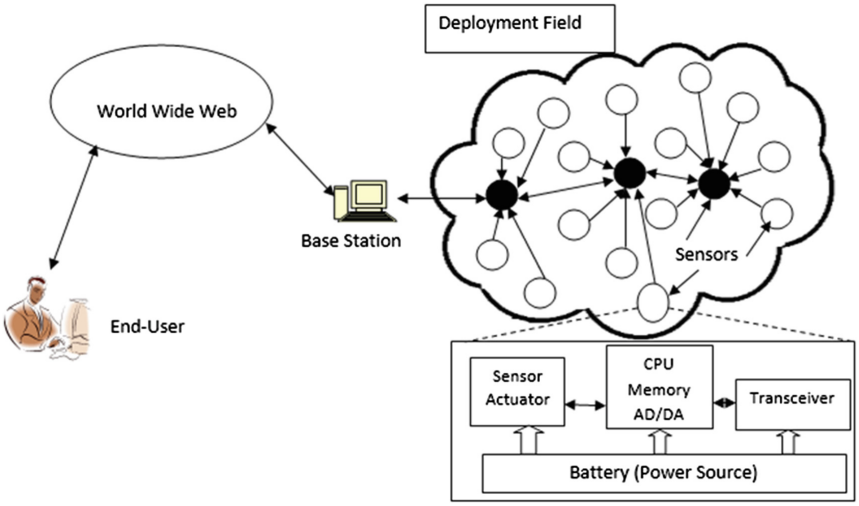


Fig. 1. WSN architecture.

In basic architecture of WSN, in sensor unit data gathering and processing operations are completed. All the important and useful data are transmitted to the base station. Transceiver unit is responsible for the reception of the instruction from the base station and to transmit the gathered data to the base station. Power source is the backbone of any device and as in WSN sensor nodes are deployed in an open environment, it is really tough to replace or provide a continuous power supply. There are many solutions to this problem provided in literature like solar power etc. but still the power sources used in sensor nodes are batteries. Analog to digital Converter (ADC), microcontrollers used in WSN, understands binary and some of the analog sensors are used whose outputs are analog and this output needs to be converted to the digital signals. In sensor node GPS is placed which helps to find the location for randomly deployed sensor nodes [4]. Most of the sensor nodes are common to all applications like temperature sensors, humidity sensor etc. otherwise, sensors can be designed according to application requirements. In this chapter sensors available for smart agriculture or used in smart agriculture will be studied. Also, various techniques used in smart agriculture, issues and challenges present in smart agriculture will be discussed.

1.2 Internet of Things (IoT)

Internet of things is a technology which connect physical electronic devices through internet. These devices are capable in gathering and exchanging data (information) over

a network as these devices are equipped with unique addressing. IoT is based on embedded system technology as it contains both hardware and software, this allows IoT devices to communicate in both the states (inside and outside environment). IoT is based on three layers system, which are sensing (perception layer), network layer (MAC & Routing) for the data transfer, and application layer related with the output [5, 6]. Internet is used as human to human communication whereas IoT is internet for machine to machine communication. IoT may be used in abundance of applications which includes smart cities, smart buildings, agriculture, defense and healthcare etc. (Fig. 2).

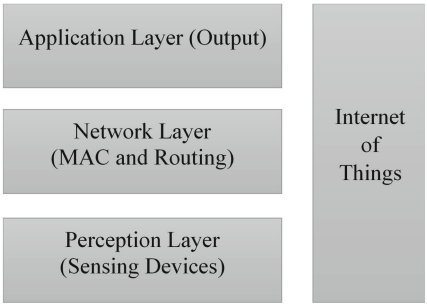


Fig. 2. Architecture of IoT systems.

Smart agriculture is one of the most potential area of research and almost whole world is getting influenced by the applications of WSN and IoT solutions for it. These solutions include precision equipment, geo-positioning, actuators, sensors, UAV's (drones), robotics and automation etc. [7, 8]. IoT offers so many options for smart farming like useful data collection regarding crops and soil, crop control and automatic farming methods. As the sensors used in are capable of providing useful information to the farmers regarding their crops yield process, moisture level, soil nutrition, pest infestation and information regarding above said parameters can be very useful for the farmer to increase his productivity (Fig. 3).

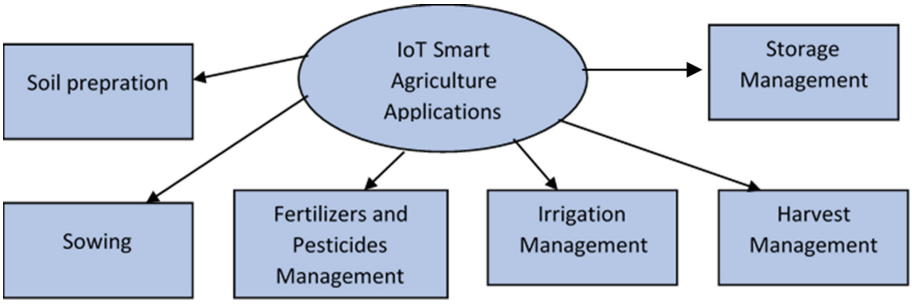


Fig. 3. IoT applications in agriculture industry.

2 Literature Study Process

Most of the papers included in this chapter are from last five years, until unless it seems to be important to include some of oldest papers. The research questions are designed, and the relevant research works are referred accordingly.

2.1 Research Questions

The chapter's main focus is to provide answers to the questions related to use of WSN in smart agriculture. Major research questions that will be answered in this review are:

RQ1. What are the possibilities to use WSN and IoT in agriculture?

RQ2. What are newly developed sensors to be used for making smart agriculture a revolution?

RQ3. What are various issues and challenges researchers may face, when they are working with WSN in agriculture?

2.2 Information Source

Due to wide scope of this book, it was suggested that, different research databases can be extracted for existing work on smart agriculture with WSN. So, in this chapter mainly five databases are considered in searching, to generate the state of the art in use of WSN and IoT with agriculture. These databases are

1. IEEE Xplore (www.ieeexplore.ieee.org)
2. ACM digital library (dl.acm.org)
3. Science direct (www.sciencedirect.com)
4. Google Scholar (www.scholar.google.com)
5. Springer (www.springer.com)
6. Taylor & Francis Online (https://tandfonline.com/)

The papers considered for the review in this chapter are only from high impact research journals and conferences. These articles are indexed in SCI, Scopus and Web of Sciences databases. The searching keywords were related to sensors, WSN, IoT, Precision agriculture, Smart agriculture, Crop management, soil management, monitoring crops, irrigation control and other related words.

3 Review of Literature

This article is concerned about the research in smart agriculture using sensors and IoT, published in reputed journals during last five years. The literature survey includes crop monitoring research, sensors to be used in smart agriculture and communication technologies for smart agriculture. These categories of literature are summarized in upcoming subsections.

3.1 Crop Management with WSN

Agriculture is the backbone for the humans as it is one of the main sources of food. Agriculture has a great role in the growth of countries' economy. This field offers a huge amount of employment for the people. So, the growth in production of agriculture products is also very important. Traditional methods are still in use and are not so much effective in the productivity of the agriculture output [9]. In order to address all the issues in agriculture it is necessary to introduce automation with the help of WSN and IoT. The table below present some the recent research on crop monitoring technologies using WSN and IoT [10]. In the following table the findings of authors from last five year in the area of crop monitoring are discussed. The papers discussed in the following table are from reputed databases only and also only last three years are considered for this review (Table 1).

Table 1. Crop monitoring research during last three years (2017–2019)

Sr. No.	Title	Author	Year	Crops	Findings
1	IoT based smart crop-field monitoring and automation irrigation system [11]	R. Nageswara Rao, B. Sridhar	2018		Irrigation system is developed with low complex circuit. Temperature sensor and moisture sensor is used in the development. This type of sensor nodes can be very useful in the field to monitor crops and will be able to keep a check on the irrigation of the specific crop which will help in the overall production of the crops
2	Effective Utilization of IoT for Low-cost Crop Monitoring and Automation [12]	Petcharat Suriyachai, Jakkapong Pansit	2018		Authors have developed an IoT-based device for the monitoring crops as well as for the automation also. Low cost sensor node has been used and clustered wireless sensor network is created to collect the data

(*continued*)

Table 1. (*continued*)

Sr. No.	Title	Author	Year	Crops	Findings
					with the help of IoT cloud-based platform. Moreover, authors have also provided a weather API to provide the weather forecast, if the system receive the notification regarding the rain possibility, the system will avoid all its schedules to water the plants. AA Batteries are used in the sensor node if the sensor nodes batteries are low a line message will be sent to the user to change the or replace the batteries. Google API will help in to find the location of the sensor node
3	IOT Based Crop-Field Monitoring and Irrigation Automation [13]	P. Rajalakshmi, S. Devi Mahalakshmi	2017		Researchers have designed and implemented an automatic system for irrigation and this system reduced the water consumption to a greater extent used in this research paper. Authors claimed it a cost effective and beneficial. This system is useful for green houses. Authors are currently working

(*continued*)

Table 1. (*continued*)

Sr. No.	Title	Author	Year	Crops	Findings
					on Data mining algorithms for the predictions of crop water requirements
4	Agro-tech: a digital model for monitoring soil and crops using Internet of things (iot) [14]	Mr. O. Pandithurai, S. Aishwarya, B. Aparna, K. Kavitha	2017		In this paper authors claimed that their embedded hardware kit & software will work as a helping hand to the farmers. Their system can detect the soil and crop parameters and the data will be transferred with the help of the IoT to the software which AGRO-TECH on the basis of the data sensed by the soil sensor irrigation system will start and stop its working. This system generates weekly reports and gsm-based system will inform user if in any case a emergency situation occurs
5	IoT enabled Plant Sensing Systems for Small and Large Scale Automated Horticultural Monitoring [15]	Sherjeel Khan, Muhammad Mustafa Hussain	2019	Barley Plant, Lucky Bamboo	In this paper authors have shown high performing sensor which is lightweight platform that can be placed on a plant leaf to monitor the surrounding climate around the plant Furthermore they have demonstrated a strain sensor fabricated Used to check the growth of

(*continued*)

Table 1. (*continued*)

Sr. No.	Title	Author	Year	Crops	Findings
					the plant growth can be checked in micrometers. This system can be used for a large area as authors have demonstrated in this paper they have also developed a drone made up of flexible sensors Wings of the drone what made up of biodegradable paper to soften the landing of the drones Light humidity and heat sensors are mounted on the drones to monitor the growth of the crop
6	A Novel Framework for Smart Crop Monitoring Using Internet of Things (IOT) [16]	Kamal Kumar Ghanshala, Rahul Chauhan, R.C. Joshi	2018		Authors have proposed a 4 level framework For crop monitoring the proposed system is based on soil nutrients and IoT devices. Edge computing and cloud computing techniques were used as these can be accessible to monitor the stored data from anywhere. Whole system is designed to achieve the proper utilization of fertilizers in an effective manner to achieve the high yield from the fields

(*continued*)

Table 1. (*continued*)

Sr. No.	Title	Author	Year	Crops	Findings
7	Agricultural Crop Monitoring using IOT- A Study [17]	Dr. D. K. Sreekantha, A. M. Kavya	2017		According to the authors IoT has enabled user to monitor their crops, due to which farmers are able to increase their productivity and hence their profits are also increased. Sensor of different type are used to monitor crops and collect important information
8	Rice Crop Monitoring System - A IoT Based Machine Vision Approach [18]	P. Tanmayee	2017	Rice	In this paper author have done their research by collecting periodic images of the crops. The system developed by the authors, help farmers to reduce the need of pesticides it also reduces the human interface. The system is able to detect the disease in early stage but as the system is on wireless some time delay may occur

3.2 Sensors Used in Smart Agriculture

Sensors/Sensor nodes are compact in size, cheap and easily available. A sensor node mainly consists a microcontroller, transceiver, power source, memory, ADC (analog-to-digital converter) and finally one or more sensors [36]. The microcontroller is the brain of the sensor node which processes all of the data gathered and also controls the functionality of all components mounted on the node. The transceiver transmits the collected data as well as receives the data to and fro from the base station or control

section using wireless transmission media like RF (radio frequency), optical communication (laser) and infrared. Sensor nodes produce a measurable response to any physical change that occurs around them. Conditions like temperature, humidity, pressure etc. can be detected by the sensors easily. Following table presents the details about sensors used in various research papers during last five years. From the table one can know the possibility of using sensor nodes and type of microcontrollers in smart agriculture applications (Table 2).

Table 2. Sensors used in research on smart agriculture during last five years (2015–2019).

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
1	Acquisition and Mining of Agricultural Data Using Ubiquitous Sensors with Internet of Things [19]	M. R. Suma, P. Madhumathy	2018	DHT11, Standard Soil Sensor	ATMEL ATmega328P, Raspberry Pi3	The system was successfully developed and executed in targeted area. Major hardware used to create the system are like Arduino, Raspberry Pi 3 model software's used are Django Web Framework, for communication purposes standard 433 MHz RF link is used. Authors have noticed major problem in communication system the mode they have used is half duplex communication mode. They have suggested that with the proper hardware these problems can be reduced, however they are satisfied that by having these problems they have successfully implemented the

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
						system and achieved results
2	IOT Based Smart Agriculture System [20]	G. Sushanth, S. Sujatha	2018	LM35 Temp, humidity, moisture and motion sensor	Arduino Uno R3, ESP8266 Node MCU, GSM Module	Hardware used the authors to develop system are Arduino UNO R3, ESP8266 Node MCU, GSM Module, capacitive soil sensor LM35 temperature sensor, Humidity sensor, Motion sensor, after collecting all the desired information from the sensor it is transmitted to the IoT gateway, farmer will get notified through a SMS and the decision logic unit will decide the necessary action to be taken according to the data collected by the sensors and sent to the cloud web server and maintained in a database
3	Secure smart agriculture monitoring technique through isolation [21]	George Suciu, Cristiana-Ioana Istrate, Maria-Cristina Dițu	2019	Rain Gauge, Wind Speed and Direction, Temperature and Humidity, Pyranometer, Leaf Wetness	Raspberry Pi 3B+	In the proposed system farmers can get various information mainly regarding crop, soil and weather to monitor their crops. With the help of specific algorithms

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
						developed using python data sent to the cloud platform will be analyzed. Processed results will be sent back to the farmers to improve the agricultural process. This system will allow farmers to remotely access the irrigation system to their fields. Moreover, same device can be used to disaster management also. ADCON RTU is used for the transmission proposes
4	Smart Farming – IoT in Agriculture [22]	Rahul Dagar, Subhranil Som, Sunil Kumar Khatri	2018	Water Volume Sensor, Soil pH sensor, Soil Moisture Sensor, Air Temperature Sensor, Motion detector Sensor	ESP8266 Node MCU	IoT has so many useful applications in different domains of agriculture. In the proposed system authors provided a solution for the problems like wastage of water and electricity. Water flow sensor is used to control the irrigation to the fields moreover, the flow of the water can also be measured. Other issue they

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
						have addressed is insecticide, fertilizers and pesticides. In this paper authors have proposed greenhouse so they have claimed that use of greenhouse will reduce the outer interference of the insects and as they are using soil sensor, pH sensor all information is stored to a cloud which can further enhance the decision making power on the basis of data collected by the sensors
5	Design of IoT Blockchain Based Smart Agriculture for Enlightening Safety and Security [23]	M. Shyamala Devi, R. Suguna, Aparna Shashikant Joshi, Rupali Amit Bagate	2019	Temperature Sensor, Pressure Sensor, Illuminance Control, Wind speed, Air Control CO2, Pressure Control, Pollution Control Moisture Water Control, Smoke, Fire Control, PH Control Node		New architectural framework is introduced which is claimed to increase the performance of security and data transparency. Furthermore, authors are trying to enhance architecture to predict the performance of the parameters
6	Sensing and Visualization in Agriculture with Affordable	Takashi Okayasu, Andri Prima Nugroho, Daisaku Arita, Takashi	2017	SHT71 Sensirion Temperature humidity sensor, Solar radiation	Arduino Ethernet, Raspberry Pi	Several ICT systems related to sensing, visualizing and analysing for the

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
	Smart Devices [24]	Yoshinaga, Yoshiki Hashimoto, and Rin-ichiro Tachiguchi		sensor BH1603FVC, Soil moisture content sensor WD-3-W-5E, Night Vision Camera		advancement of agriculture has been introduced. System can make decision according to the farmers need according to the valuable information stored in SD Card. These developments can be improved according to farmers need, environmental factors and situations
7	Smart Irrigation: Towards Next Generation Agriculture [25]	A. Rabadiya Kinjal, B. Shivangi Patel and C. Chintan Bhatt	2017	Soil moisture sensor HL-01, HL-69	Node MCU	Proposed system is utilized when analysis of used water and irrigation cycle is required. According to the experimental results farmer can easily take decision to water his fields in a season
8	Low Cost Weather Station for Climate-Smart Agriculture [26]	Sonam Tenzin, Satetha Siyang, Theerapat Pobkrut, Teerakiat Kerdcharoen	2017	4 Cloud-based stations and 1 Davis Vantage Pro2	PIC24FJ64, Raspberry Pi	Authors have designed and installed the low-cost reliable microclimate weather station called Cloud-based station. Comparison has been made in between two installed weather stations which are cloud based stations and Davis vantage pro2 on the basis

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
						of their study they have shown that cloud based weather station is equivalently efficient to measure parameters like air temperature, relative humidity and wind direction in the end they have stated that cloud based weathers station will be more preferable on the basis of its cost
9	AgriSys: A Smart and Ubiquitous Controlled-Environment Agriculture System [27]	Aalaa Abdullah, Shahad Al Enazi and Issam Damaj	2016	Temperature, humidity, pH, soil moisture and thermocouple	Fuzzy Controller MIMO. Simulation on LabVIEW	Researchers have done Simulation using LabVIEW and proposed a system "AgriSys" The system has an easy-to-upgrade bank of inference rules to control the agricultural environment. Systems working is based on the input of several sensors like temperature, humidity & pH. The system provides high increase in the productivity
10	Smart Drip Irrigation System for sustainable Agriculture [28]	Kavianand G, Nivas V M, Kiruthika R, Lalitha S	2016	Temperature, humidity, moisture, soil pH and soil nitrogen sensor	ARM 9 Processor	The aim kept in mind by the authors is to design a fully automatic drip irrigation system

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
						using ARM microcontroller and GSM. Their system provides R-T feedback which is helpful in controlling the activities of the irrigation system effectively. Depending upon the moisture content system will automatically turn on and off. The system will provide the required information regarding th pH content of the soil moreover, they have used a soil nitrogen level sensor this will provide farmers information regarding the nitrogen level of the soil
11	A Model for Smart Agriculture Using IoT [29]	Prof. K. A. Patil, Prof. N. R. Kale	2016	Temperature and Relative Humidity, Light Intensity, Barometric Pressure, Proximity sensing and Buzzer Ubi-Sense mote (M)	WINGZ	In this paper a system is proposed which is agricultural model in integration with ICT. By using the proposed approach, received updated information allows the ranchers to receive the useful information

(*continued*)

Table 2. (*continued*)

Sr. No.	Title	Author	Year	Sensors Used	Microcontroller	Findings
						regarding weather, temperature, humidity, pressure
12	A Smart M2M Deployment to Control the Agriculture Irrigation [30]	Alberto Reche, Sandra Sendra, Juan R. Díaz, and Jaime Lloret	2015	Soil moisture sensor (VH400), soil temperature sensor (THERM200)	Arduino Board	A real deployment of a smart M2M system is done in this paper to have control on the agriculture irrigation, humidity and temperature Sensor are used as a function of the weather parameters and based on the smart algorithm developed by the authors, the system takes decision which one of the sprinkler should be enabled on and which one should be turned off. The system developed by the researchers from this paper allows ranchers to water their crops more effectively and reduces the water wastage

3.3 Potential Area of Applications of WSN and IoT in Agriculture

IoT basic component description is provided in Sect. 2 and it uncovers its extraordinary capacity of dealing with the applications of the agriculture and ongoing patterns of the PA (precision agriculture). Developed IoT devices are of low cost and tiny in size along with daily advancements in sensor technology has contributed in a great manner toward agriculture field [31]. Various types of sensors like radiation, pressure, wind, climate

stations, climate sensors, temperature & humidity sensors gives stress to the point that it is all about sensor and sensor information streams, which are deployed to the open environment for observations, sensing, thinking, learning mining, and controlling the devices according to the need. Additionally, recently, there is a growing enthusiasm for high gauge and safe rustic things. This example has yielded the prerequisite for interoperable, flowed, solid, and exact co-appointments conspicuousness structures. The IoT gathering of headways gives all the correct gadgets to building and keeping up such structure and organizations, uncommonly expected to help supply chains in cultivating and floricultural regions [32]. Wired and wireless sensor have been utilized for the agricultural applications in recent decade. Recognizing the earth wherein age occurs, and, even more starting late, the responses of the plants to the air is huge for taking the privilege and continuously accurate decisions, redesigning productivity and nature of the cultivars. The standard WSN have starting late progressed to IoT welcoming Wireless sensor frameworks, by grasping progressively ordinary measures with respect to correspondence, empowering remote access to the web and realizing wise counts for meta-treatment of the data significance to improve checking or conceivably control. Adaptable devices, with high computational limits, favorable structure factor and simplicity, would these days have the option to be used, on batteries, and work for huge parcels, with or without the assistance of force gathering modules. Likewise, at present introduced devices have sufficient resources for help all the more mentioning sensors, for instance, picture sensors, and the assistance of continuously propelled frameworks organization shows, such TCP/IP, growing the standard WSN arranging capacities. A terrible portrayal of composing on checking and control could be Monitoring and, at times, creation of early cautions, by methods for streamlined rules. This fuses multi-point checking for getting and immersing climatic slants in nursery advancement [33] Detecting is of high centrality in agriculture. WSNs have been commonly used in air and soil checking associations both in open field and in controlled condition cultivation. Controlled condition agribusiness Greenhouses have been seemed to show colossal climate vacillation, which impacts the proficiency of the plants. Nursery improvement is dynamically outrageous, in like manner, when in doubt, it requires higher exactness to the extent watching and control a few assessments have concentrated just on confined and remote checking. A great part of the time, data is taken care of and addressed in various graphical ways [32]. Despite the high-exactness checking, there have been studies presenting structures which circuit meta-getting ready strategies with data proceeded onward remote establishments through the web. Utilizing outstandingly surveyed conditions, yield and climate models, such structures produce assessments of the environment just as reap status all together for the cultivator to settle on better decisions or get early alarms [33].

3.4 Challenges in Smart Agriculture

Adoption, utility and applications [34] of WSN and IoT in agriculture is not without multitude of challenges and the requirement of addressing difficult research problems. Some of the challenges researchers may face during their research in smart agriculture are discussed in following subsections. These challenges may also act as future perspective for research in precision agriculture using WSN and IoT.

3.4.1 Data Analysis

Data science becomes the most important and popular field of research in computer science. Data analysis is very important in almost all of the applications of WSN and IoT. The decision made by the users, while applying WSN to certain applications, depend on the data collected by the sensors. The challenges in smart agriculture also include this problem [37]. The issue impose problem of integration of sensor nodes to analytic application which can further make decisions or drive automation activities. If integration is successful than it will be cost effective for the farmers and may contribute to increase the production.

3.4.2 Hardware Systems

WSN and IoT in smart agriculture faces many difficulties. The foremost problem is living the hardware in the open environment and expect it to work in harsh environmental conditions also. These harsh conditions may harm the normal embedded systems which expose it's electronic components to the open conditions like high sunlight based radiation, outrageous temperatures, downpour or high dampness, solid breezes, vibrations and different risk. These conditions may damage the electronic circuits inside the devices [38]. The end-gadget ought to stay dynamic and limit trustworthy for huge misfortunes relying upon the compelled influence resources of batteries. Along these lines, appropriate programming instruments and low-control capacities are required, since the progressive battery substitution or reset of the stations, for example in a large-scale open field course of action, isn't straightforward.

3.4.3 Security Issues

Like any other industry, ranchers need to think about security and safety of the technology used by him in proper manner. The PA concept brings the agribusiness into the risk of data theft and hacking. Moreover, ranchers do not have proper knowledge of data protection in this field [39]. Developers of IoT devices uses IoT devices to collect the information and data analysis to make agriculture practices more efficient. However, ranchers are still using traditional methods for agriculture which do not have data security concept.

3.4.4 Networking Challenges

Odd situations of the nature offer great difficulties to the equipment, and to the system layer. Remote communication is used in the field of agriculture to overcome the cost of the wires which are used in wired devices [40]. Nature is known to be one of the fundamental contemplations which lead to low remote association quality, through the multi-way multiplication effects and its promise to establishment uproar Real-world game plans, has shown that the presentation of standard handsets is affected by temperature sogginess human closeness and various preventions inside the space in which a remote center point attempts to pass on. According to this information collected by the sensor can be transferred with the utilizations of the powerful and dependable enhancement done in technological development as per the challenges and requirement of the rustic conditions [35].

Despite of above challenges nowadays, many manufacturers of farm gadgets provides complete solutions in integration with IoT devices. In their business it plays vital

role. As these Precision agriculture solutions provides ranchers a huge set of data to enhance their farming and knowledge by gathering real-time data. As these devices are this much important these devices should have capabilities for data storage, security, deep analytics and device management on the data received from the remote sensing techniques, on-field deployed sensors and images from drones. This will generate data to educate farmers and scientist with capabilities of better decision-making.

4 Conclusions

Internet of things involving agricultural machinery, can be utilized to manage standard farming fields, whereas ranchers still needs to play the role of both scientist and the person to keep an eye for unforeseen situations. Farmers can feel relaxed by investing in digitalization treatment of the plant diseases and monitoring the livestock. New ITC devices can be useful in tackling crop diseases and pest controls. As there is a lack of knowledge about these ITC devices in farmers. Agriculture industries still needs to convince ranchers towards the benefits of these technological advancements of IoTs. Internet of Things provides farmers a platform to exchange information and establish connections and cooperation's. This can further be important that they may develop an informal communication system which can play a vital role in advancing the formal communication system.

References

1. Chaudhary, D.D., Nayse, S.P., Waghmare, L.M.: Application of wireless sensor networks for green house parameters control in precision agriculture. Int. J. Wirel. Mob. Netw. **3**(1), 140–149 (2011)
2. El-kader, S.M.A., El-Basioni, B.M.M.: Precision farming solution in Egypt using the wireless sensor network technology. Egypt. Inform. J. **14**, 221–233 (2013)
3. Keshtgary, M., Deljoom, A.: An efficient wireless sensor network for precision agriculture. Can. J. Multimedia Wirel. Netw. **3**(1), 1–5 (2012)
4. Ahsan, A., Ahmed, B.: Identification of the type of agriculture suited for application of wireless sensor network. Russ. J. Agric. Socio-Econ. Sci. **12**(12), 19–36 (2012)
5. Botta, A., de Donato, W., Persico, V., Pescape, A.: Integration of cloud computing and internet of things: a survey. Future Gener. Comput. Syst. **56**, 684–700 (2014). https://doi.org/10.1016/j.future.2015.09.021
6. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013). https://doi.org/10.1016/j.future.2013.01.010
7. Edwards Murphy, F., Popovici, E., Whelan, P., Magno, M.: Development of a heterogeneous wireless sensor network for instrumentation and analysis of beehives. In: 2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp. 346–351 (2015). https://doi.org/10.1109/I2MTC.2015.7151292
8. Jayaraman, P.P., Palmer, D., Zaslavsky, A., Georgakopoulos, D.: Do-it-yourself digital agriculture applications with semantically enhanced IoT platform. In: 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 1–6 (2015). https://doi.org/10.1109/ISSNIP.2015.7106951

9. Barcelo-Ordinas, J.M., Chanet, J.P., Hou, K.-M., Garcia-Vidal, J.: A survey of wireless sensor technologies applied to precision agriculture. In: Precision Agriculture 13, pp 801–808 (2016)
10. Liu, Y., Wang, H., Wang, J., Qian, K., Kong, N., Wang, K., et al.: Enterprise-oriented IoT name service for agricultural product supply chain management. Int. J. Distrib. Sens. Netw. **11**(8), 1–12 (2015). https://doi.org/10.1155/2015/308165
11. Nageswara Rao, R., Sridhar, B.: IoT based smart crop-field monitoring and automation irrigation system. In: Proceedings of 2nd International Conference on Inventive Systems and Control. ICISC 2018, no. Icisc, pp. 478–483 (2018)
12. Suriyachai, P., Pansit, J.: Effective utilization of IoT for low-cost crop monitoring and automation. In: International Symposium on Wireless Personal Multimedia Communications WPMC, vol. 2018-November, pp. 246–251 (2019)
13. Rajalakshmi, P.: IOT based crop-field monitoring and irrigation automation. In: 2018 2nd International Conference on Inventive Systems and Control, no. Icisc, pp. 478–483 (2018)
14. Pandithurai, O., Aishwarya, S., Aparna, B., Kavitha, K.: Agro-tech: a digital model for monitoring soil and crops using internet of things (IOT). In: Proceedings of 3rd IEEE International Conference on Science Technology Engineering & Management. ICONSTEM 2017, vol. 2018-Janua, pp. 342–346 (2018)
15. Khan, S., Hussain, M.M.: IoT enabled plant sensing systems for small and large scale automated horticultural monitoring. In: IEEE 5th World Forum Internet Things, WF-IoT 2019 - Conference Proceedings, pp. 303–308 (2019)
16. Ghanshala, K.K., Chauhan, R., Joshi, R.C.: A novel framework for smart crop monitoring using internet of things (IOT). In: 1st International Conference on Secure Cyber Computing and Communication. ICSCCC 2018, pp. 62–67 (2019)
17. Sreekantha, D.K., Kavya, A.M.: Agricultural crop monitoring using IOT - a study. In: Proceedings of 2017 11th International Conference on Intelligent Systems and Control. ISCO 2017, pp. 134–139 (2017)
18. Tanmayee, P.: Rice crop monitoring system-A lot based machine vision approach. In: 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software. ICNETS2 2017, pp. 26–29 (2017)
19. Suma, M.R., Madhumathy, P.: Acquisition and mining of agricultural data using ubiquitous sensors with internet of things. In: International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol. 15. https://doi.org/10.1007/978-981-10-8681-6_24
20. Sushanth, G., Sujatha, S.: IOT based smart agriculture system. In: 2018 International Conference on Wireless Communications, Signal Processing and Networking. WiSPNET 2018, pp. 1–4 (2018)
21. Suciu, G., Istrate, C., Ditu, M.: Through isolation. In: 2019 Global IoT Summit, pp. 1–5 (2019)
22. Dagar, R., Som, S., Khatri, S.K.: Smart farming - IoT in agriculture. In: Proceedings of International Conference on Inventive Research in Computing Applications. ICIRCA 2018, no. Icirca, pp. 1052–1056 (2018)
23. Somani, A.K., Ramakrishna, S., Chaudhary, A., Choudhary, C., Agarwal, B.: Emerging Technologies in Computer Engineering: Microservices in Big Data Analytics, vol. 985. Springer, Singapore (2019)
24. Okayasu, T., Nugroho, A.P., Arita, D., Yoshinaga, T., Hashimoto, Y., Tachiguchi, R.: Sensing and visualization in agriculture with affordable smart devices. In: Smart Sensors IoT Frontier, pp. 1–378 (2017)

25. Rabadiya Kinjal, A., Shivangi Patel, B., Chintan Bhatt, C.: Smart irrigation: towards next generation agriculture. In: Internet of Things and Big Data Analytics Toward Next-Generation Intelligence, vol. 30, pp. 315–333. Springer (2018)
26. Tenzin, S., Siyang, S., Pobkrut, T., Kerdcharoen, T.: Low cost weather station for climate-smart agriculture. In: 2017 9th International Conference on Knowledge and Smart Technology Crunching Information of Everything. KST 2017, pp. 172–177 (2017)
27. Abdullah, A., Al Enazi, S., Damaj, I.: AgriSys: a smart and ubiquitous controlled-environment agriculture system, MAGRISYS: a smart and ubiquitous controlled-environment agriculture system. In: Proceedings of International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018, pp. 764–768 (2019)
28. Kavianand, G., Nivas, V.M., Kiruthika, R., Lalitha, S.: Smart drip irrigation system for sustainable agriculture. In: Proceedings of 2016 IEEE International Conference on Technological Innovations in ICT for Agriculture and Rural Development. TIAR 2016, no. Tiar, pp. 19–22 (2016)
29. Patil, K.A., Kale, N.R.: A model for smart agriculture using IOT. Int. J. Innov. Technol. Explor. Eng. **8**(6), 1656–1659 (2019)
30. Reche, A., Sendra, S., Díaz, J.R., Lloret, J.: A smart M2M deployment to control the agriculture irrigation. In: Ad-hoc Networks and Wireless: ADHOC-NOW 2014 International Workshops ETSD, MARSS, MWaoN, SecAN, SSPA, and WiSARN Benidorm, Spain, June 22–27, 2014 Revised Selected Papers. Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence), vol. 8629, pp. 139–151 (2015)
31. Katsoulas, N., Elvanidi, A., Ferentinos, K.P., Kacira, M., Bartzanas, T., Kittas, C.: Crop reflectance monitoring as a tool for water stress detection in greenhouses: a review. Biosyst. Eng. **151**, 374–398. https://doi.org/10.1016/j.biosystemseng.2016.10.003
32. Katsoulas, N., Ferentinos, K.P., Tzounis, A., Bartzanas, T., Kittas, C.: Spatially distributed greenhouse climate control based on wireless sensor network measurements. Acta Hortic. **1154**, 111–120 (2017). https://doi.org/10.17660/ActaHortic.2017.1154.15
33. Ferentinos, K.P., Katsoulas, N., Tzounis, A., Kittas, C., Bartzanas, T.: A climate control methodology based on wireless sensor networks in greenhouses. Acta Hortic. **1107**, 75–82. https://doi.org/10.17660/ActaHortic.2015.1107.9
34. Bonomi, F., Milito, R., Natarajan, P., Zhu, J:. Fog computing: a platform for internet of things and analytics. Studies in Computational Intelligence, vol. 546, pp. 169–186. https://doi.org/10.1007/978-3-319-05029-4_7
35. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015). https://doi.org/10.1016/j.comnet.2014.11.008
36. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
37. Kumar, N., Singh, Y., Singh, P.K.: Reputation-based energy efficient opportunistic routing for wireless sensor networks. J. Telecommun. Electron. Comput. Eng. **9**(3), 29–33 (2017)
38. Kumar, N., Singh, Y., Singh, P.K.: An energy efficient trust aware opportunistic routing protocol for wireless sensor network. Int. J. Inf. Syst. Model. Des. (IJISMD) **8**(2), 30–44 (2017)
39. Kumar, N., Singh, Y.: Trust and packet load balancing based secure opportunistic routing protocol for WSN. In: 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 463–467. IEEE, September 2017
40. Kumar, N., Singh, Y.: An energy efficient and trust management based opportunistic routing metric for wireless sensor networks. In: 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 611–616. IEEE, December 2016

Detection and Monitoring of Forest Fire Using Serial Communication and Wi-Fi Wireless Sensor Network

Harsh Deep Ahlawat(✉) and R. P. Chauhan(✉)

National Institute of Technology, Kurukshetra,
Kurukshetra 136119, Haryana, India
hda9009@gmail.com, chauhanrpc@gmail.com

Abstract. Enhancements in the communication technologies have led to the origin of Wireless Sensor Networks. They allow inter-transmission of the information with or without using the Internet facilities. The detection of forest fire is one of the crucial utilizations of WSN, and our matter of concern is to focus on the detection of fire and monitoring the transfer of information. In this regard, we design an efficient real-time setup which accumulates the information from various places, and uploads them on the remote web server. Through Wi-Fi, the information from numerous places having lack of Internet facility is transmitted to an intermediary server, and same is uploaded on the remote web server using the Internet. We employ NodeMCU micro-controller which has built-in ESP 8266 Wi-Fi module for establishing steadfast communication within the network. Moreover, we implement the proposed elucidation on the Arduino Integrated Development Environment (IDE).

Keywords: Wireless Sensor Network (WSN) · NodeMCU · ESP 8266 · Internet · Wireless fidelity (Wi-Fi) · Arduino IDE

1 Introduction

Wireless Sensor Networks (WSNs) represent a group of spatially dispersed autonomous sensors whose purpose is to collect the information, or to perform certain controlling tasks. These sensors are capable of detecting the physical phenomena, and continuously observe the physical conditions of the environment. The environmental information can be accumulated and delivered to the central location [1]. Each sensor node is affixed wirelessly to the cluster head so that communication can take place in a seamless manner [2], as shown in Fig. 1. Each sensor node contains a micro-controller, transceiver, and a battery source. The environmental parameters that are commonly measured includes temperature, humidity, smoke, gases, and so on. The node present inside a cluster transmits the sensor information wirelessly to the cluster head, and the cluster head delivers the same information wirelessly to the base station with and without using the Internet accessibilities. Furthermore, all the cluster areas can also be monitored from the base station [3].

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 464–492, 2020.
https://doi.org/10.1007/978-3-030-40305-8_23

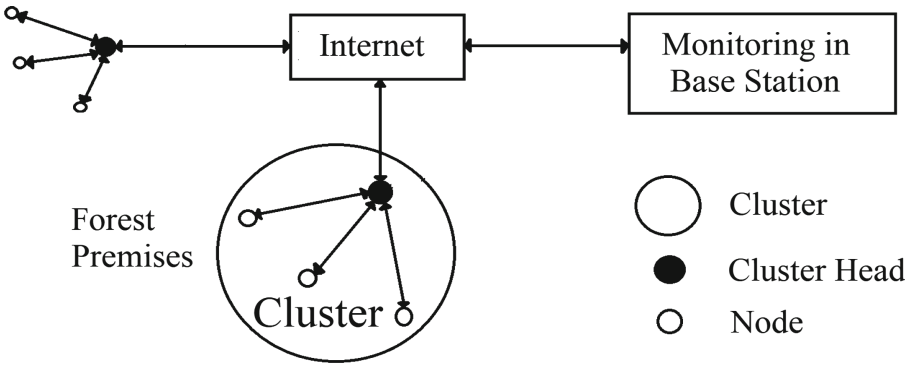


Fig. 1. The structure of WSNs for monitoring forest fire.

WSNs are mainly used for short-range and low data transmission rate with ultra-low power consumption [4]. The different types of wireless protocols are ZigBee, Wi-Fi (IEEE 802.11 b/g/n), etc. These protocols are used for specific purposes, and each protocol is having different characteristics to perform some task. Table 1 summaries some of the wireless technologies in terms of certain characteristics.

Table 1. Wireless sensor protocols characteristics.

Protocols	Data rates	Range	Power consumption
ZigBee	250 Kbps	100 m	Low
Wi-Fi	11 Mbps	100 m	High
Bluetooth	3 Mbps	10 m	Medium
RF	50 Kbps	50 m	Low

Now-a-days, WSNs are being used in multiple applications, such as area monitoring, natural disaster prevention and detection, healthcare monitoring, environmental monitoring, and so forth [5]. Forest fire detection is one of the crucial applications of WSN because it causes significant damage to the natural and human resources, if not detected in the early stages. The fire in the forest eradicates the infrastructure, and also affects human life. Some of the common causes include human carelessness, and fuel exposure to extreme heat and aridity. However, in plenty of cases, the damages caused by fire to the public safety and natural resources are extremely intolerable [6]. Therefore, an early stage detection of forest fires can be deemed crucial.

According to the forest survey of India (FSI), the frequency of detected forest fire in a particular area over a period of interval indicates proneness of the area to forest fires [7]. FSI determined the forest area under fire proneness classes, and thus provided the total number of forest fire points in the last thirteen years across the country. The grid size coverage of these forest fire points is 5 km $\times$ 5 km, and the frequency of forest fire points, in each grid, is determined by the frequency of forest fires points observed in the respective grid. Figure 2 shows the basic data of accumulated forest fire points that are detected by FSI in the last 13 years since 2004.

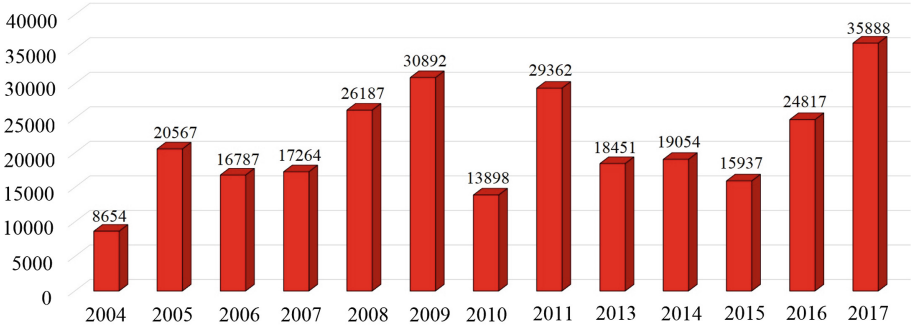


Fig. 2. Graphical representation of the total forest fires in thirteen years in India.

In the current scenario, various techniques are already available based on WSN which can detect and monitor the fire in the forest premises. Following are discussed below:

- In [8], wildfire detection using WSN data harvesting application has been discussed. Their work was based on network, hardware, and software architecture, and they have presented an algorithm on temperature variation-based fire detection system. They have used two types of nodes: sensor nodes, and cluster head. The communication occurred from sensor node to cluster head using ZigBee wireless links. Their result shows that when the wind blows from the fire, it carries heat energy due to which the temperature value rises very rapidly. Their observations were accurate for timely detecting wildfire with ambient temperature sensors.
- In [9], a hierarchical WSNs aim at early fire detection in risky areas, geographical information systems, integrated fire-fighting command centres, and fire simulators has been discussed. They have used two types of nodes, out of which one node SNs was used to collect data from the environment, and the other node CNs was used to gather data from the SNs, and the information was transmitted to the control centre by using WSN. In their work, the information was gathered to detect early fire, and data can be enrolled to fire-fighting for some preventive tasks. Their experiments for fire detection were perfect including rarest cases of false alarms.
- In [10], monitoring of field ecology and forest fire warning using a wireless system, IoT, and multi-sensor technology has been discussed. In their work, the design of monitoring network consists of several field ecological stations, a cloud server, and an online system software were used to monitor real-time data. Using logistic regression function, they have solved problems in quantitative scoring of the interval of fire weather indexes, and achieved a fine forecasting of fire weather grades. The success ratio of data transmission, they have obtained, through Beidou satellite were 98.57%, and through GPRS were 99.89%. Their system can be useful for big data monitoring of field ecology, meteorological disaster monitoring, etc.
- In [11], authors have presented a novel approach to detect the peat fire risk area using two methods which include, the impedance model, and the differential interferometric SAR technique. The SAR technique was based on the knowledge of

annual subsidence rate associated with the GWT. The work carried by using three layers of a new impedance model approach of soil roughness parameters as a layer between air and soil surface. Their result shows that DInSAR approach was successful in detecting fire risk area following groundwater table simulation. The correlation test results, they have provided, for pair A: 0.71, and for pair B: 0.85. Also, the impedance model gave significant results, and indications were based on high correlation coefficient.

- In [12], a real-time identification of different combustion phases using a developed ZigBee WSN based multi-sensor system and artificial neural network prediction model has been discussed. They have conducted an experiment using burning materials from residuals of forest to test responses of each node under no smouldering, smouldering-dominated, and flaming-dominated combustion conditions. The conducted test shows that the multiple sensor input provides an accuracy greater than 82.5%, and the single sensor input accuracy lies around 50.9%–92.5%. Moreover, based on their results, they have also proposed to reduce the cost with a relatively high fire identification rate.

In this paper, we introduce a newly launched micro-controller which is based on Wi-Fi protocol "NodeMCU". It is a low-cost implementation, and has a medium data rate transmission as compared to other protocols. The main advantage of NodeMCU is that we can either connect this device to the Internet, or we can create a new self-independent Wi-Fi server. However, the complexity of NodeMCU is high, but it is more suitable than other mentioned protocols. We demonstrate a test by making a cluster node of an area of approximately 5 hectares. Moreover, we configure NodeMCU devices as a server, routers, and clients. All the clients are connected either to the main server, or to the routers, and the flow of information executes from clients to server, or from clients to routers to servers.

The rest of the paper is organized as follows: Challenges during forest fire detection in real time scenario is discussed in Sect. 2, and related work is discussed in Sect. 3. Furthermore, Sect. 4 describes NodeMCU hardware containing built-in ESP8266 module, and interfacing of sensors we use in our model. Section 5 presents the real-time implementation of WSN along with its results and challenges faced during implementation of the system. Finally, Sect. 6 concludes the paper with future work.

2 Challenges During Forest Fire Detection in Real Time Scenario

For a successful forest fire detection system, the most critical and prominent issue is the immediate response and the early detection of the fire threats in order to reduce the scale of the disasters. However, fires in the forest increases very rapidly and exponentially. Thus, it is crucial that the forest fires must be interfered in the starting minutes before spreading [9]. Otherwise, once the fire is initiated, and starts spreading widely, it will be very difficult to control over it. Rather than depending upon unreliable watch towers, multiple techniques are already available, in the current scenario, that detect fires at early stages, and provides the accurate information of the environment.

These prominent techniques include satellite-based systems, WSNs, charge-coupled camera (CCD) and so on. However, in these recent technologies, the presence of multiple challenges still exists in the real time scenario due to which the early detection of forest fires is still lacking, and have no control over the widespread of fires. A few challenges are discussed below:

2.1 Satellite-Based System

The earth-orbiting satellites are enrolled for the detection and observation of the forest fires. In this system, the advanced very high-resolution radiometer (AVHRR), and the moderate resolution imaging radiometer (MODIS) are used. The images are collected from the satellite for the detection of forest fire. However, these satellites provide the images of the scanning surface of the earth over a long period of time which results in the failure of swiftness and effectiveness of the early forest fire detection system. Moreover, it is impossible for geostationary or low earth orbit (LEO) satellites to provide a full coverage of the forest premises. Moreover, the quality in terms of accuracy of the satellite images can be affected depending upon the weather conditions. Thus, for a good satellite-based forest fire detection system, satellites have to focus on a single forest which may be less suitable, and not possible due to various restrictions.

2.2 Wireless Sensor Networks

WSNs are an emerging technology which consists of a very small size, limited power, and low-cost devices, and they also have the capabilities of computing, sensing, and wireless communication. However, it can solve the line of sight and the early detection of forest fire problems, but there are several other challenges in WSNs that have to be rectified in the real time scenario. A few challenges of WSNs are discussed as follows.

Forecasting Capabilities. Predicting the forest fire is one of the important issues. However, fires in the forest spread very rapidly. Therefore, the mandatory requirement to control over the pervasiveness of forest fire is to perform some necessary actions and calculations for the forecasting of rapid-fire spreading direction. The node must be actively connected to the cluster-heads in the critical areas, and must transmit the information more frequently.

Power Consumption. It is a very critical task which is to be achieved in WSNs applications, especially, while monitoring the environmental information. During transmission of information in the form of packets, the sensor nodes consume more power that are kept at a distant place from the cluster-heads, i.e. the consumption of the battery depends upon the distance. The more is the distance, the more will be the consumption of the battery consumed by the sensor node during transmission mode and consumed by the cluster-heads during receiving mode.

Less Trivial Information. The omission of redundant information, and transmitting only the necessary and mandatory data to the cluster-heads are come under one of the challenging tasks in forest fire detection. This will not only prevent the unnecessary traffic throughout the network, but also aid in simplifying the data processing at the

cluster-heads. Moreover, during ignition of forest fire, rather than continuously transmitting temperature information and alert messages to the base station, the cluster heads make some evaluations. These evaluations investigate the received temperature and humidity information, and search for any threat, or any alert situation. The investigation can be done in multiple ways, like comparing of several values which are provided by the interfaced sensors at the sensor node, or the comparison of various values that are received by the cluster-head from numerous sensor nodes, and so on. Thus, if the compared values are equivalent to the alert values, only then cluster heads will deliver the information to the further wirelessly connected network coordinators, otherwise all the information must be dumped.

Prediction of Faulty Nodes. It is one of the mandatory challenges in detecting forest fires. There are some uncertainties that the connection between the parent node and the child nodes gets demolished, and no transmission of information will take place. In that particular situation, child nodes must find an alternative path to deliver the information to any other cluster-head, i.e. parent node.

Prediction of Shortest Path. It is another important challenge in the forest fire detection system. However, sensor nodes are wirelessly connected to cluster-heads, and cluster-heads are further connected to network coordinators. And finally, all network coordinators transmit the information to the base station. Therefore, to control the pervasiveness of fire in the forest, the information must be delivered from sensor nodes to the base station very quickly in a very short span of time. And, this can be done by predicting the shortest route from sensor node to the base station.

Cost and Maintenance. During the implementation of any devices, cost plays a vital role in the whole hardware setup. The cost includes the hardware parts, various varieties of interfaced sensors, batteries, and so forth. In a numerous quantity, the hardware setup must be deployed in various regions of the forest premises which detects the environment information, and transfer it to the base station. Thus, a huge amount of deployment of nodes increases the cost factor. Moreover, the drainage of source batteries, regular time-to-time maintenance like replacement of faulty sensors, faulty nodes, batteries, and so on are the other challenges after deployment of hardware in the forest premises.

2.3 Optical Sensors and Coupled Charged Devices Video-Surveillance

These techniques are generally used for the development of automated early recognition and early warning of the forest fires. These systems are installed on the top of the towers. Video-camera surveillance is used for smoke recognition, infrared (IR) is used for the detection of heat flow of the fire, IR spectrometers are used to identify the spectral characteristics of smoke, and LIDAR are used to measure the laser rays reflected from the smoke particles [13]. These cameras and detectors sense the environmental changes, and transmit information to the base station. In these systems, the accuracy is highly affected by weather conditions such as clouds, light reflections, and so on. Due to these weather conditions, the sight image may get disrupted, and a clear image cannot receive at the base station. Moreover, these systems can identify smoke

up to a range of 1 km, thus the identification of ignition of the forest fires at initial stage seems very difficult. Fires can be identified, using these systems, only when they are spread pervasively, and a huge amount of smoke is generated. Moreover, the cost of these systems is extremely high. Therefore, automatic video surveillance systems are not usually recommendable to a large forest field.

The above-mentioned technologies have their own advantages and disadvantages. However, it is not feasible to rely on unreliable technologies. Therefore, in Table 2, some comparisons on different technologies have been shown which aid in determining that relying on WSNs is better than relying on other technologies.

Table 2. Various comparisons in technologies.

Surveillance → / Comparisons ↓	Human-based	Satellite-based	Camera-based	WSNs
Implementation cost	Very low	Very high	High	Low
Detection efficiency	Low	Low	Medium	High
Detection accuracy	Low	Medium	Medium	High
Detection time	Very high	High	Medium	Low

3 Related Work

Numerous technologies based on WSNs are already available to detect and to monitor forest fires. The literature survey shows that the systems based on sensor networks, satellites, and various wireless systems which are already implemented. Some of them are discussed below.

Shi, Cao, et al. [14] presented a network that ensured a shorter response time and a better reliability from the edge computing perspectives. The smart objects represented a simpler network which were implemented. Though, cost is a major factor in their implementation, therefore it is not a useful approach.

Neumann, Almeida, Endler [15] presented on a smart forest fire detection modelling on Internet of Things. Their idea was based on mobile hubs, and the results were based on the scalability test using remote sensors. Their work provided a scope of using a low-cost Bluetooth protocol, and to transmit the data from sensors in the edge. However, the practical implementation of their work is still lacking.

Bhosle, Gavhane [16] expressed their work on the concept of forest disaster management using WSN. The proposal model was based on the technological solutions for managing disaster, and rescue operations. They have analyzed that if the fire is detected, in that scenario, the node receives all the information and transmit it to the nearest sink node. Moreover, the node compares the collected information with its predefined data. If the collected information is greater: transmit an emergency signal, otherwise sends a warning signal to the end user. This approach is comparatively unique; however, it is still lacking practical implementation.

Another system for forest fire detection is based on satellite imagery: MODIS [17]. It described the study of images taken from the satellites. However, in this system, the

weather conditions and the cloud layers are the main problems. The clouds absorb some parts of the frequency spectrum, and reduces the spectral resolution of the images which are taken from the satellite. Though, satellites can monitor a huge amount of forest area, but due to its long scanning cycle, high cost, and the poor resolution of the image, it is not useful in real time applications. Moreover, satellite can detect fires when it has been spread widely in a large quantity, otherwise it will be highly difficult to identify where the fire in the forest has inaugurated at some particular area.

Huh, Lee [18] presented their work on the concept of enhancement contextual forest fire detection with prediction interval analysis of surface temperature. They have proposed a method that uses a negative relation between vegetation amount and land surface temperature. Moreover, their analysis was based on the differences between the brightness temperature which was estimated from a regression model, and the vegetation amount which was measured by the normalized difference vegetation index. Their results were based on the improvement of the accuracy and precision accuracy using contextual algorithm, but the practical existence does not exist.

Chakraborty, Banerjee, et al. [19] presented on the time varying modelling of land cover change dynamics due to forest fires. They have proposed a model to capture the time varying changes in the vegetation growth cycle, and detected abrupt changes in land cover due to forest fires. Furthermore, they have designed a sequential Monte Carlo estimation approach of the time varying frequency for non-linear model using the particle filter, and proposed a binary hypothesis land cover change detector. Though, their proposed model shows the valid results over different geographic locations, and provides spatial scalability, but there is no practical implementation.

Marchese, Mazzeo, et al. [20] presented on the issues and possible improvements in winter fire detection by satellite radiance. They have proposed a study based on the investigation of winter fire regimes characterizing the aforementioned regions using AVHRR and MODIS data. They have worked on self-adaptive algorithm which compare RST fires and MOD14/MYD14 fire detection products in order to assess their performance in the detection of winter fire. Their study focused on the investigation issues affecting satellite monitoring by encouraging the usage of multiplatform observing system, integrating data provided by the spinning enhanced visible, and infrared imager abroad MSG satellites for better supporting fire management activities.

Dhief, Sabri, et al. [21] expressed a review of forest fire surveillance technologies: mobile ad-hoc network routing protocols perspective. They have identified and reviewed on the modern techniques which are used in the forest fire detection based on MANET routing protocols such as reactive location aided routing, proactive optimized link state routing, and LAR-based reliable routing protocol. Their analysis shows that the performance of LAR protocol as an excellent contribution for the detection of fire in terms of routing criteria, information energy, route busyness, and so on. Moreover, LAR shows high positivity in terms of performance metrics except in E2E delay. And, finally, they have showed that the data required to be transmitted in a faster manner as compared to the reactive routing protocol.

Yuan, Lie, Zhang [22] presented on an aerial images-based forest fire detection for firefighting using optical remote sensing techniques and unmanned aerial vehicles. Their work proposed a vision-based forest fire detection approach using color and motion features for the processing images captured from the camera mounted on a

UAV which was moving during the whole mission period. They have used a color-based fire detection algorithm with light computational demand to extract fire-colored pixels by making use of chromatic feature of fire, and obtained fire candidate regions for further analysis. Moreover, they have used two types of optical flow algorithms: a classical optical flow algorithm, and an optimal mass transport optical flow algorithm, and both were combined to compute motion vectors of the fire candidate regions. Their results signify the enhanced reliability, accuracy of forest fire detection, and also reduces false alarm rates.

Polivka, Wang, et al. [23] presented on improving nocturnal fire detection with the VIIRS da-night band. They have expressed their work on the existing techniques for satellite remote sensing of fires, and took advantages of DNB aboard the VIIRS to develop the firelight detection algorithm. FILDA improved detections of fire pixel selection with smaller and cooler subpixel hotspots. FILDA, they showed, to be effective in detecting flares, and characterizing fire lines during large forest fires. Moreover, VIIRS fire product algorithm included a modified candidate fire pixel selection approach from FILDA which lowered the 4 μm brightness temperature threshold. Their algorithm results show a large increase in the number of detected fire pixels that could be verified with the finer resolution ASTER data. Moreover, they showed that quantitative use of DNB was to improve fire detection that could lead to reduced response times to wildfires, and better estimate of fire characteristics at night.

Leal, Hirakawa, Pereira [24] presented onboard fuzzy logic approach to active fire detection in Brazilian Amazon forest. Their work presented on the nature of data in the onboard processing, the variables in the environment, and fuzzy logic which was suitable for the process of recognizing the patterns in the data. They have showed that the noise of the images acquired by the sensors could be mitigated by the functions of variables, and the outcomes were optimized when compared to the algorithm which was used in ground stations. The fuzzy system, as they have described, was to handle the errors produced by the lack of information of some variables and of the general conditions of an embedded system. Their test results were an improvement in the hit rate as compared with the same image which was analyzed by Setzer's algorithm.

Castro, Gil, et al. [25] presented on the forest fire prevention, detection, and fighting based on fuzzy logic, and wireless sensor networks. They have described a proposal that focused on the short-term estimation of forest fire controller based on fuzzy logic, and decision-making methods. The environmental monitoring of various dynamic risk factors was to performed with WSNs and IoT technologies, and analyzed with the fuzzy-based controller. The polluting gases and the oxygen level were measured to estimate the existence of fire risks in the short-term, and to detect occurrence of out-breaks. However, the proposal is unique, but there is no practical existence of this approach.

In the context of the above studies, we propose our work which is based on real-time implementation using NodeMCU micro-controller, as it provides a complete and self-contained Wi-Fi networking system. It can be used to offload Wi-Fi networking function. Furthermore, the practical implementation of this device can overcome a few other mentioned methods in detecting forest fires by transmitting the environmental data at the base station.

4 NodeMCU and Its Specifications

NodeMCU is an open based IoT platform which has built-in Wi-Fi chip on the system that runs on the ESP 8266 [26, 27]. The ESP 8266 is built-in SoC (System on Chip) with full integrated TCP/UDP/IP stack networking protocol [28–30]. It has capabilities to connect either to the Internet services, or independently, it can host a server-client network. The prominent factor of this device is its modes of operation. The device can be configured either as a client, or as a server, or it can be used as a transceiver mode to communicate with other devices [29, 31]. The following are some specifications of ESP 8266:

Sleeping Modes. In ESP8266, there are three types of sleeping modes: light sleep, modem sleep, and deep sleep. These three sleeping modes are used for various purposes, and have different functions. However, light sleep and modem sleep are almost equivalent, as they both turned off the system clock, and also suspend the internal CPU. They both awake automatically, thus we do not require to configure both of them externally [26]. The most prominent is deep sleep mode because in this mode, all the parameters turned off, except real time clock (RTC). The differences in these types of sleeping modes are described in Table 3.

Table 3. ESP 8266 module features.

System parameters	Sleeping modes		
	Light	Modem	Deep
Wi-Fi	Off	Off	Off
System clock	Off	On	Off
RTC	On	On	On
CPU	Pending	On	Off

In this paper, deep sleep mode has been used, and the key factor which is to be considered here is that the deep sleep mode cannot enter into sleep by itself, as we have to configure it externally via coding. Similarly, to wake the device, an additional low pulse signal is required which is provided from GPIO 16 pin to the RST pin of the NodeMCU so that the device can reset itself, and starts the process once again.

Received Signal Strength. The received signal strength indicator (RSSI) is the measurement of the power available in the client. If multiple servers are present, the client use to connect to that server which is having the strongest signals, and rest of the server signals will be renounced [32]. RSSI value is measured in decibels or dBm, and the logarithm range lies from 0 dBm to −110 dBm. The closer value to 0 dBm indicates strongest signal, and weaker signal represents farther values.

Auto-Connect. It is an ESP 8266 Arduino library which helps in connecting servers at runtime without writing hard-coded SSID and password again [26]. If the connection of the client gets disconnected to the server, it is used to connect to the same server once again. The client consumes a few seconds for re-connection; however, the

authentication data of the connected server will be already saved in the memory of NodeMCU automatically.

The interfacing of multiple sensors is done with the micro-controller so that all sensor nodes have capabilities to sense various environmental parameters. Here, we have considered two parameters, i.e. temperature and humidity, as shown in Fig. 3. However, LM35 provides analog output data, thus it is interfaced with Analog pin A0, and DHT 11 provides digital output data, thus it can be interfaced with any of the digital IO pins D0-D8 [33]. Though, D0 or GPIO 16 pin connects with reset pin to wake-up the controller from sleep mode [34]. Therefore, we have interfaced DHT 11 with D2 pin. This interfacing is done with each and every router and client, we have initiated.

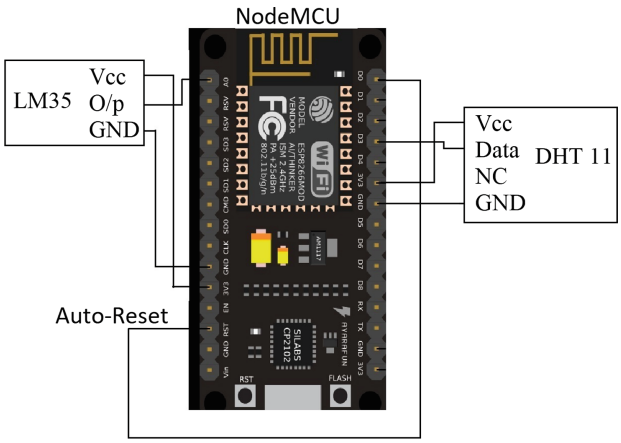


Fig. 3. Layout connection diagram of NodeMCU micro-controller.

5 Implementation and Results

NodeMCU micro-controller devices are implemented in three logical types of nodes: server, routers, and clients. The devices which deliver the sensor information is termed as client, the devices which collect the information is termed as server, and the devices which collect the information and deliver the same again is termed as routers. The target is to deliver the sensor information in the network without using the Internet facilities. However, Internet connection is mandatory for uploading the information on the web server. Thus, a separate client is interfaced serially with the server that collects all the information from the server, and uploads the same on the Internet.

5.1 One-to-One Communication

In this communication setup, information is transmitted by all the clients which are wirelessly connected to the server with a specific IP address. Moreover, this IP address has a unique SSID and a password which is accepted by all the connected clients,

except one client which is interfaced serially. Clients 1, 2, and 3 transmit the information, and the server receives it. This communication within a network is known as one-to-one, or single server-multiple client communication as shown in Fig. 4.

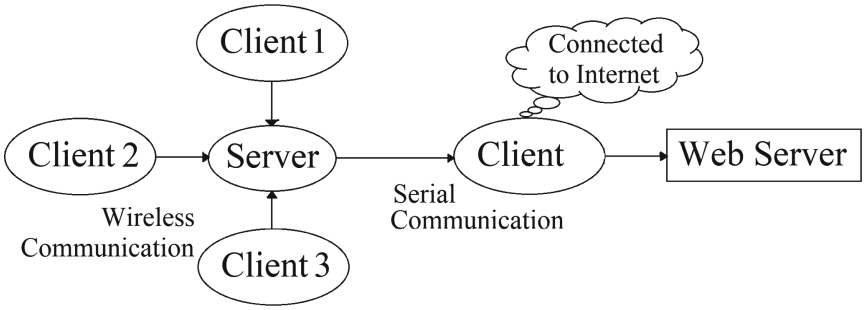


Fig. 4. Flow of information in single server - multiple clients communication.

Here, we have implemented four clients and one server. Three clients are connected wirelessly to the server, and the fourth client interfaced serially with the same server. The server initiates its own SSID – "HDA" with an IP Address – "192.168.4.1". When the server is established, and it stays in idle state until any client gets connected to it. On the other hand, all the clients are also initialized. The moment when the stationary mode of clients 1, 2, and 3 are initialized, they start searching for the server's SSID, i.e. HDA.

Clients 1–3 are interfaced with temperature and humidity sensors, i.e. LM35 and DHT 11, respectively, and the purpose of these sensors is to collect the environmental parameters. For the fire detection, we have provided some threshold values so that temperature and humidity are taken into contemplation, and surveys can be conducted. If the sensed value satisfies the provided threshold values, i.e. (i) temperature increases beyond 55 °C, and (ii) humidity decreases below 25; clients 1, 2, 3 start transmitting the information to the server. Simultaneously, the server also starts receiving the information automatically, and also forwarding the same to the serially interfaced client. Though, the interfaced client is connected to the Internet, it uploads all the received information on the web server. A flow diagram is shown in Fig. 5.

To maintain the steadfast communication between server and clients 1, 2, and 3, all the devices must have an equivalent port number – "9000", and a similar IP address – "192.168.4.1". This is done so as to maintain the systematic flow of information from clients to the server. To analyze the fire detection, restrictions provided in the form of threshold values must be satisfied. And for the reliable transmission of information, the sensor values must cross the provided threshold values. The instant when the conditions gets valid, information will be transmitted to the server, otherwise no flow of information will take place. The monitoring of the transmitted and received information on the serial monitor is shown in Fig. 6.

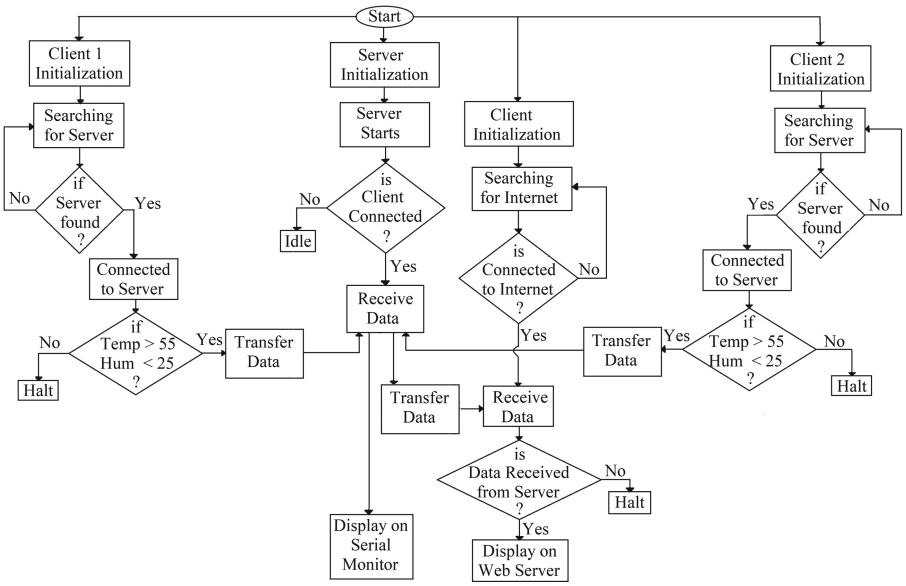


Fig. 5. Flow diagram of single server - multiple clients communication.

In Fig. 6, the canonical monitoring and transmission of environmental information is described, as discussed in Fig. 4. During the initialization period, all clients willingly to be in-searching mode until server signals aren't found. The moment when all the clients get connected successfully to the server, a string - the SSID is connected with: the name of the server and the signal strength of the server is printed on the serial monitor, COM 8, 9 and 10, of Arduino IDE. After the successful establishment of the connection, all clients are inclined to transmit the collected information from the interfaced sensors to the wirelessly connected server. However, transmission won't occur because of the provided threshold values at the client side. During the initiation

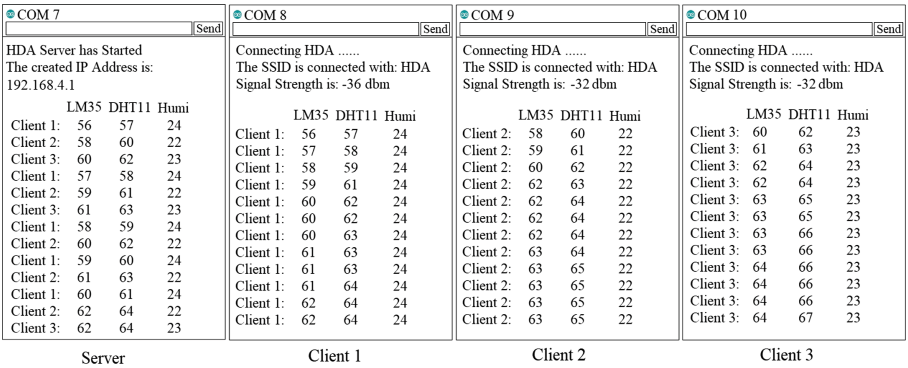


Fig. 6. Monitoring of sensor data on the serial monitor of Arduino IDE.

of fire when the temperature level and the humidity level varies, and at par restrictions, as described above, clients initiated the transmission flow to the server. Client 1 begins to transmit the information, in continuation, client 2, and client 3, simultaneously, also begin to proceed the collected information to the server. Hence, all the collected information is displayed on the server's serial monitor, i.e. at COM 7.

The sensors which are interfaced with every client collects the information at every single minute, and deliver it to the server. Figure 7 shows the graphical representation of the sensor data from all the clients. The three various representations of 2-D graphs denote the values of temperature and humidity at y-axis, and x-axis denotes the time duration in minutes.

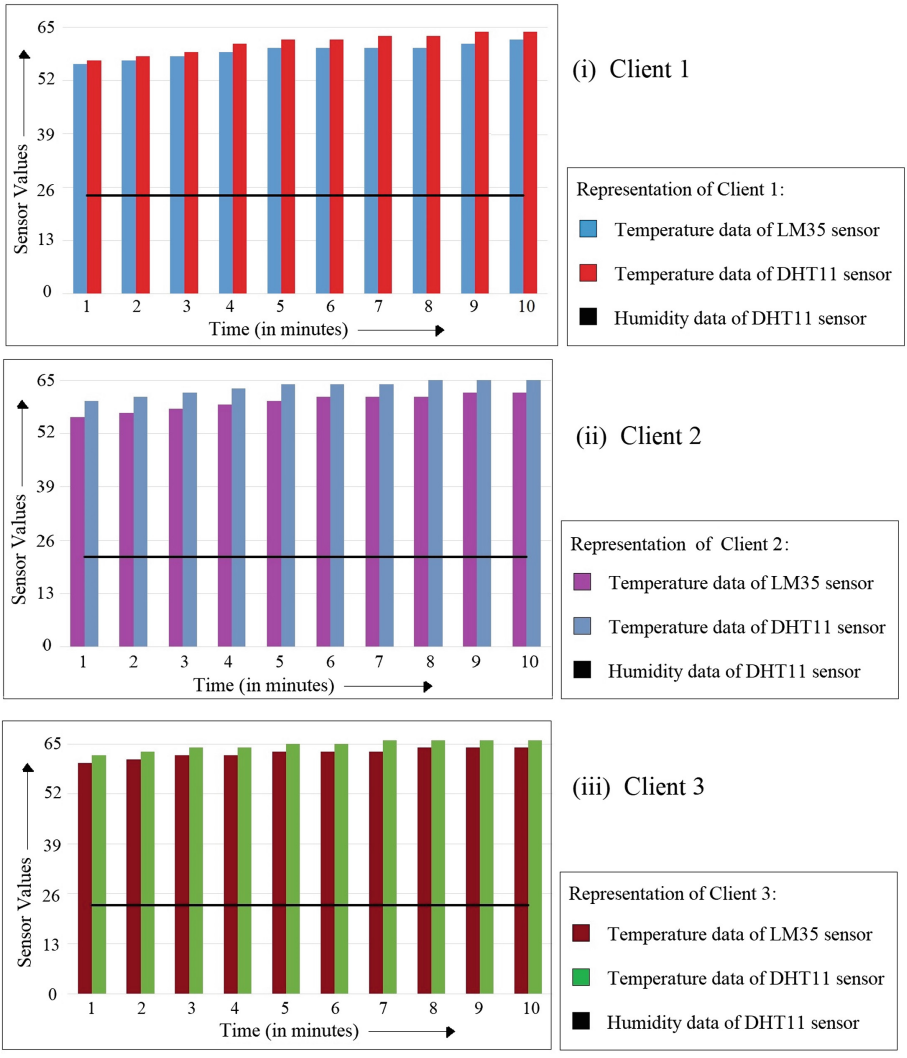


Fig. 7. Graphical representation of sensor data in one-to-one communication.

The range of the server can reach up to a distance of 40 m, and exceeding this range will lead to the loss of information. Thus, for the establishment of a proper communication, all the clients must be available within the provided range of the server so that the information can be delivered reliably and efficiently at the destination point. Moreover, the time of arrival of an information to reach to the server is less than a second. It means that when an information is departure from any client, it reaches to the server within a second. However, the loss of information may occur due the presence of physical hindrance, but it is very negligible. Using this mode of communication, out of 1000 transmitted information 947 have been received by the server simultaneously. This indicates that the accuracy of one-to-one communication is $94 \pm 3\%$. This accuracy has been analyzed when all the clients are deployed at the range of 30 m from the server, and connection are established properly. In case of any corruption in the server's signal, clients will not deliver any information to the server.

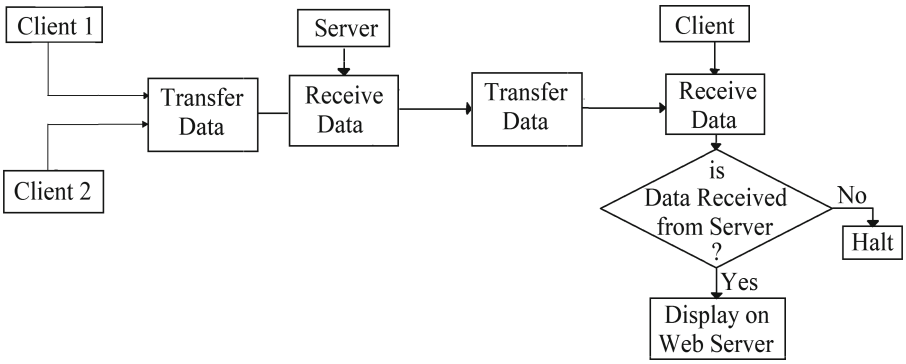


Fig. 8. Flow diagram of uploading the received information on web server.

In Fig. 8, uploading of received information from client 1 and client 2 on the web server has shown. When the information from connected clients 1 and 2 received by the server, the server again transmits the same collected information to the connected client. After receiving the information, the server starts forwarding the same information to the serially interfaced client sequentially. Moreover, we have provided the Internet facility with an IP address of "192.168.43.10" so that the interfaced client can be connected to the Internet. And, it can access the Internet data so that all the received information from the server can be uploaded on the web server, as shown in Fig. 9.

For this implementation, we have used the Arduino IDE software for the coding purpose. Using IDE software, we able to monitor all the transmitted and received information on the serial monitor of the IDE through ports COM 7, 8, 9, and 10. COM 7 represents received information by the server, and COM 8, 9, 10 represents transmitted information from clients 1, 2 and 3 respectively, and COM 11 represents uploaded information on the web server by the interfaced client.

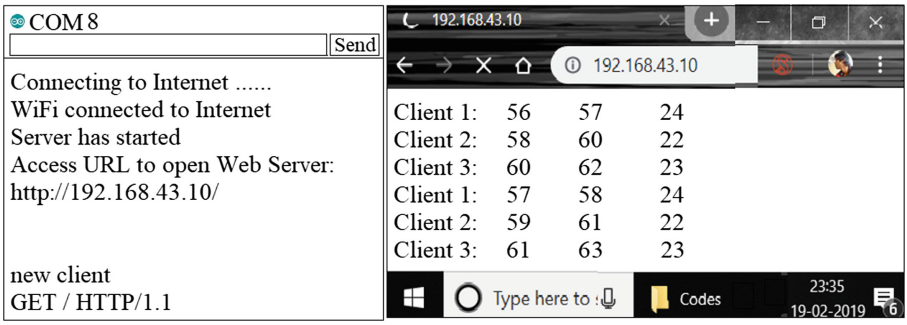


Fig. 9. Creating a web server, and uploading received information on the web server.

5.2 Many-to-One Communication

In this communication setup also, information is deliberately transmitted by all the wirelessly connected clients to the server which are having a specific IP address. In addition, server as well as routers contain a unique SSID and a password which is accepted by all the connected clients, except one client which is interfaced serially. Clients 3 and 4 deliver the information and the routers 1 and 2 collect it.

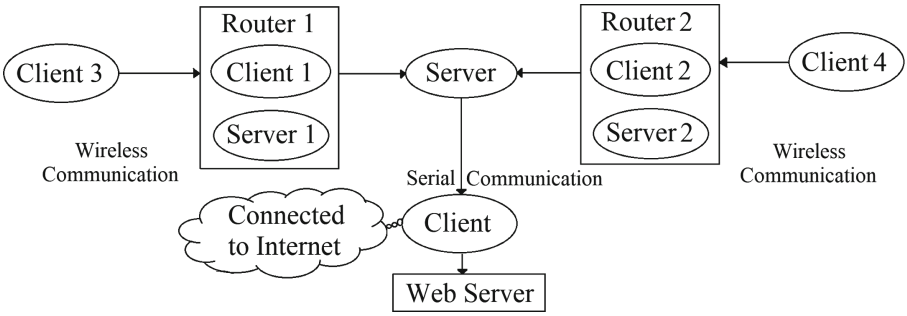


Fig. 10. Flow of information in multiple servers - multiple clients communication.

The collected information by the routers are re-transmitted to the server, and this communication within a network is known as multiple servers-multiple client communication or many-to-one communication, as shown in Fig. 10.

Here, we have implemented three clients, two routers, and one server. Clients 3, 4 are connected wirelessly to the routers 1, 2, and sequentially, the routers 1, 2 are connected wirelessly to the server, and the third client is interfaced serially with the same server. The server initiates its own SSID – "HDA", and the routers (when acting as a server, after connecting with the main server) initiates its own SSID – "HDA1" and "HDA2" for router 1 and router 2, respectively. All initiated servers are having a similar IP address – "192.168.4.2". When the server is established, it stays in idle state until any client gets connected to it. Simultaneously, all clients and routers are also

initialized. The moment when stationary mode of routers 1, 2 are initialized, they start searching for the server's SSID. And if found, both the routers get connected to the server, and creates an independent server so that clients 3, 4 get connected to the routers. Client 3 gets connected to router 1, and client 4 gets connected to router 2.

Clients 3 and 4, and routers 1 and 2, all are interfaced with temperature and humidity sensors. Here also, we have provided threshold values for the detection of fire. If the sensed value satisfies the threshold values, i.e. (i) temperature increases beyond 55 °C, and (ii) humidity decreases below 25; clients 3, 4 start transmitting the environmental information to the routers 1, 2, respectively. Moreover, the routers 1, 2 also start receiving the information, and simultaneously, re-transmitting the same including their own information to the server. Once the server receives all the information from both routers, it again forwards the same information to the serially connected client so that all the received information by the server can be uploaded on the web server. A flow diagram is shown in Fig. 11.

Clients communicate with the server through a network service provided by the transport layer. The transport layer we have used here is transmission control protocol (TCP), and it can either be used through Internet services or in stand-alone private networks [35]. To initiate the communication, clients 3, 4 must know the IP Address and the port number of the server, otherwise clients may get connected with the server but due to a different communication channel, i.e. the specific port number and the IP address, the information will not be transmitted. The monitoring of transmitted and received information on the serial monitor is shown in Fig. 12.

In Fig. 12, the canonical monitoring and transmission of environmental information is shown, as described in Fig. 10. During the initialization period, all clients willingly to be in-searching mode until server signals aren't found. The moment when both clients get connected successfully to the router's server, a string - the SSID is connected with: the name of the server and the signal strength of the server gets printed on the serial monitor, COM 8 and 9, of Arduino IDE. Similarly, routers (when acting as clients) get connected to the server signals, and displayed a string indicating the name of the server and the strength of the signal on the serial monitor, COM 6 and 7, of Arduino IDE. Once the establishment of the connection is done successfully, all clients are ready to transmit the collected information from the interfaced sensors to the wirelessly connected routers, and likewise, routers transmit information to the server. However, transmission won't occur because of the provided threshold values, as described above, at the transmission side. During the initiation of fire, the temperature level and the humidity level varies, and at par restrictions, both the clients initiated the transmission flow to the routers, and the routers initiated the flow to the server. It means that clients 3, 4 begins to transmit the information to routers 1 and 2, and simultaneously, routers 1 and 2 also proceed the collected information to the server including their own information (when acting as clients). Hence, all the collected information is displayed on the server's serial monitor, i.e. at COM 7.

The sensors which are interfaced with every client and routers provide the information at every minute, and deliver it to the server. Figure 13 shows the graphical representation of the sensor information from all the routers and clients. The four various representations of 2-D graphs denote the values of temperature and humidity at y-axis, and x-axis denotes the time duration in minutes.

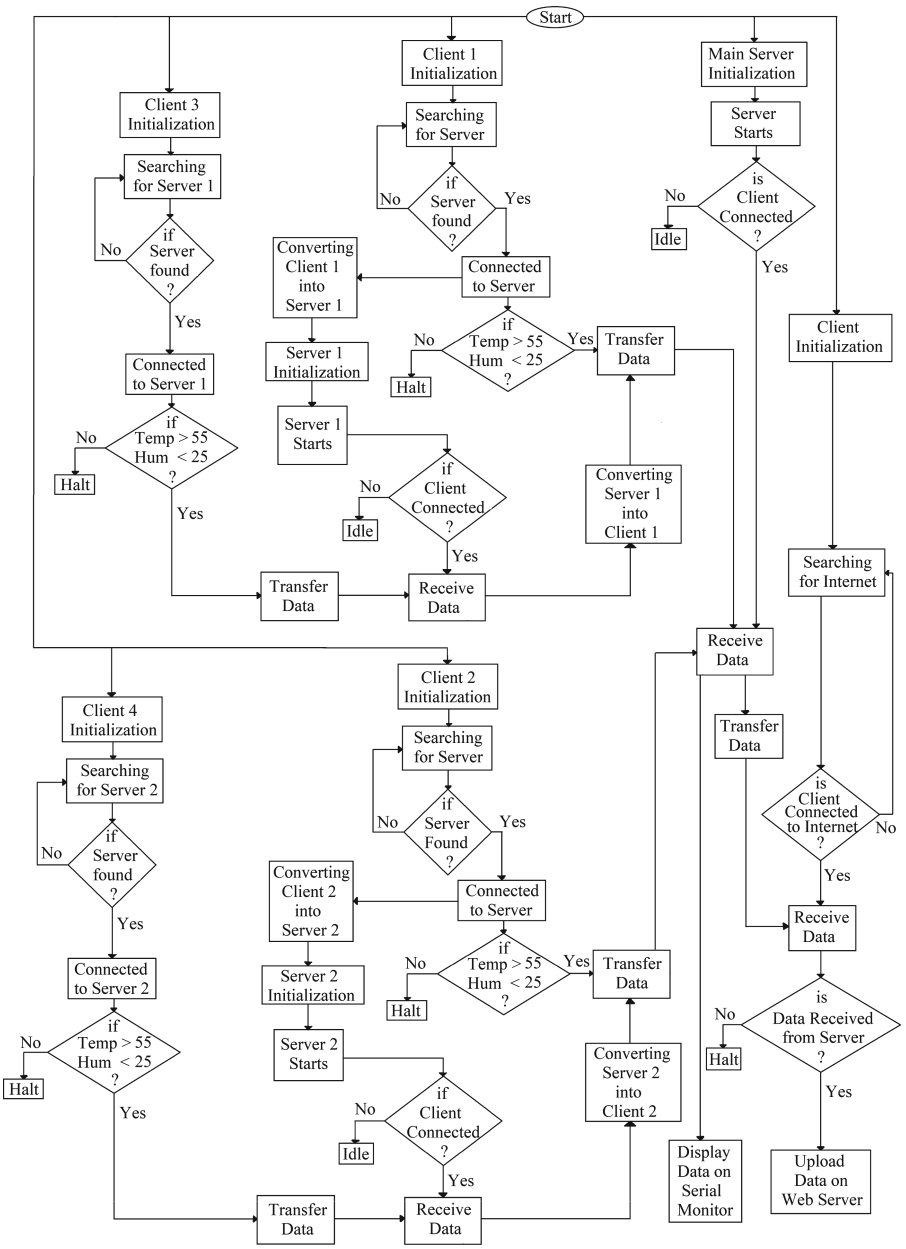


Fig. 11. Flow diagram of multiple servers - multiple clients communication.

In addition, the range of the server can reach up to a distance of 40 m, and exceeding this range will lead to the loss of information. Thus, we have covered a total distance of 120 m by connecting two routers horizontally. For the establishment of a

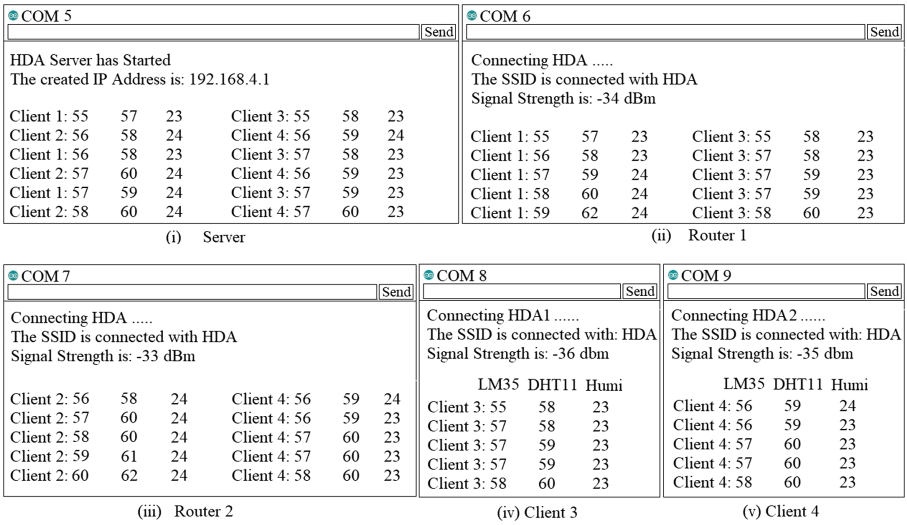


Fig. 12. Monitoring of sensor data on the serial monitor of Arduino IDE.

proper communication, all clients must be available within the provided range of the router's server signal, and routers must be available within the provided range of the server's signal. This is done so that the information can be delivered reliably and efficiently at the destination point. Here also, the time of arrival of an information to reach at the destination point from the source point is less than a second. It means that when an information is departure from any client, it reaches to the server via routers within a second. Using this mode of communication, out of 1000 transmitted information 921 have been collected by the server simultaneously. Thus, the accuracy of many-to-one communication is $92 \pm 3\%$. This accuracy has been analyzed when clients are horizontally deployed opposite to each other at the range of 30 m from the routers, and routers are horizontally deployed opposite to each other at the range of 30 m from the server. In case of any corruption in the server's signal or the router's signals, the flow of information will not be established.

After receiving information from both the routers, the server starts forwarding the received information to the serially interfaced client, sequentially. Moreover, we have provided Internet facility with an IP address of "192.168.43.10" so that the client can be connected to the Internet, and able to access the Internet data. Thus, all the information received by the server can be uploaded on the web server. Using the IDE software, we able to monitor all the transmitted and received information on the serial monitor of IDE through ports COM 5, 6, 7, 8, and 9. COM 5 represents collected information by the server, and COM 6, 7 represents collected information by the routers including their own information, and COM 8, 9 represents the transmitted information from clients 3 and 4. And finally, COM 11 represents uploaded information on the web server by the interfaced client, as shown in Fig. 14.

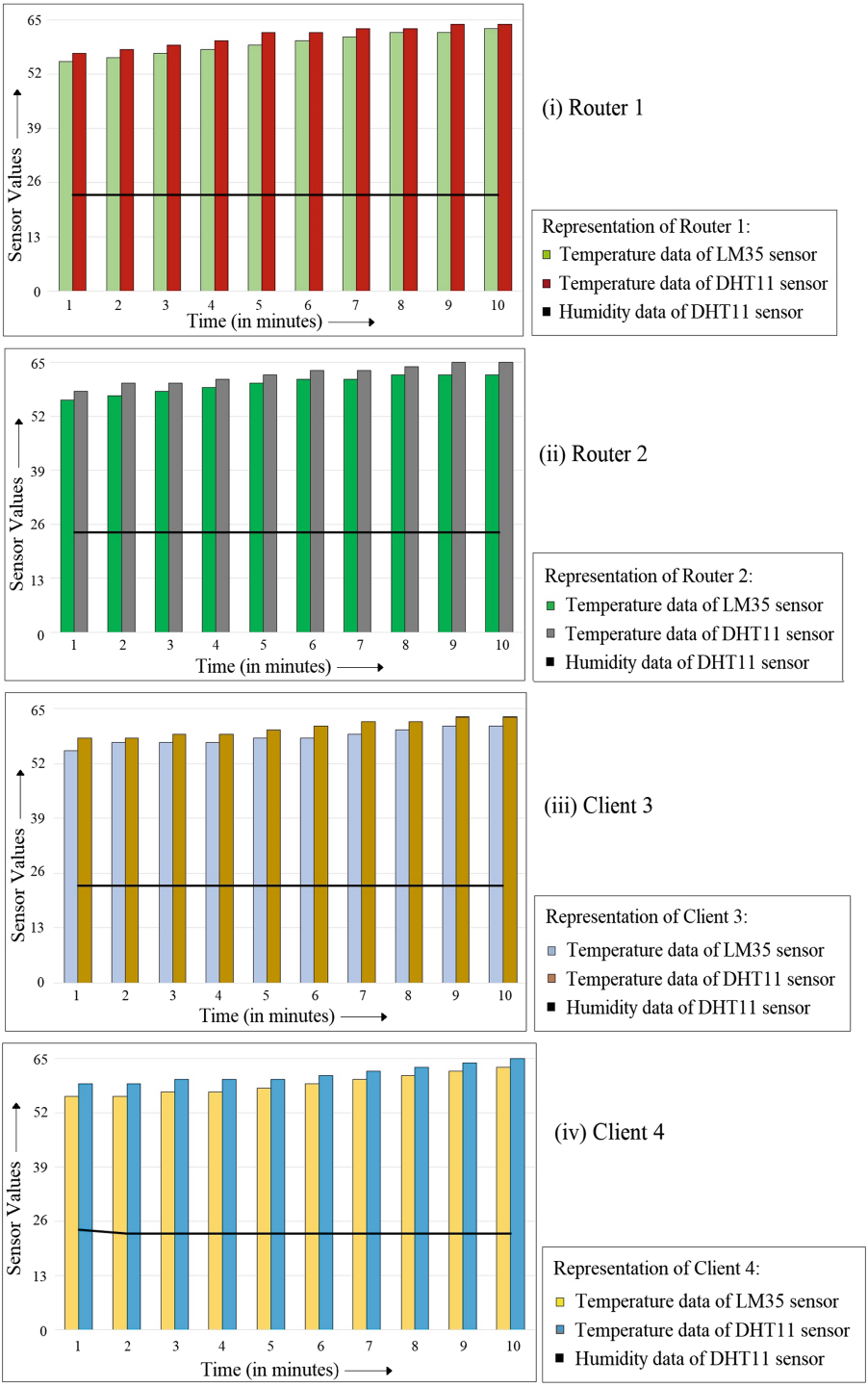


Fig. 13. Graphical representation of the sensor data in many-to-one communication.

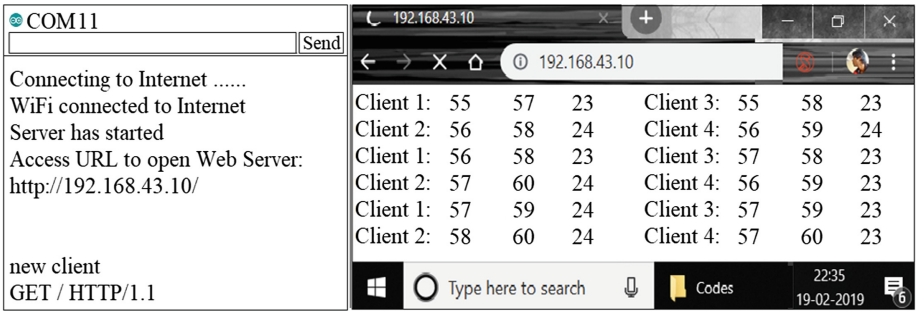


Fig. 14. Creating a web server, and uploading received information on the web server.

5.3 Challenges During the Implementation of the Forest Fire System

During implementation of one-to-one, or many-to-communication, a few issues have been occurred, which are needed to be care of. The challenges are discussed as following.

Perplexity of Wireless Communication. In many-to-one communication, when all clients are properly connected to routers, and routers are further connected to the server, there may generation of some circumstances that the information transmitted by the client 3 can be received by the router 2, and the information transmitted by the client 4 can be received by the router 1. Likewise, the information transmitted by the router 1 can be received by the router 2, and vice-a-versa. This may happen due to improper deployment of nodes, i.e. clients 3 are deployed nearer to the range of server 2, and clients 4 are deployed nearer to the range of server 1. Therefore, to prevent this muddling of communication, routers 1 and 2 should be kept opposite to each other so that their ranges can be unreachable. In the same manner, clients are also deployed in such a way they unable to detect other server's signals.

Connectivity Issues. In both modes of communication, in rare cases, clients are unable to connect to the server's signals which results in connectivity problem between clients and the server. During this issue, clients bide in searching mode even in the availability of server's signals. Thus, devices require a reset so that they can re-start its processing again. Therefore, to solve this issue, we have short-circuited GPIO 0 pin with RST pin of NodeMCU micro-controller. Moreover, we have provided a condition that if, somehow, any client fails to connect to the server within an interval of 10 s; devices will reset themselves, and re-starts the processing from the initialization.

Uploading Information on Web Server. During communication, server receives all the information from the connected clients, and it further uploads the received information to the web server. The issue that occurred here are: a constant refreshing of page

is required for the visibility of any new uploaded information. Moreover, the uploaded information on the web server is volatile. Once the Internet gets disrupted, all the uploaded information will be disappeared.

5.4 Reliability of the Implementation of the Forest Fire System

We have conducted an experiment to check the reliability of the system. The devices started transmitting the information to the server starting from 9 am for 5 min, and went back to sleep for 55 min. Again, the devices woke up at 10 am, transmitted the information for 5 min, and went back to sleep for 55 min. This periodical process continued till 8.05 pm, as shown in Fig. 15. Here, we didn't provide any thresholds during transmission. Moreover, the sensed temperature values provided by the interfaced sensors are then compared with the Internet provided temperature data. Thus, an error in the sensing values can be detected.

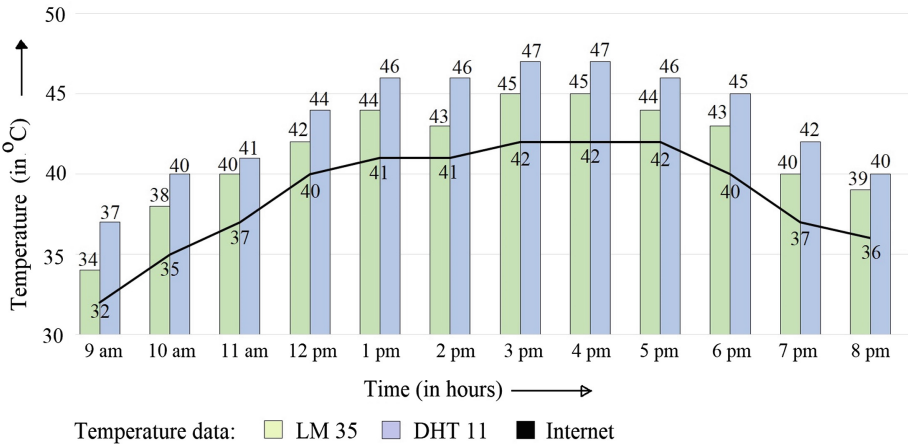


Fig. 15. Hourly temperature data provided by the sensors and the Internet.

From Fig. 15, we can identify the error between the Internet provided values and the interfaced sensor values. Thus, an average deviation in LM35 and DHT 11 sensor values from the Internet provided values are +3 °C and +4 °C, respectively. Moreover, the gaps, in the figure, between the time (in hours) duration at x-axis indicates that the devices were in sleeping mode, and no communication occurred during these intervals. Tables 4 and 5 show the transmission and receiving of information from client to the server. During transmission and receiving of information, there were some moments occurred when the server didn't receive the transmitted information. Thus, a blank space was shown on the serial display of Arduino IDE, as shown in Tables 4 and 5.

Table 4. Transmission and receiving of information using one-to-one communication.

Internet Temperature Readings	Transmission information		Received information	
	LM 35	DHT 11	LM 35	DHT 11
32	34	37	34	37
35	38	40	–	–
37	40	41	40	41
40	42	44	42	44
41	44	46	44	46
41	43	46	43	46
42	45	47	–	–

Table 5. Transmission, transceiving, and receiving of information using many-to-one communication.

Internet Temperature Readings	Transmitted information		Router information		Received information	
	LM 35	DHT11	LM 35	DHT11	LM 35	DHT11
41	44	46	44	46	44	46
41	43	46	43	46	43	46
42	45	47	45	47	45	47
42	44	46	–	–	–	–
40	43	45	43	45	43	45
37	40	42	–	–	–	–
36	39	40	39	40	39	40

In addition, the packet delivery ratio (PDR), in the communication setup, is defined as the ratio of the total number of packets received by the server to the total number of packets transmitted by the clients, i.e.

$$\text{PDR} = \frac{\text{Total Number of Packets Received by the Server}}{\text{Total Number of Packets Transmitted by the Clients}} \tag{1}$$

During 12 h of reliability testing, 1800 packets in the form of string were transmitted by the clients, and out of them 1740 packets were received using both the modes of communication. Therefore, from Eq. (1), we can say that,

$$\text{PDR} = \frac{1740}{1800} = 96.67\%$$

5.5 Friedman's Test

It is a test which helps to determine whether the wireless transmission of information for each condition differ significantly from the values which would be expected by chance [36], as shown in Eq. (2). The test statistic provided by Friedman's is:

$$\Upsilon_1 = \frac{12}{nK(K+1)} \sum_{k=1}^{K} R^2{}_k - 3n(K+1) \tag{2}$$

where, $R_k = \sum_{i=1}^{n} R_{ik}$ is the sum of the rank for wireless transmitted information k over n blocks [37]. Considering the null hypothesis, n as 7, the statistic Υ_1 has an asymptotic Chi-square distribution with $K - 1$ degree of freedom. Table 6 shows the transmission, transceiving, and receiving of the information using both types of communication, i.e. one-to-one and many-to-one communication. In this, we have demonstrated an experiment to compare the amount of information which are received by the server in several time duration. The experiment is divided into 3 different time duration starting from 9 am −12 noon, 12 noon to 4 pm, and 4 to 8 pm. The experiment was conducted in 7 different days. During all the several scenarios, the information is transmitted by the connected clients and server receives them continuously.

Table 6. Transmission, transceiving, and receiving of information from clients to server.

	Morning (9–12 noon)	Afternoon (12–4 pm)	Evening (4–8 pm)
Day 1	586	581	579
Day 2	580	576	582
Day 3	578	584	581
Day 4	585	582	589
Day 5	583	577	586
Day 6	575	572	577
Day 7	576	583	585

Out of the total 600 transmitted information during one phase, very few of them are lost due to presence of hindrances, and rest of them are collected by the server. It means that out of 1800 information that are transmitted during a day, only 1746 information are received on day 1, 1738 information are received on day 2, 1743 are received on day 3, and so on. And the rest of the unreceived information are lost.

In Friedman's Test, considering the α level of significance as 0.05, the calculated chi square value will be 6.34, and the table value is 5.588. Furthermore, the α-value will be 0.0421 which is less than 0.05. These results show that the calculated chi-square value is greater than the table value. Therefore, we can reject the null hypothesis since,

$$\Upsilon_1 \geq \chi^2{}_{K-1;1-\alpha} \tag{3}$$

Thus, due to the rejection of null hypothesis from Eq. (3), we able to conclude that the transmission of information from transmitter to receiver changes significantly across the time.

5.6 Wilcoxon Signed-Ranks Test

In this test, we have measured the number of received information by the server when the information is transmitted at every hour by the clients during the wake-up interval of 5 min. Out of 150 transmitted information, few of them are lost due to the presence of physical hindrances. This non-parametric test has been done with consecutive two days observations, i.e. day 1 and day 2, day 3 and day 4, and day 5 and day 6, as shown in Tables 7, 8, 9 respectively.

The requirement for the Wilcoxon Tests for the paired sample information where the D_i are independent, and corresponds to Day 1 – Day 2, or Day 3 – Day 4, or Day 5 – Day 6 for all i = 1, 2, …. 12. Moreover, in this test, we have used the H_o null hypothesis where the distribution of differences score in the received information is symmetrical about zero. In Tables 7, 8, 9, columns 1, 2 and 3 shows the consecutive received information by the server at every hour. Column 4 contains the difference between the received information, and column 5 contains the absolute value of these differences [38]. Column 6 contains the adjusted rankings of the non-zero value derived from column 5. And, finally columns 7 and 8 shows the values where the difference in column 4 is positive and the difference in column 4 is negative respectively.

Table 7. Wilcoxon signed-ranks test for day 1 and day 2 received information.

Hours	Day 1	Day 2	Difference	Absolute difference	Rank	Positive rank (T+)	Negative rank (T−)
9 am	146	142	4	4	8.5	8.5	
10 am	142	147	−5	5	10.5		10.5
11 am	144	142	2	2	3.5	3.5	
12 pm	147	144	3	3	6.5	3.5	
1 pm	145	148	−3	3	6.5		6.5
2 pm	140	146	−6	6	12		12
3 pm	141	142	−1	1	1		1
4 pm	148	146	2	2	3.5	3.5	
5 pm	143	145	−2	2	3.5		3.5
6 pm	146	148	−2	2	3.5		3.5
7 pm	143	147	−4	4	8.5		8.5
8 pm	149	144	5	5	10.5	10.5	
Total						29.5	45.5

$T^+ = 29.5$ and $T^- = 45.5$. The smaller of these values is the test statistics T is 29.5 (positive rank).

Table 8. Wilcoxon signed-ranks test for day 3 and day 4 received information.

Hours	Day 3	Day 4	Difference	Absolute difference	Rank	Positive rank (T+)	Negative rank (T−)
9 am	142	148	−6	6	12		12
10 am	145	141	4	4	8	8	
11 am	147	143	4	4	8	8	
12 pm	146	142	4	4	8	8	
1 pm	142	146	−4	4	8		8
2 pm	144	145	−1	1	1		1
3 pm	149	145	4	4	8	8	
4 pm	146	149	−3	3	4		4
5 pm	148	143	5	5	11	11	
6 pm	144	147	−3	3	4		4
7 pm	147	145	2	2	2	2	
8 pm	149	146	3	3	4	4	
Total						49	29

T^+= 49 and T^- = 29. The smaller of these values is the test statistics T is 29 (negative rank).

Table 9. Wilcoxon signed-ranks test for day 5 and day 6 received information.

Hours	Day 5	Day 6	Difference	Absolute difference	Rank	Positive rank (T+)	Negative rank (T−)
9 am	144	145	−1	1	2.5		2.5
10 am	145	144	1	1	2.5	2.5	
11 am	147	145	2	2	5.5	5.5	
12 pm	141	142	−1	1	2.5		2.5
1 pm	143	147	−4	4	8		8
2 pm	148	141	7	7	11	11	
3 pm	149	143	6	6	9	9	
4 pm	146	147	−1	1	2.5		2.5
5 pm	142	149	−7	7	11		11
6 pm	145	147	−2	2	5.5		5.5
7 pm	141	148	−7	7	11		11
8 pm	143	146	−3	3	7		7
Total						28	50

T^+ = 28 and T^- = 50. The smaller of these values is the test statistics T is 28 (positive rank)

We have performed a two-tailed Wilcoxon Signed Ranks Test for the Paired Samples with $\alpha = 0.05$ to the test. From the Wilcoxon Signed-Ranks Table, the critical value for the T statistic is 13 for n € sample hours, i.e. 12. However, $T_{critical} = 13$ which is less than T in all the three cases, i.e. $T_{critical} < T$.

(i) $13 < 29.5$ (ii) $13 < 29$, and (iii) $13 < 28$

Therefore, with the smaller $T_{critical}$ value, we cannot reject the null hypothesis (i.e. $p > 0.05$), and hence we can conclude that there are no significant differences in transmitting and receiving of information during consecutive days.

These results show that the implementation of the forest fire detection system is very much reliable. Moreover, the loss of information occurred during communication is due to the presence of environmental factors, such as hindrances present in an area. The hindrances present in the environment are wind, dust, sand, rain, etc. The hindrances present in the forest premises are trees, movement of animals, bridges, and so on. Due to these presences of hindrances signals will get affected, and leads to the loss of information.

The requirements in terms of future research direction of this implementation are: (i) to detect faulty clients, or routers, or the server nodes, (ii) to identify the shortest route for the transmission of information from a cluster node to the base station, (iii) the minimum consumption of battery source.

6 Conclusion and Future Work

We have presented a hardware implementation of WSNs for the detection and monitoring of forest fire using serial communication and Wi-Fi. The designed is based on the wireless communication with and without using Internet facilities between clients, routers and server. The interfaced sensors provide the environmental information for the detection of fires. If the collected values satisfy the provided threshold values; clients deliver all the collected information wirelessly to the main server without using the Internet. Once the information is received by the server, the same again be forwarded to the serially interfaced client, and uploaded to the web server by using the Internet facilities. For the successful establishment of the design, we have used two types of communication: (i) one-to-one communication, and (ii) many-to-one communication. During the implementation, we have covered a total distance of 120 m by connecting several routers. And, we have analyzed that the flow of information from clients to server is very efficient, and provides an accuracy of $94 \pm 3\%$ in one-to-one communication, and $92 \pm 3\%$ in many-to-one communication. Moreover, we showed that both modes of communication provide PDR of 96.67% which indicates the reliability of the system. We have also conducted Friedman's and Wilcoxon Signed-Rank Test, and there we have shown that how the amount of collected information varies in different time duration. Therefore, we would like to proceed the same hardware setup in future for the detection of toxic [39] types of gases present during the occurrence of fire such as Carbon Dioxide (CO2), Carbon Monoxide (CO) and other toxic gases.

Acknowledgment. This project was introduced by CSIR-CSIO, Delhi, India. We would like to thank Dr. Paramita Guha for providing knowledge and support regarding this project.

References

1. Wang, G., Zhang, J., et al.: A forest fire monitoring system based on GPRS and ZigBee wireless sensor network. In: 5th International Conference on Industrial Electronics and Applications, Taiwan, pp. 1859–1862. IEEE (2010)
2. Gislason, D.: Zigbee Wireless Networking, 1st edn. Elsevier, New York (2002)
3. Zhang, J., Li, W., et al.: Forest fire detection system based on a ZigBee wireless sensor network. Front. For. China **3**(4), 369–374 (2008)
4. Gupta, B.B., Quamara, M.: An overview of Internet of Things (IoT): architectural aspects, challenges, and protocols. Concurrency Comput. Pract. Exper., e4946 (2018). https://doi.org/10.1002/cpe.4946
5. Dener, M., Ozkok, Y., Bostancioglu, C.: Fire detection systems in wireless sensor networks. In: World Conference Procedia Social and Behavioral Sciences, Turkey, pp. 1846–1850. Elsevier (2015)
6. Ferreira, A., Pinto, P.: Wireless Sensor Network for Forest Fire Detection. FEUP, Portugal (2017)
7. Kumar, S., Chaudhary, A., et al.: Identification of fire prone forest areas based on GIS analysis of archived forest fire points detected in last thirteen years. Technical Information Series, India, vol. 1, no. 1 (2019)
8. Ulucinar, A.R., Korpeoglu, I., Cetin, A.E.: A Wi-Fi cluster based wireless sensor network application and deployment for wildfire detection. Int. J. Distrib. Sens. Netw. **10**(10) (2014). Article ID 651957
9. Pico, A.M., Araujo, A., et al.: Forest monitoring and wildland early fire detection by a hierarchical wireless sensor network. J. Sens., 1–8 (2016). Article ID 8325845. https://doi.org/10.1155/2016/8325845
10. Zheng, Y., Zhao, Y., et al.: An intelligent wireless system for field ecology monitoring and forest fire warning. Sensors **18**(12), 4457–4473 (2018)
11. Widodo, J., Izumi, Y., et al.: Detection of peat fire risk area based on impedance model and DInSAR approaches using ALOS-2 PALSAR-2 data. IEEE Access **7**, 22395–22407 (2019)
12. Yan, X., Cheng, J., et al.: Real-time identification of smoldering and flaming combustion phases in forest using a wireless sensor network-based multi-sensor system and artificial neural network. Sensors **16**(8), 1228 (2016). PMC 5017393
13. Alkhatib, A.A.A.: A review on forest fire detection techniques. Int. J. Distrib. Sens. Netw. **10** (3) (2014). Article ID 597368
14. Shi, W., Cao, J., et al.: Edge computing vision and challenges. Internet Things J. **3**(5), 637–646 (2016)
15. Neumann, G.B., de Almeida, V.P., Endler, M.: Smart forests fire detection service. In: Symposium on Computer and Communications, Brazil, pp. 1276–1279. IEEE (2018)
16. Bhosle, A.S., Gavhane, L.M.: Forest disaster management with wireless sensor network. In: International Conference on Electrical, Electronics, and Optimization Technique, India, pp. 287–289. IEEE (2016)
17. Ganesh, U.A., Anand, M., et al.: Forest fire detection using optimized solar powered ZigBee wireless sensor networks. Int. J. Sci. Eng. Res. **4**(6), 586–596 (2013)
18. Huh, Y., Lee, J.: Enhanced contextual forest fire detection with prediction interval analysis of surface temperature using vegetation amount. Int. J. Remote Sens. **38**(11), 3375–3393 (2017)
19. Chakraborty, S., Banerjee, A., et al.: Time-varying modelling of land cover change dynamics due to forest fires. J. Sel. Top. Appl. Earth Obs. Remote Sens. **11**(6), 1769–1776 (2018)
20. Marchese, F., Mazzeo, G., et al.: Issues and possible improvements in winter fires detection by satellite radiances analysis: lesson learned in two regions of northern Italy. J. Sel. Top. Appl. Earth Obs. Remote Sens. **10**(7), 3297–3313 (2017)

21. Dhief, F.T.A., Sabri, N., et al.: A review of forest fire surveillance technologies: mobile ad-hoc network routing protocols perspective. J. King Saud Univ. Comput. Inf. Sci. **31**, 135–146 (2019)
22. Yuan, C., Liu, Z., Zhang, Y.: Aerial images-based forest fire detection for firefighting using optical remote sensing techniques and unmanned aerial vehicles. J. Intell. Robot. Syst. **88**, 635–654 (2017)
23. Polivka, T.N., Wang, J., et al.: Improving nocturnal fire detection with the VIIRS day-night band. Trans. Geosci. Remote Sens. **54**(9), 5503–5519 (2016)
24. Leal, B.E.Z., Hirakawa, A.R., Pereira, T.D.: Onboard fuzzy logic approach to active fire detection in Brazilian Amazon forest. Trans. Aerosp. Electron. Syst. **52**(2), 883–890 (2016)
25. Castra, J.T., Gil, P.C., et al.: Forest fire prevention, detection, and fighting based on fuzzy logic and wireless sensor networks. Complexity, 1–17 (2018). Article ID 1639715. https://doi.org/10.1155/2018/1639715
26. NodeMCU documentation. https://nodemcu.readthedocs.io/en/master/. Accessed 5 Dec 2019
27. Benchoff, B.: A Dev Board for the ESP LUA Interpreter. Accessed 10 Feb 2019
28. Saha, S., Majumdar, A.: Data center temperature monitoring with ESP8266 based wireless sensor network and cloud-based dashboard with real time alert system. In: Devices for Integrated Circuit, India, pp. 307–310. IEEE (2017)
29. Rajalakshmi, A., Shahnasser, H.: Internet of things using node red and alexa. In: 17th International Symposium on Communications and Information Technologies, Australia (2018)
30. Poongothai, M., Subramanian, P.M., Rajeswari, A.: Design and implementation of IoT based smart laboratory. In: 5th International Conference on Industrial Engineering and Applications, Singapore, pp. 169–173. IEEE (2018)
31. Walia, N.K., Kalra, P., Mehrotra, D.: An IoT by information retrieval approach smart lights controlled using Wi-Fi. In: 6th International Conference Cloud System and Big Data Engineering, India, pp. 708–712. IEEE (2016)
32. Barai, S., Biswas, D., Sau, B.: Estimate distance measurement using NodeMCU ESP8266 based on RSSI technique. In: Proceedings of Conference on Antenna Measurements and Applications, Japan, pp. 170–173. IEEE (2017)
33. Bhatnagar, H.V., Kumar, P., et al.: Implementation model of Wi-Fi based smart home system. In: International Conference on Advances in Computing and Communication Engineering, France, pp. 23–28. IEEE (2018)
34. Schwartz, M.: Internet of Things with ESP8266. Packt Publishing Ltd., Birmingham (2016)
35. Computer Networking. https://www.diffen.com/difference/TCP_vs_UDP. Accessed 15 Feb 2019
36. Pereira, D.G., Afonso, A., Medeiros, F.M.: Overview of Friedman's test and post-hoc analysis. In: Communications in Statistics – Simulation and Computation, pp. 2636–2653. Taylor & Francis (2015)
37. Fan, G.F., Peng, L.L., Hong, W.C.: Short term load forecasting based on phase space reconstruction algorithm and bi-square kernel regression model. Appl. Energy **224**, 13–33 (2018)
38. Dong, Y., Zhang, Z., Hong, W.C.: A hybrid seasonal mechanism with a chaotic cuckoo search algorithm with a support vector regression model for electric load forecasting. Energies **11**(4), 1009 (2018)
39. Mohapatra, S., Khilar, P.M.: Forest fire monitoring and detection of faulty nodes using wireless sensor network. In: TENCON Proceedings of the International Conference, Singapore, pp. 3232–3236, IEEE (2016)

Application of Supervised Learning Approach for Target Localization in Wireless Sensor Network

Satish R. Jondhale[1(✉)], Raed Shubair[2], Rekha P. Labade[1], Jaime Lloret[3], and Pramod R. Gunjal[1]

[1] Department of E&TC, Amrutvahini College of Engineering, Sangamner, India
profsatishjondhale@gmail.com, rplabade@gmail.com, pramod.gunjal@avcoe.org

[2] Department of Electrical Engineering and Computer Science, MIT, Cambridge, USA
rshubair@mit.edu

[3] Polytechnic University of Valencia, Valencia, Spain
jlloret@dcom.upv.es

Abstract. In the context of indoor environments, the Received Signal Strength Indicator (RSSI) measurements are generally coupled with noise uncertainty due to signal propagation issues such as multipath propagation, Non-Line of Sight (NLOS), reflection. In order to deal with this problem, the localization algorithm is required to be efficient in terms of Localization Accuracy and Execution Speed. The Artificial Neural Network (ANN) does not need prior knowledge of noise statistics during its operations. This paper evaluates the comparison of localization performance of various supervised learning architectures such as Generalized Regression Neural Network (GRNN), Multilayer Perceptron (MLP), Radial Basis Function Network (RBFN), and Feed Forward Neural Network (FFNT) for the Wireless Sensor Network (WSN) based indoor localization problem. The comparison of localization accuracy under the simulated static indoor environment of 100 × 100 m^2 with 15 anchor nodes advocate the suitability of the application of supervised learning approach for the indoor localization problems over the traditional trilateration-based approach. The proposed supervised learning implementations are tested and compared with the traditional trilateration-based localization technique by varying the variance of RSSI measurement noise from 0 dBm to 5 dBm in the steps of 1 dBm. Out of all the proposed supervised learning architectures, the GRNN based implementation shows higher localization accuracy.

Keywords: Received Signal Strength Indicator (RSSI) · Generalized Regression Neural Network (GRNN) · Multilayer Perceptron (MLP) · Radial Basis Function Network (RBFN) · Feed Forward Neural Network (FFNT) · Wireless Sensor Network (WSN)

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 493–519, 2020.
https://doi.org/10.1007/978-3-030-40305-8_24

1 Introduction

Continuous technological revolution in Radio Frequency (RF) and Micro-Electromechanical System (MEMS) technology enabled the use of WSN for various of new positioning, tracking and navigation applications [1–3]. The object Localization and Tracking (L&T) is one of the important research areas of WSN. Today WSN is being an integral part of plenty of civilian applications such as locating mobile objects in indoor environments, wildlife tracking, monitoring and maintenance of under buried pipes as well as wide variety of Location Based Services (LBS's). The L&T is basically an estimation of locations of the mobile object (localization problem) and estimation of its actual trajectory (tracking problem) with the help of field measurements collected during its motion [4]. The localization is basically a one-step solution of a multi-step tracking problem. The L&T of objects in an indoor environment with high accuracy can trigger variety of new LBS applications. However, environmental dynamicity due to RF signal propagation issues such as NLOS, signal attenuation, multi path propagation makes the indoor L&T problem highly challenging. Though Global Positioning System (GPS) can be used to locate the objects in the indoor environment, the major hurdle is the demand of the line of sight (LOS) of GPS receivers with satellites. Additionally, attaching a GPS module to every sensor node is very expensive alternative [5–7]. The localization accuracy of the GPS for outdoor environment is around 3.5 m which is not suitable for the indoor LBS [6]. Therefore, the current research trend is to develop GPS-Less system for L&T for indoor environments. The WSN features such as easy deployment and lower cost, self-organizing capability and unattended working, make them an superior option for L&T applications. The dominant wireless technologies to implement WSN based indoor L&T system are RFID [8–10], Bluetooth [11, 12] and Wi-Fi [13, 14].

The WSN driven localization can be broadly categorized as Range Based (relies on computation of distances between nodes) and Range Free (relies on the utilization of information other than distance (range free approach) [4]. The first category utilizes field measurements such as Angle of Arrival (AoA), Time of Arrival (ToA), Time Difference of Arrival (TDoA), and RSSI [4]. In the ToA based approach, time of arrival of signal from the transmitter to receiver is used to estimate distances, whereas the TDoA based approach uses time difference of arrival of signals traveling between transmitter and receiver. The major problems with ToA and TDoA are: requirement of the perfect time synchronization between transmitter and receiver, NLOS, interferences. The AoA based approach utilizes angles of arrival of signals between target and sensor nodes. The requirement of an array of directional antennas is the major drawback of AoA technique. As against this, the RSSI based localization approach neither need clock synchronization or any additional hardware [15–18]. Additionally, this approach is simple to use and has comparatively a lower power requirement. That's why it has been widely used measurement type for WSN based L&T applications. In the RSSI-based approach distance between transmitter and receiver are estimated by utilizing RSS using an appropriate signal path loss model [19, 20].

Majority of RSSI based localization schemes relies on trilateration. It generally suffers with the imperfect computations of distances. The major sources of errors are:

(1) nonlinear system dynamics, (2) fluctuations in RSSI measurements, and (3) issues such as signal attenuation, NLOS, multipath fading, and shadowing effects. To deal with these problems, the trilateration technique is required to be replaced with some advanced technique. The ANN can quickly learn from noisy environment and can yield high localization accuracy than the trilateration technique [21, 22]. As against Kalman Filter (KF), there is no need of prior knowledge of the noise distribution in ANN based approach [17]. This chapter explore the possibilities of various ANN architectures to replace trilateration technique for indoor L&T. The proposed ANN based indoor localization techniques do not need to compute the distances between transmitter and receiver. Instead of distance computations, the proposed ANN techniques are capable of estimating unknown target location based on the field measurements (RSSI) directly. The paper outline is as follows: Sect. 2 discusses the existing ANN based localization systems. Section 3 presents the dominant WSN based indoor target localization techniques. Section 4 presents the system assumption and design. The discussion on results is given in Sect. 5. The conclusions and future scope are highlighted in Sect. 6.

2 Related Work

RSSI-based localisation approaches can be classified into Path Loss Model based methods [23–25] and RF Fingerprinting based methods [25–27]. The former approach first converts the RSSI's into distances using the path loss model, and then computes the target location using these distances and coordinates of anchor (reference) nodes. However, the accurate computation of distances using noisy RSSI measurements using the path loss model is highly challenging task. The reason behind this is the inaccurate calibration of parameters of the given path loss model. The selection of appropriate values of model parameters is highly challenging in the context of environmental dynamicity [23]. Even though the path loss model works well for a certain time period, its performance degrades if the RF environment changes further. In the RF fingerprinting based approach a radio map is built in the offline stage and the unknown target location are estimated by comparing online RSSI measurement vector with radio map constructed offline. In [27], the authors proposed a BLE fingerprinting based indoor positioning system using 19 beacons distributed in an area of 600 m^2. The authors also investigated the impact of important issues such as fast fading, beacon density, transmit power, and transmit frequency on the positioning accuracy. The proposed approach shows the improved localization accuracy than Wi-Fi fingerprinting based approach. In other fingerprinting solutions [26], unknown target locations are estimated using Bayesian theory and kernel functions. The major problem with the fingerprinting based approach is the requirement of comparing the input real time RSSI measurement vector for a given time instance with the offline radio map each time. This comparison requirement for each new real time RSSI measurement vector increases the computational complexity of the overall system, making it unsuitable for obtaining real time L&T performance. The authors in [28] adopted a novel concept of application of multiple frequencies and powers between the target object and each reference location to build a larger RSS fingerprint.

ANN is a very popular alternative to approximate multimodal and highly nonlinear models. Once trained with a suitable input and output vectors in the offline stage, the ANN has the capability to discover any linear or non-linear relationship between them. Recently, several ANN based solutions such as MLP [28], convolutional neural network (CNN) [30], machine learning [31, 32], multi-layer neural network (MLNN) [33], FFNT [21, 34], combination of machine learning and kalman filter (KF) [35], GRNN [36–38] etc., have been proposed in the literature for L&T applications. In [28], the MLP architecture with 3 layers and 16 neurons is devised to approximate the locations from the RSSI measurements. The work in [30] proposes a novel wireless signal compensation model which is based on population density, distance, and operative frequency for the considered indoor environment. Once the number of individuals (population density) is calculated using CNN based approach, then, the mapping between the signal attenuation and the population density is adopted in the proposed model. At the end, for the location estimation the traditional trilateration technique is employed. The simulation results demonstrate that the proposed model improves the localization accuracy and is superior to existing RSSI based implementations. The novel concept of RF signature consisting of RSSI, Channel Transfer Function (CTF) and Frequency Coherence Function (FCF), has also been tried along with machine learning approach for indoor target localization problem recently [31, 32]. A combination of RF signals parameters such as link quality indicator (LQI), RSSI are utilized in training and testing the ANN. The experimentation results in a position accuracy of 1.65 m. In [33], the authors neither employed path loss model or RF fingerprinting for the problem of RSSI-based indoor localisation. The authors proposed MLNN based approach integrates three stages: RSSI signals transforming section, denoising section and the localization section. The database of RSSI measurements is utilized to train MLNN to get network parameters. To further refine the localization accuracy a boosting method is designed. Experimental results prove the efficacy of the proposed algorithm. The research work in [34] used a FFNT based approach to estimate the position of the mobile node using a ZigBee based WSN in the indoor environment. The mobile node is supposed to collect the RSSI measurements from five anchor nodes. These RSSI measurements are used to train the proposed FFNT using Levenberg-Marquardt (LM) training algorithm. The positioning performance of the proposed approach and that of a weighted k-nearest neighbour are compared. The results with ANN are observed to be superior to weighted k-nearest neighbour if three anchor nodes are utilized at the cost of high economical budget. In [21], two techniques were employed to estimate the distance between the mobile target and the anchor in both the outdoor and indoor environments. The first approach was based on the LNSM model, while the second on a proposed PSO–ANN algorithm. The hybrid PSO–ANN algorithm shoes higher accuracy in distance estimation than that with LNSM based approach. The work in [35] proposed a machine learning approach along with KF for target tracking. In this, the RSSI measurements are collected to construct radio map which is then used with machine learning algorithms to estimate target locations using only RSSI measurements. The fingerprinting computes a first location estimate of the mobile target, which is then refined with the KF.

The GRNN is a highly parallel neural network which can also be used for target L&T applications [36–42]. In [38], the GRNN based algorithm GRNNα, is proposed to

estimate target locations in 3-D. The performance of the proposed algorithm is compared with that of KF using extensive simulations. The GRNN can be trained with the simulated [41] or real time (obtained from WSN nodes) [37] RSSI measurements received at mobile target and the corresponding actual target locations. In [36], we have proposed a novel GRNN based localization algorithms (namely GRNN+KF and GRNN +Unscented KF (UKF)) as against the traditional trilateration-based approach, to obtain location estimates in WSN, which are then refined using KF. The proposed algorithms are compared with traditional RSSI-based, GRNN-based approach, RSSI+KF and RSSI +UKF algorithms. In [37], two algorithms GRNN+KF and GRNN+UKF are proposed to locate a moving person using PSOC BLE nodes and smartphone. The proposed algorithms demonstrate tracking accuracy of the order of few centimeters [37, 41].

Although ANN is widely adopted in target L&T applications, most of these above implementations are still facing the following challenges: (1) Low Localization Accuracy, (2) Requirement of large training samples, (3) Inability to accommodate environmental dynamicity due to signal propagation issues such as fading, reflections, multipath propagation, and NLOS, (4) Inability to deal with highly nonlinear RSSI-Distance mapping. None of the above implementations have tested and verified their algorithms for the variation in the variance of the measurement noise. To address all of these important issues, this paper focuses on application of various types ANN architectures which are efficient in terms of the localization accuracy, computational complexity and are capable to deal with RSSI noise uncertainty due to above signal propagation issues for the given indoor environment. The comparison of localization performance of these proposed ANN architecture is made with the traditional trilateration-based technique.

3 Indoor Localization Techniques

3.1 LNSM Propagation Model Based Localization

The real time RSSI measurements can be generated for the problem indoor positioning of objects using various types wireless sensor nodes (for example, PSOC BLE Nodes [37]), whereas the artificial RSSI measurements can be generated using a suitable propagation models [36, 43]. The path loss models such as free-space model, two-ray model, and LNSM are quite popular for parameter estimation [38]. Due to better flexibility in various parameter settings, the LNSM is widely adopted by WSN community for simulations. This paper follows the LNSM to generate RSSI measurements. The LNSM is the most suitable model. Its mathematical form is presented in detail below.

The RSSI $(z_{\ell j,k})$ received at the node N_ℓ with coordinates $(x_{\ell k}, y_{\ell k})$ at time k, after being transmitted from the node N_j with coordinates (x_{jk}, y_{jk}), propagates as follows [37, 43]:

$$z_{\ell j,k} = P_r(d_0) - 10n \log(d_{lj,k}/d_0) + X_\sigma, \tag{1}$$

where

- $P_r(d_0)$ is RSSI measured at receiver node located at some reference distance d_0 (generally $d_0 = 1$ m),
- X_σ is normal random variable with a standard deviation of σ. Here, the variance is varied from 0 dBm to 5 dBm in the steps of 1 dBm,
- n is the path loss exponent. Higher the value of n, higher would be the number of obstacles and signal attenuation. The Table 1 shows values of n for typical environments [43].

Table 1. Values of path loss exponent for few typical environments (n)

Environment		n
Outdoor	Free space	2
	Shadowed urban area	2.7 to 5
Indoor	Line-of-sight	1.6 to 1.8
	Obstructed	4 to 6

The distance $d_{\ell j,k}$ between nodes N_ℓ and N_j can be calculated using Eq. (2) as given below.

$$d_{\ell j,k} = d_0 10^{(P_r(d_0) - z_{lj,k} + X_\sigma) / 10n} \tag{2}$$

To locate target using the trilateration technique, minimum three distances of target from three anchor nodes along with their location coordinates are must [44, 45]. By measuring two RSSI values for the two known distances and $P_r(d_0)$ for the given indoor environment, one can easily compute the value of n with the help of Eq. (1). In the proposed research work, the value of n is found to be 4.5.

3.2 Proposed Supervised Learning Architectures for Indoor Target Localization

ANN is an interconnection of artificial neurons which are used to mimic the behaviour of biological neurons by the application of activation functions. These connections are made through suitable weight values which are adjusted automatically during the offline training procedure. This type of learning process is basically called as Supervised Learning. The training vector consists of a set of inputs and corresponding expected outputs. Once trained offline, now the ANN can be deployed to estimate (predict) the system output for any other random input vector in the online stage. In this paper, we apply various ANN architectures under supervised learning. Prior to the indoor localization experiments, the ANN is trained with RSSI measurements and the corresponding 2-D locations of the target in the considered indoor environment in the proposed work.

3.3 GRNN Based Indoor Localization

The GRNN is one pass learning architecture with the requirement of very few training samples [46]. The GRNN based estimation approach relies on measuring the Euclidean distance of a given sample pattern from patterns in the training set. The GRNN architecture is composed of four operating layers namely: an input layer, pattern layer, summation layer, and output layer (See Fig. 1). In this approach four RSSI measurements are fed to the input layer, then the pattern layer applies a nonlinear transformation to the applied input. The pattern layer outputs are multiplied with suitable interconnection weights to have sum operation using the summation layer. At the end the output layer yield network output (that is 2-D target location) as illustrated below.

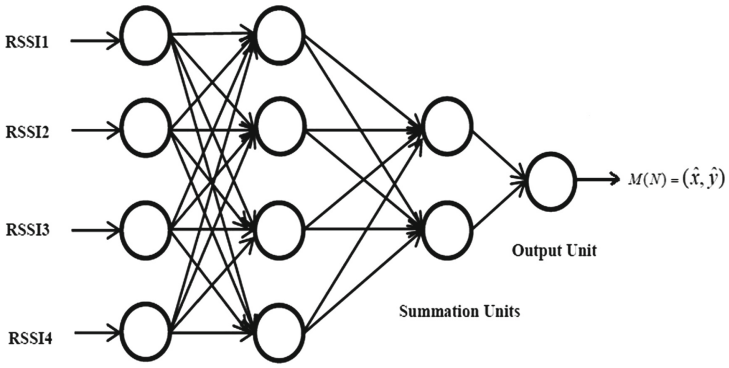


Fig. 1. The proposed GRNN architecture for localization of non-anchor nodes.

The proposed architecture can estimate unknown 2-D location (i.e. M here) for given four input RSSI measurements (i.e. N here). The M_i and N_i are sample values of M and N respectively. This mathematical modeling is given in Eqs. (3) and (4) [36, 37].

$$M(N) = \frac{\sum_{i=1}^{n} M_i \exp\left(\frac{-D_i^2}{2\sigma^2}\right)}{\sum_{i=1}^{n} \exp\left(\frac{-D_i^2}{2\sigma^2}\right)} \tag{3}$$

$$D_i^2 = (N - N_i)^T . (N - N_i) \tag{4}$$

Where, the σ is the smoothing factor (here it is taken to be 1) and n is the dimension of applied input vector (here it is $n = 4$).

3.4 RBFNN Based Indoor Localization

Being a universal approximator, RBFNN can be used to approximate any continuous function with arbitrary precision and is widely used for function approximation problems. It has a fast rate of convergence, better approximation ability and faster

learning speed compared to other neural network algorithms. The RBFNN is a three-layer feed-forward network as shown in Fig. 2. It consists of three layers: input layer, hidden layer and output layer. The transition from input to hidden layer is non-linear transformation, namely RBF function; and the converting function from hidden layer to the output layer is linear. Its structure is illustrated in Fig. 2.

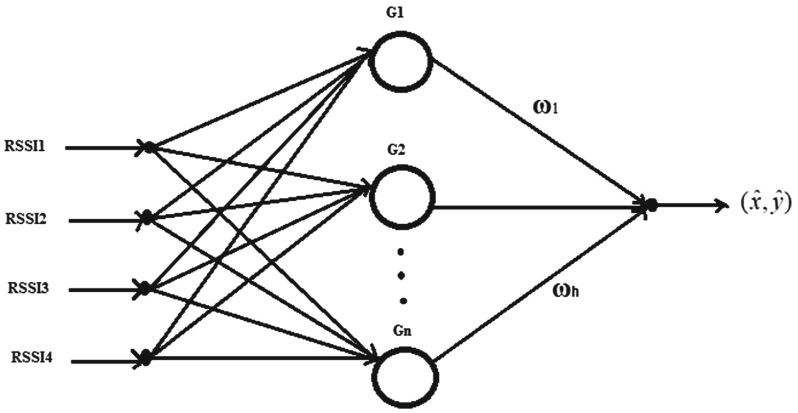


Fig. 2. The proposed RBF architecture for localization of non-anchor nodes.

The RBFNN learning algorithm is divided into two stages. The first stage is unsupervised learning phase, the centre vector and width parameters in Gaussian function of hidden node to be determined based on the input samples. In second stage after determining the parameters of the hidden layer, based on the sample, the weights between hidden and output layers can be obtained using the principle of least squares. For the radial basis function of the hidden layer, there are many different functions in the hidden layer. The most widely used function is Gaussian function as given below in Eq. (5).

$$G(X - c_i) = \exp(-\frac{1}{2\sigma_i^2} \parallel X - c_i \parallel^2) \tag{5}$$

Where, $X = [RSSI1, RSSI2, RSSI3, RSSI4]$, $\parallel X - c_i \parallel$ is the Euclidean distance, c_i is the central vector of Gaussian function of the j^{th} hidden node, this vector is a column vector that has the same dimension of the input sample X, $w_i (i = 1, 2, \ldots h)$ denotes the connection weight of the hidden layer to the output layer; (x, y) represents the actual output of the network. The relationship between hidden and output layers is linear and it provides estimated 2-D location of target as given below in Eq. (6).

$$(\hat{x}, \hat{y}) = \sum_{i=1}^{h} w_h \exp(-\frac{1}{2\sigma_i^2} \parallel X - c_i \parallel^2) \tag{6}$$

3.5 MLP Based Indoor Localization

The MLP is a type of FFNN which consists of three layers: input, hidden and output layers as shown below in Fig. 3. The activation function for the hidden neuron (node) is assumed to be piecewise linear function. Let the weights connecting the input nodes to the hidden nodes be denoted as $\mathbf{W_i^{(1)}}(i = 1, 2, \ldots, N)$ and the weights connecting the hidden node to the output node be $\mathbf{W_i^{(2)}}(i = 1, 2, \ldots, N)$, the biases for the hidden node be $b_i^{(1)}(i = 1, 2, \ldots, N)$, and the bias for the output node be $b_i^{(2)}(i = 1, 2, \ldots, N)$. The output of the MLP $(\hat{x}, \hat{y})$ location with the input feeding into the network is given below in Eq. (7).

$$(\hat{x}, \hat{y}) = \sum_{i=1}^{N} \mathbf{W_i^{(2)}} \varphi(\mathbf{W_i^{(1)}} X + \mathbf{b_i^{(1)}}) + \mathbf{b_i^{(2)}} \tag{7}$$

Where, $X = [RSSI1, RSSI2, RSSI3, RSSI4]$.

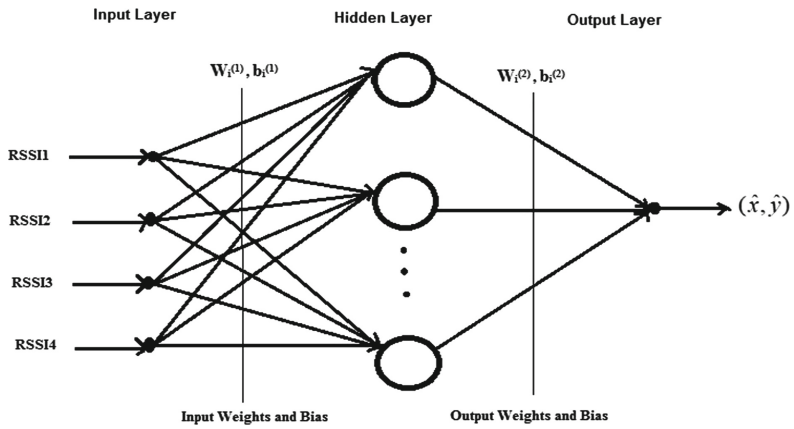


Fig. 3. The proposed MLP architecture for localization of non-anchor nodes.

3.6 FFNT Based Indoor Localization

In FFNT, the data moves only in forward direction to the output nodes. Consider a multilayer FFNT with the RSSI vector $X = [RSSI1, RSSI2, RSSI3, RSSI4]$ as input, one hidden layer with H sigmoid nodes, and a linear output unit as shown in Fig. 4. The output of the FFNT is the estimated unknown location $(\hat{x}, \hat{y})$. It is given below in Eq. (8).

$$(\hat{x}, \hat{y}) = \sum_{i=1}^{H} \mathbf{W_i^{(2)}} \sigma(\sum_{j=1}^{N} \mathbf{W_{ij}^{(1)}} X(i) + \mathbf{b_i}) \tag{8}$$

$\mathbf{W_i^{(1)}}$ denotes the weight connecting the input unit j with the hidden unit i, whereas $\mathbf{W_i^{(2)}}$ denotes the weight connecting the hidden unit i to the output unit, $b_\mathbf{i}$ denotes the bias of hidden unit i, and is the sigmoid transfer function.

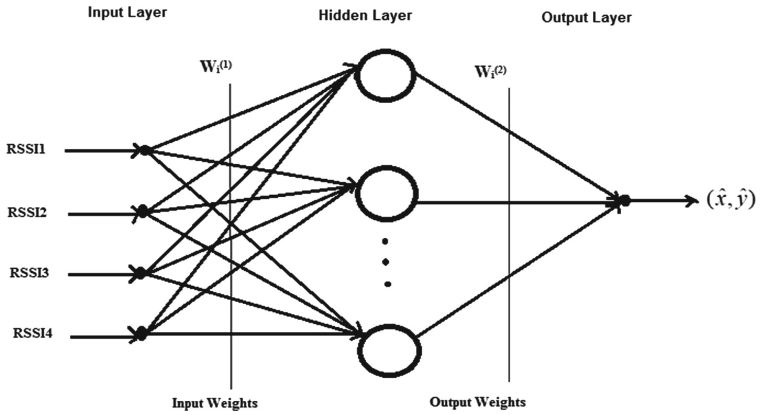


Fig. 4. The proposed FFNT architecture for localization of non-anchor nodes.

4 System Assumptions and Design

4.1 System Design

The proposed research work simulates the indoor environment of area 100 m × 100 m using MATLAB 2013a. The deployment of anchor nodes and unknown target locations (to be estimated) are shown by red asterisk points and blue asterisk points in the considered environment as shown in Fig. 5. In this work, the number of anchor nodes is 12, and the number of unknown target locations is 30. The specific 2-D locations of the deployed anchor nodes and non-anchor nodes are given in Tables 2 and 3. The transmission power and communication radius for each node are set to be 0 dBm and 30 m respectively. The RSSI measurements are generated using the LNSM model. These RSSI measurements are utilized to estimate the unknown target locations using the traditional trilateration and the proposed ANN architectures. The training time as well as execution time for the localization with the traditional trilateration and the proposed ANN architectures is determined using MATLAB commands.

The training database for the proposed ANN architectures for the given indoor localization problem is generated as shown in Fig. 3. The training database contains total 30 RSSI vectors $X_i(i = 1, 2, \ldots, p)$ and corresponding p unknown locations to be estimated during online localization phase. Thus, here $p = 30$. Each set of training data contains one RSSI vector and the corresponding unknown 2-D location. The RSSI measurements utilized in the training database are for variance of RSSI measurement

Table 2. Deployment of anchor nodes in the simulations

Anchor node number	2-D location	Anchor node number	2-D location
1	(0.933, 91.50)	7	(37.75, 73.50)
2	(17.92, 96.89)	8	(90.20, 70.21)
3	(32.68, 88.03)	9	(33.43, 59.66)
4	(40.75, 84.45)	10	(95.41, 54.28)
5	(46.50, 81.40)	11	(9.299, 46.35)
6	(87.72, 78.49)	12	(89.84, 42.92)

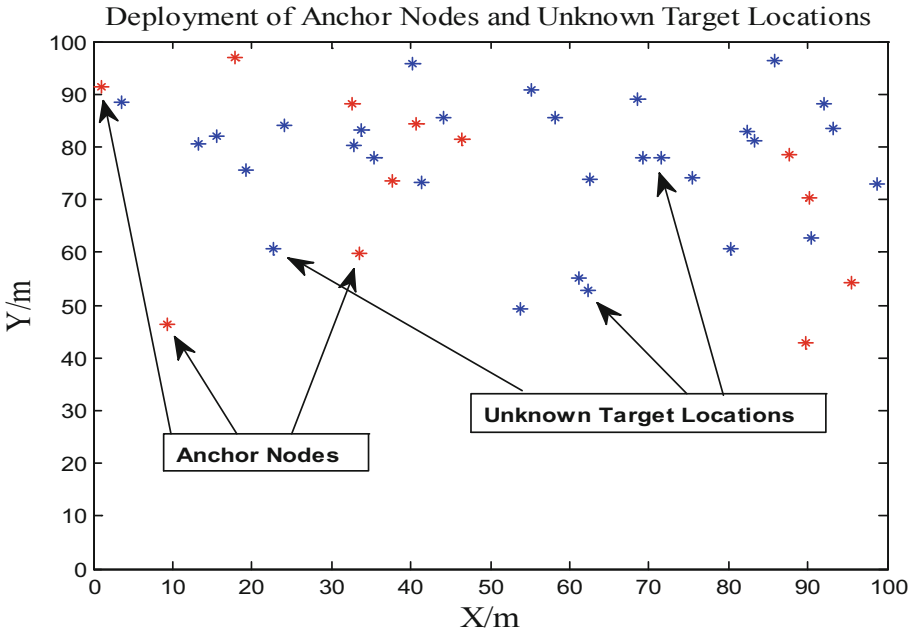


Fig. 5. The deployment of anchor and non-anchor nodes in the indoor environment of 100 m × 100 m.

noise = 0 dBm. During the online location estimation phase, the variance of RSSI measurement noise is varied from 0 dBm to 5 dBm in the steps of 1 dBm. In the simulation environment, all the 12 anchor nodes transmit one beacons to each of the 30 unknown non anchor nodes whose locations are to be estimated. That means each of these 30 unknown non anchor nodes receive 12 RSSI measurements. Out of these 12 RSSI measurements received at unknown location of non-anchor node, any 4 RSSI measurements from any 4 random anchor nodes and their corresponding 2-D locations are utilized to train the proposed ANN architectures. Thus one training set contains $X_i = [RSSI1, RSSI2, RSSI3, RSSI4]$ and (x_i, y_i). The training database contains $p = 30$

Table 3. Unknown target locations to be estimated

Number of non anchor node	Unknown 2-D location of non anchor node to be estimated	Number of non anchor node	Unknown 2-D location of non anchor node to be estimated
1	(53.86, 49.17)	16	(15.57, 81.90)
2	(69.16, 77.90)	17	(33.81, 83.23)
3	(71.52, 78.05)	18	(82.41, 82.80)
4	(91.95, 88.10)	19	(93.22, 83.51)
5	(44.09, 85.62)	20	(32.79, 80.30)
6	(55.26, 90.75)	21	(62.28, 52.66)
7	(85.72, 96.36)	22	(83.18, 81.03)
8	(98.83, 72.95)	23	(35.41, 78.04)
9	(68.53, 88.95)	24	(90.48, 62.71)
10	(61.09, 55.00)	25	(40.14, 95.69)
11	(3.487, 88.54)	26	(22.60, 60.75)
12	(13.33, 80.42)	27	(19.34, 75.44)
13	(58.27, 85.49)	28	(41.44, 73.14)
14	(80.20, 60.72)	29	(62.49, 73.86)
15	(24.11, 84.14)	30	(75.51, 74.24)

such sets which are taken for Noise Variance = 3 dBm. As mentioned earlier in the online localization phase, the trilateration based localization approach utilizes 4 real time RSSI measurements (which are higher in magnitude than rest of the others) out of 12 real time RSSI measurements. Whereas there is no such restriction of the RSSI input vector for the proposed ANN architectures for localization during online localization phase. In other words, in case of proposed ANN architectures, any 4 random RSSI measurements can be utilized for the localization. The nodes with unknown locations receive RSSI measurements from all the 12 anchor nodes, which are utilized to estimate the unknown node locations using trilateration technique. Out of these 12 RSSI measurements received at each unknown node, only those three RSSI measurements are utilized which are highest in magnitude than the rest of the others in the case of trilateration based estimation. Higher the RSSI value, more closer the unknown node is from the given anchor node. Thus in case of the trilateration based estimation; we are providing selective high amplitude RSSI measurements so as to get more accurate estimations of unknown node locations. However in case of the proposed ANN based implementations, any four random RSSI measurements are utilized during the training as well as online estimation phase. Thus RSSI input requirements for the proposed ANN architectures are less stringent as compared to that in case of trilateration based approach (Fig. 6).

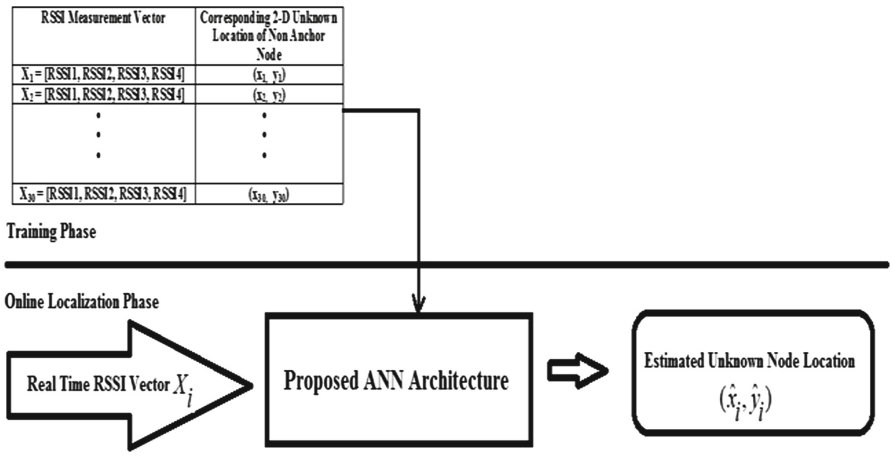


Fig. 6. Overview of system design of the proposed supervised learning based target localization approaches

4.2 Evaluation Parameters

The Localization Error represents the closeness between the estimated target location $(\hat{x}_i, \hat{y}_i)$ and actual location (x_i, y_i) to be estimated and is given in Eq. (9). The Average Localization Error is calculated by taking an average of all the Localization Errors for all the 30 estimations as given by Eq. (10). The values of these two metrics must be as low as possible to get higher localization accuracy.

$$Localization\ Error = \sqrt{(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2}, \quad i = 1, 2, \ldots p. \tag{9}$$

$$Average\ Localization\ Error = \frac{\sum_{i=1}^{p} Localization\ Error}{p} \tag{10}$$

Apart from localization accuracy, Localization Rate (Execution Speed) is also important parameter for the assessment of the efficacy of the proposed algorithms. It must be as small as possible.

4.3 Flow of the Proposed Supervised Learning Based Localization Algorithms

The detailed flow of computation of each unknown location with the proposed algorithms includes three parts as given below in Table 4.

Table 4. Flow of target localization with trilateration and the proposed approach

I. Offline Training Stage
Step 1: The proposed ANN architectures are trained with 30 sets of four RSSI measurements from randomly selected four anchor nodes and corresponding actual locations of the target.

II. Online Estimation of Unknown Target Location
Step 2:

- *For Trilateration Based Estimation:*

The target receives RSSI measurements transmitted by all 12 anchor nodes. These RSSI values are dispatched to the Base station.

- *For Proposed ANN Based Estimations:*

The target receives RSSI transmitted from selected four anchor nodes. These RSSI values are dispatched to Base station.

Step 3:

- *For Trilateration Based Estimation:*

The base station run trilateration algorithm to compute the position estimate of target location. The localization errors in x and y location estimates are computed using Equation (9) as well as recorded.

- *For Proposed ANN Based Estimations:*

The base station runs the proposed ANN algorithms to compute the location estimate of unknown target location. The localization errors in x and y location estimates are computed as well as recorded.

III. Computation of Average Localization Error
Step 4: The Average Localization Error for all simulation experiments in both Phase I and Phase II are computed using Equation (10).ZZ

Note: *1) The Step 2 and the Step 3 are repeated for each new unknown target location ($p = 30$).*

2) The Step 2 to the Step 5 are repeated for varying the Noise Variance from 0 dBm to 5 dBm in the steps of 1 dBm.

5 Discussion on Results

To differentiate the estimation results of unknown target locations with the trilateration and the proposed supervised learning based ANN implementations, different color markers are used in the simulation results (See Figs. 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18). The red marker "$*$" indicates the anchor node positions, the blue marker

"*" represents the actual position of unknown nodes, the black marker "+" denotes the estimated location of unknown nodes using the traditional trilateration, whereas the red marker "o", the green marker "+", the black marker ".", and the orange marker "+" indicate estimated position of unknown nodes using proposed GRNN, BRBFN, MLP and FFNT based supervised learning approaches.

The simulation result of the target localization for all the noise variance cases (Variation in Variance from 0 dBm to 5 dBm) of the RSSI measurements are shown in Figs. 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18 and the comparison of Average Localization Errors for all of these proposed implementations are given in Table 5. In order to save the space, the detailed comparison Localization Errors of each of the 30 target locations with all of these implementations is presented for only a case with Variance = 5 dBm in Table 6. Here it is found that the estimations with GRNN algorithm are very closer to the unknown locations as compared to that with rest of the others. Table 7 shows the comparison of Localization Rates for the Trilateration and the Proposed Supervised Learning based algorithms.

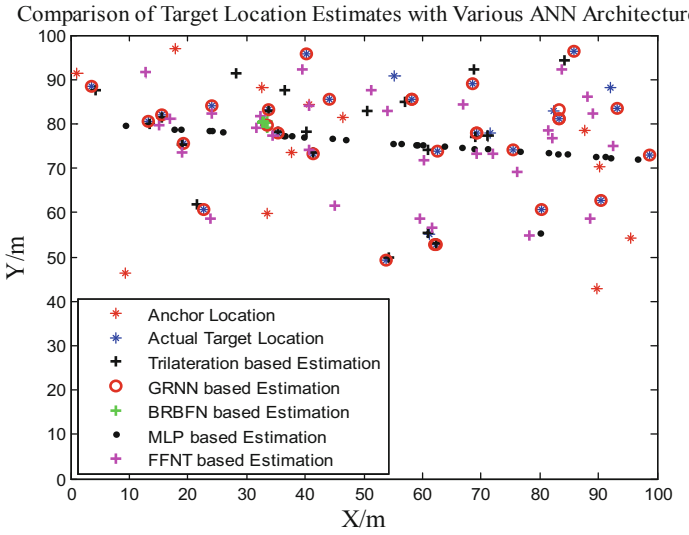


Fig. 7. Actual target location and estimated locations with the traditional trilateration technique and the proposed ANN architectures (mean = 0, variance = 0)

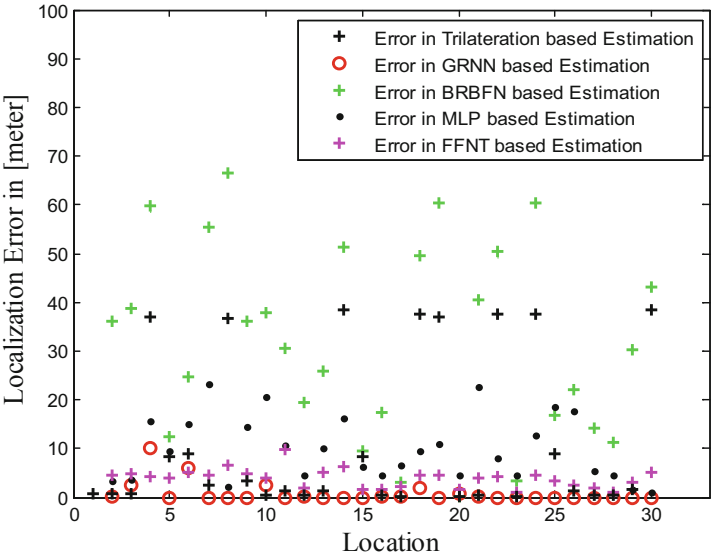


Fig. 8. Comparison of localization performance of traditional trilateration technique with the proposed ANN architectures (mean = 0, variance = 0)

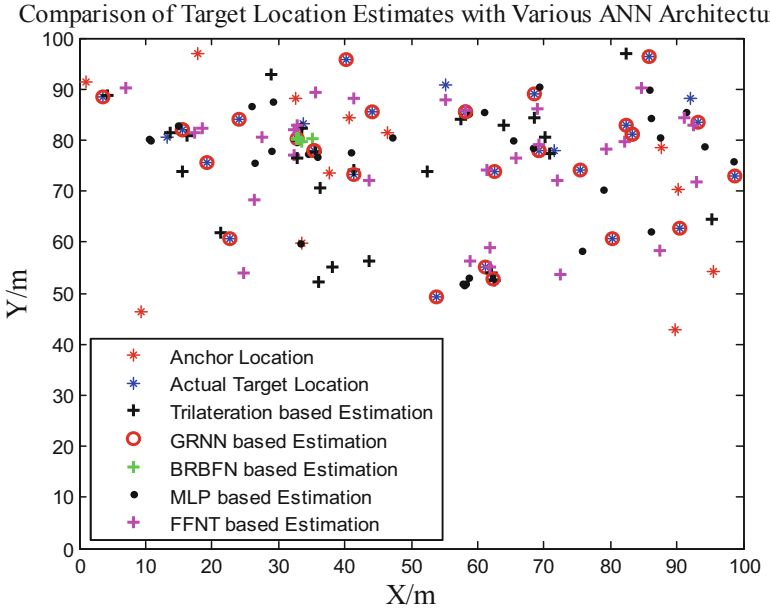


Fig. 9. Actual target location and estimated locations with the traditional trilateration technique and the proposed ANN architectures (mean = 0, variance = 1)

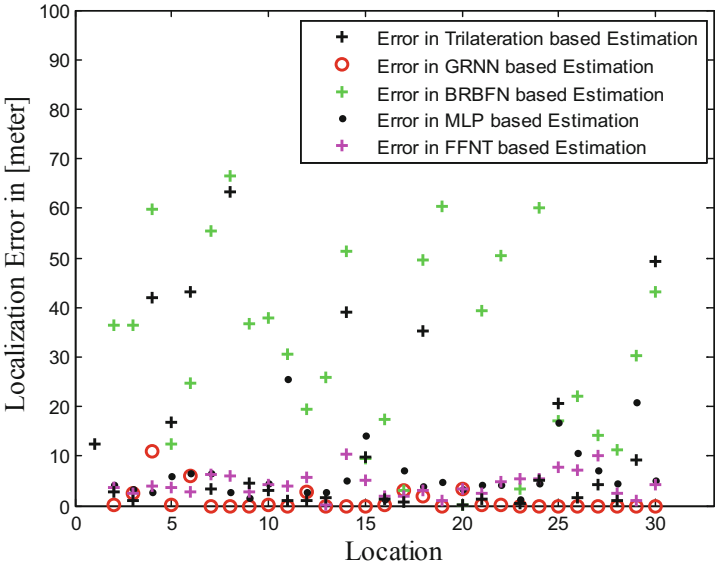


Fig. 10. Comparison of localization performance of traditional trilateration technique with the proposed ANN architectures (mean = 0, variance = 1)

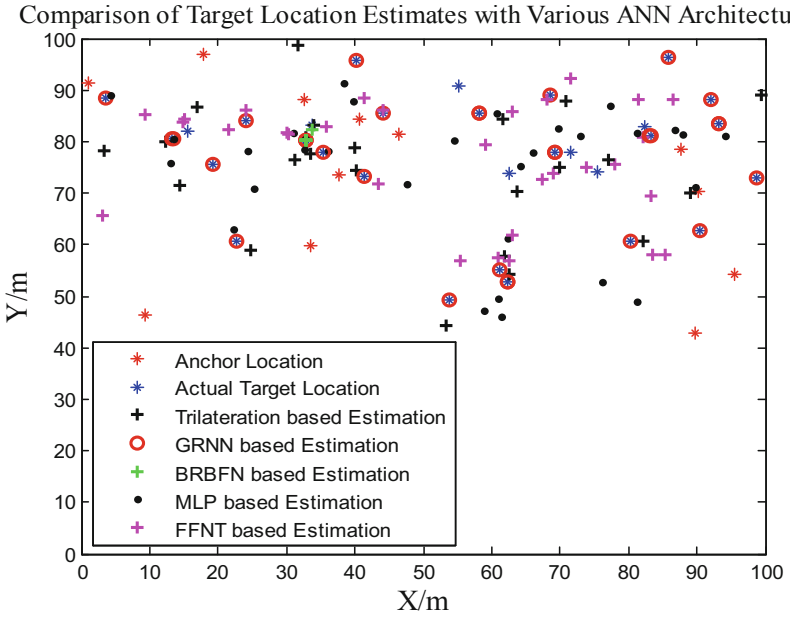


Fig. 11. Actual target location and estimated locations with the traditional trilateration technique and the proposed ANN architectures (mean = 0, variance = 2)

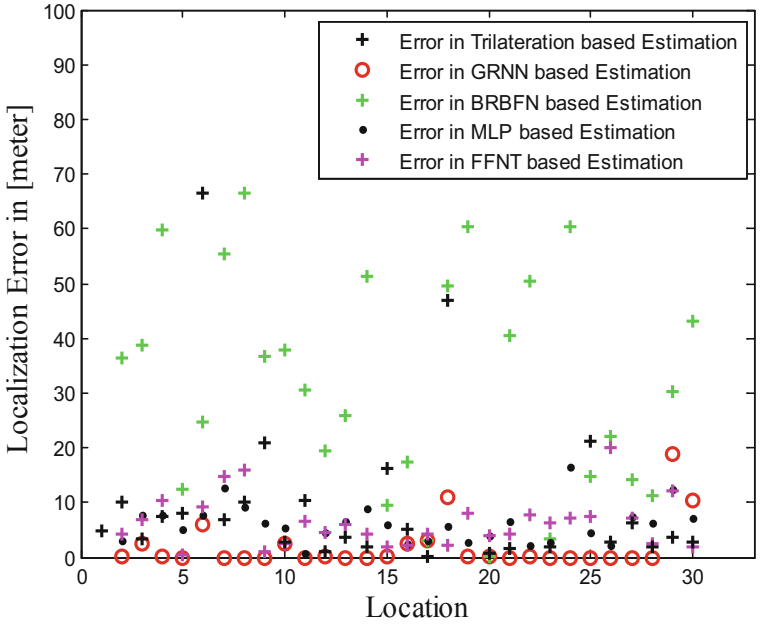


Fig. 12. Comparison of localization performance of traditional trilateration technique with the proposed ANN architectures (mean = 0, variance = 2)

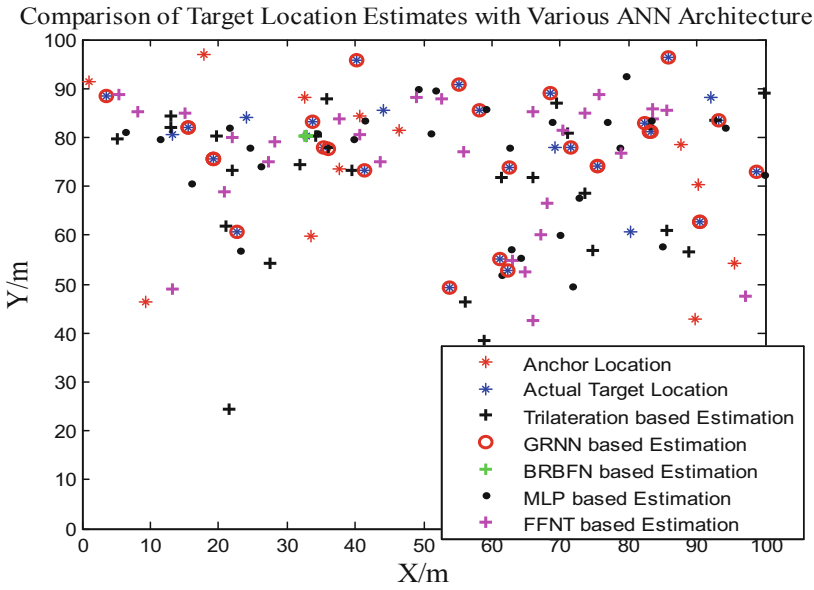


Fig. 13. Actual target location and estimated locations with the traditional trilateration technique and the proposed ANN architectures (mean = 0, variance = 3)

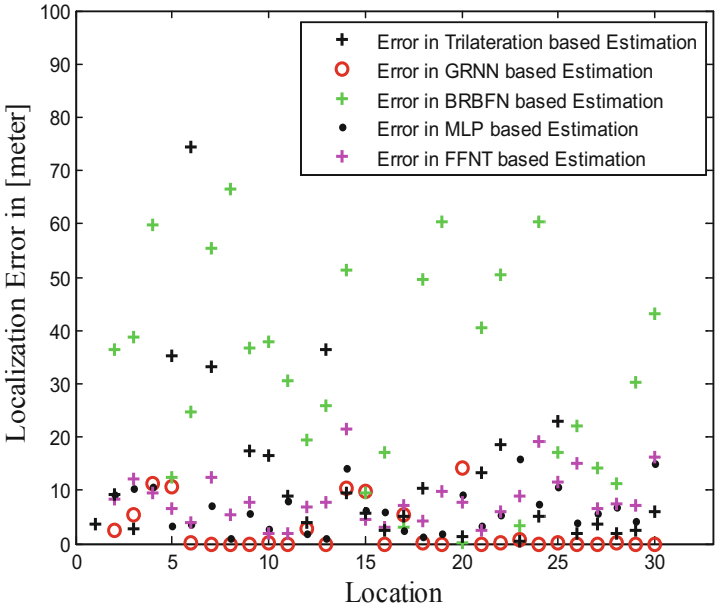


Fig. 14. Comparison of localization performance of traditional trilateration technique with the proposed ANN architectures (mean = 0, variance = 3)

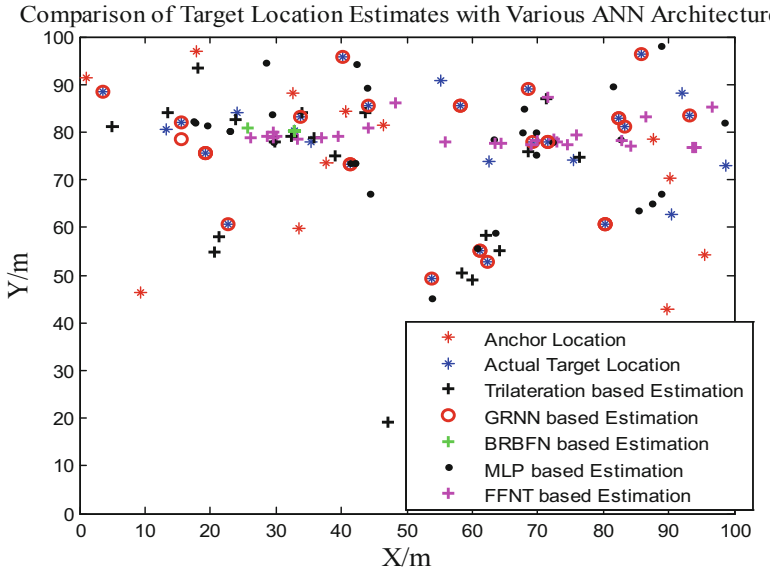


Fig. 15. Actual target location and estimated locations with the traditional trilateration technique and the proposed ANN architectures (mean = 0, variance = 4)

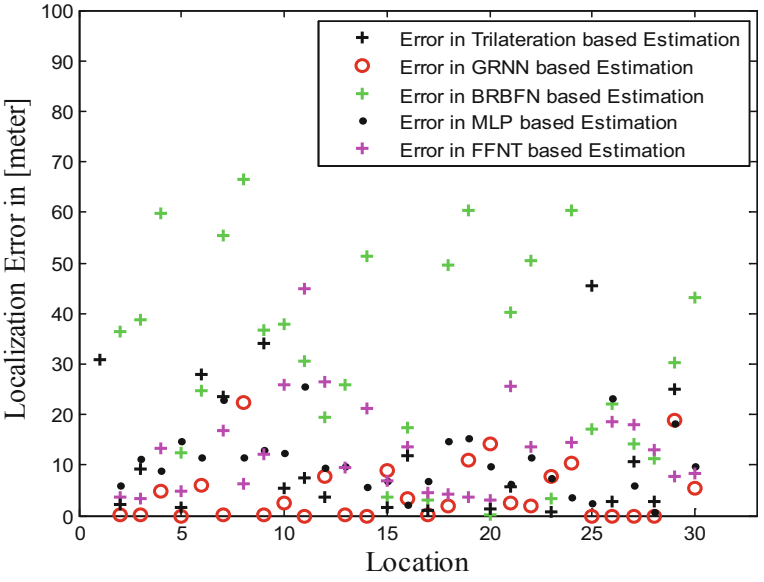


Fig. 16. Comparison of localization performance of traditional trilateration technique with the proposed ANN architectures (mean = 0, variance = 4)

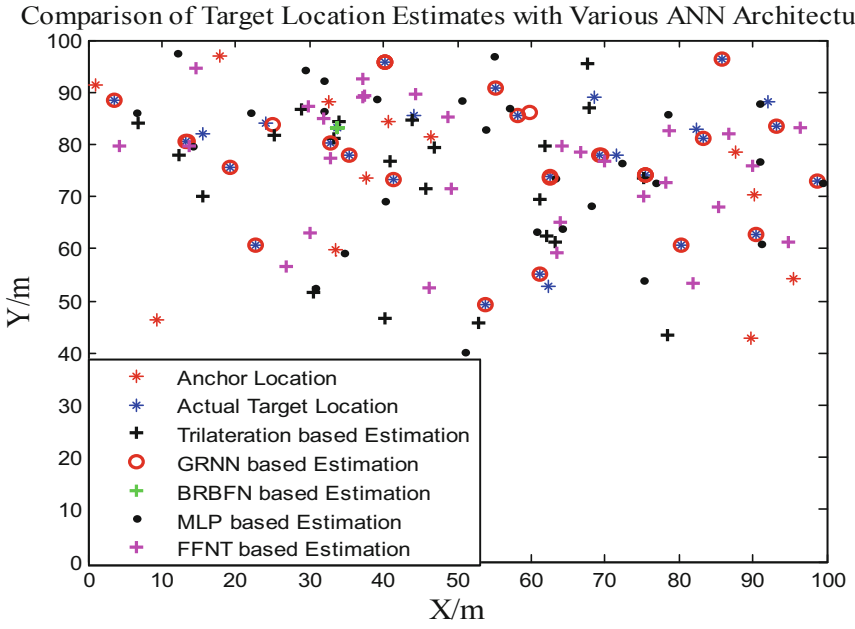


Fig. 17. Actual target location and estimated locations with the traditional trilateration technique and the proposed ANN architectures (mean = 0, variance = 5)

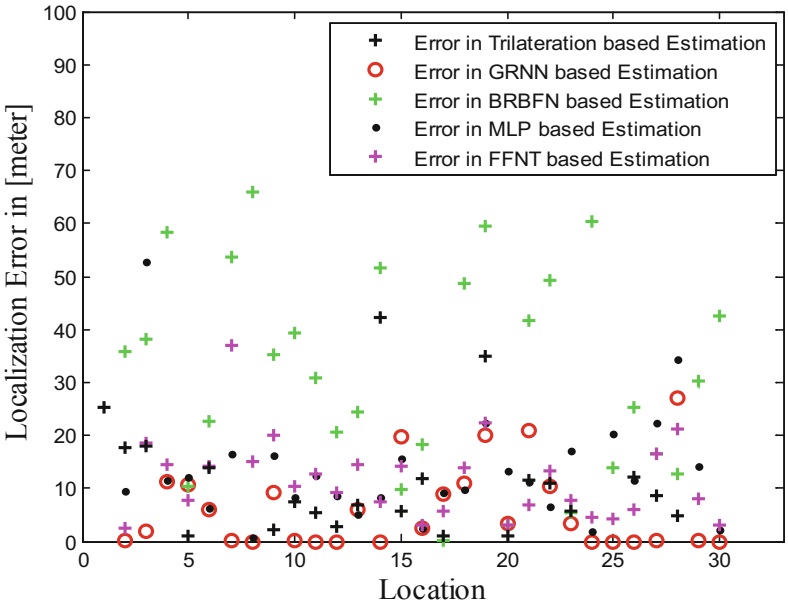


Fig. 18. Comparison of localization performance of traditional trilateration technique with the proposed ANN architectures (mean = 0, variance = 5).

Table 5. Comparison of average localization errors for the trilateration and the proposed algorithms

	Average localization error (in meters)					
	Mean = 0, Variance = 0	Mean = 0, Variance = 1	Mean = 0, Variance = 2	Mean = 0, Variance = 3	Mean = 0, Variance = 4	Mean = 0, Variance = 5
Trilateration	1.8×10^{-12}	18.4003	25.8983	52.6342	100.9870	112.1606
GRNN	0.0299	1.0159	1.4658	1.8056	4.3337	5.9327
RBFN	30.8758	32.0829	31.9808	32.2104	32.0088	32.2104
MLP	2.4088	6.4494	6.1534	9.6483	10.9416	20.3532
FFNT	3.5790	4.3791	7.5724	9.7214	38.3910	10.8043

From Table 5 it is clear that there is comparatively very slight increase in the Average Localization Errors in case of the GRNN based implementation as compared to the traditional trilateration based technique as well as rest of the other supervised learning architectures. Although the trilateration-based technique shows lowest Average Localization Error as compared to the rest of the others, but it is for ideal RF channel (i.e. Variance = 0 dBm). But as the Variance is increased up to 5 dBm in the steps of 1 dBm, the Average Localization Error increases significantly thereafter. The RBFN architecture shows the worst location estimation performance for the considered environmental setup. The reason behind this could be small training database. In other words, the localization performance of the RBFN may be improved if

Table 6. Comparison of location estimations with the trilateration and the proposed supervised learning based approaches against the actual locations of target for RSSI measurement noise with variance of 5 dBm.

Actual location of non anchor node to be estimated	Trilateration based estimation	GRNN based estimation	RBF based estimation	MLP based estimation	FFNN based estimation
(53.86, 49.17)	(78.46, 43.33)	**(41.43, 73.14)**	(33.83, 83.29)	(50.64, 88.46)	(49.18, 71.43)
(69.16, 77.90)	(63.28, 61.28)	**(69.16, 77.90)**	(33.83, 83.29)	(68.14, 68.32)	(66.64, 78.48)
(71.52, 78.05)	(67.72, 95.57)	**(69.53, 77.92)**	(33.83, 83.29)	(56.55, 128.5)	(90.03, 75.99)
(91.95, 88.10)	(925.6, 340.4)	**(83.17, 81.02)**	(33.83, 83.29)	(90.89, 76.66)	(78.63, 82.62)
(44.09, 85.62)	(43.89, 84.65)	**(40.14, 95.68)**	(33.83, 83.29)	(31.91, 86.43)	(37.28, 89.01)
(55.26, 90.75)	(46.90, 79.52)	**(58.26, 85.49)**	(33.83, 83.29)	(54.94, 97.07)	(64.23, 79.63)
(85.72, 96.36)	(233.8, 135.9)	**(85.72, 96.35)**	(33.83, 83.29)	(80.12, 111.9)	(120.4, 83.26)
(98.83, 72.95)	(−104.9, 8.60)	**(98.83, 72.95)**	(33.83, 83.29)	(99.42, 72.58)	(86.83, 82.03)
(68.53, 88.95)	(67.76, 86.91)	**(59.79, 86.00)**	(33.83, 83.29)	(63.23, 73.45)	(48.72, 85.35)
(61.09, 55.00)	(62.05, 62.34)	**(61.09, 55.00)**	(33.83, 83.29)	(60.78, 63.31)	(64.00, 65.02)
(3.487, 88.54)	(6.83, 84.19)	**(3.48, 88.54)**	(33.83, 83.29)	(11.99, 97.57)	(14.54, 94.67)
(13.33, 80.42)	(12.32, 77.78)	**(13.33, 80.42)**	(33.83, 83.29)	(6.62, 86.00)	(4.20, 79.60)
(58.27, 85.49)	(61.97, 79.79)	**(55.25, 90.75)**	(33.83, 83.29)	(53.81, 82.78)	(44.40, 89.54)
(80.20, 60.72)	(40.31, 46.56)	**(80.20, 60.72)**	(33.83, 83.29)	(75.27, 53.99)	(81.85, 53.44)
(24.11, 84.14)	(28.99, 86.82)	**(40.14, 95.68)**	(33.83, 83.29)	(39.06, 88.72)	(37.33, 89.42)
(15.57, 81.90)	(15.63, 70.01)	**(13.40, 80.47)**	(33.83, 83.29)	(14.21, 79.79)	(13.77, 79.59)
(33.81, 83.23)	(33.93, 84.25)	**(24.95, 83.76)**	(33.83, 83.29)	(31.93, 92.30)	(29.82, 87.25)
(82.41, 82.80)	(392.2, 175.6)	**(93.21, 83.50)**	(33.83, 83.29)	(91.01, 87.72)	(96.38, 83.22)
(93.22, 83.51)	(61.09, 69.51)	**(75.51, 74.24)**	(33.83, 83.29)	(72.13, 76.32)	(75.33, 70.05)

(*continued*)

Table 6. (*continued*)

Actual location of non anchor node to be estimated	Trilateration based estimation	GRNN based estimation	RBF based estimation	MLP based estimation	FFNN based estimation
(32.79, 80.30)	(33.31, 81.26)	**(35.40, 78.04)**	(33.83, 83.29)	(40.10, 69.01)	(32.72, 77.27)
(62.28, 52.66)	(52.92, 45.71)	**(62.48, 73.62)**	(33.83, 83.29)	(64.06, 63.86)	(63.55, 59.28)
(83.18, 81.03)	(75.18, 73.46)	**(75.51, 74.24)**	(33.83, 83.29)	(78.43, 85.68)	(85.43, 68.01)
(35.41, 78.04)	(40.94, 76.82)	**(32.79, 80.29)**	(33.83, 83.29)	(29.43, 94.22)	(31.86, 84.80)
(90.48, 62.71)	(−55.71, 15.26)	**(90.48, 62.71)**	(33.83, 83.29)	(91.14, 60.99)	(94.75, 61.22)
(40.14, 95.69)	(100.9, 227.1)	**(40.14, 95.69)**	(33.83, 83.29)	(22.08, 86.19)	(37.25, 92.45)
(22.60, 60.75)	(30.56, 51.53)	**(22.59, 60.75)**	(33.83, 83.29)	(30.72, 52.46)	(26.77, 56.52)
(19.34, 75.44)	(25.32, 81.69)	**(19.34, 75.44)**	(33.83, 83.29)	(34.66, 59.07)	(30.05, 62.90)
(41.44, 73.14)	(45.81, 71.39)	**(53.86, 49.17)**	(33.83, 83.29)	(50.96, 40.23)	(46.16, 52.53)
(62.49, 73.86)	(−68.14, −167.1)	**(62.49, 73.86)**	(33.83, 83.29)	(57.01, 86.88)	(69.99, 76.79)
(75.51, 74.24)	(518.1, 208)	**(75.51, 74.24)**	(33.83, 83.29)	(76.95, 72.68)	(78.19, 72.56)
Average localization error	112.1606	**5.9327**	32.2104	20.3532	10.8043

large training database is used for its training. From the Table 5, it is clear that there is slight race of achieving better localization performance in between the MLP and the FFNT architectures. For some of the cases the MLP shows better localization performance, whereas for the rest of the other cases, the FFNT wins the race. We believe that by doing the changes in the input RSSI vector dimension, number of neurons in the hidden layer, and the size of the training database, one may achieve different localization results.

As already discussed, lower the localization rate, more quickly the system can provide the location updates of unknown target locations. From the Table 7, it is clear that the trilateration shows the lowest localization rate, whereas the FFNT shows the highest localization rate. Although the trilateration technique shows lowest localization rate, its localization performance is very poor (See Table 6). The GRNN architecture shows the best localization performance at the cost localization rate of only 0.936908 s.

Table 7. Comparison of localization rates for the trilateration and the proposed algorithms

Sr. no.	Localization technique	Localization rate (in seconds)
1	Trilateration	0.000255
2	GRNN	0.936908
3	RBFN	0.176954
4	MLP	0.568664
5	FFNN	1.328370

The major contributions of our work are: (1) The proposed research work introduces a various type of ANN based range free localization algorithms as an alternative to range based trilateration-based localization technique with the help of WSN. These ANN based algorithms work on the principle of the Supervised Learning. Being range free system implementations, there is no need of computation of distances between transmitter and receiver nodes for the positioning of target, (2) The proposed ANN based implementations are tested and compared with the traditional trilateration based localization technique by varying the variance of RSSI measurement noise from 0 dBm to 5 dBm in the steps of 1 dBm. Out of all the ANN-based architectures, the GRNN based implementation demonstrates superior localization performance (lowest localization accuracy) irrespective of the nonlinear system dynamics, and the environmental dynamicity (uncertainty in noise distribution in RSSI measurements).

6 Conclusions and Future Work

In this research work the application of Supervised Learning based approach is introduced for target localization in WSN to deal with uncertainty in RSSI measurement noise due to various signal propagation. The proposed architectures are trained with 30 sets of four RSSI measurements from any four anchor nodes and corresponding actual locations of the target. The proposed architectures are validated using real-time RSSI measurements corresponding to 30 unknown locations. To account the fluctuations in RSSI measurements, the noise variance is varied from 0 dBm to 5 dBm in the steps of 1 dBm. The corresponding simulation and numeric results are given for the indoor area of 100×100 m^2. In all of these results it is found that, the proposed GRNN based localization algorithm outperforms the trilateration algorithm as well as rest of the remaining considered ANN architectures.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)

3. Khan, M.S., Capobianco, A.-D., Asif, S.M., Anagnostou, D.E., Shubair, R.M., Braaten, B. D.: A compact CSRR-enabled UWB diversity antenna. IEEE Antennas Wirel. Propag. Lett. **16**, 808–812 (2016)
4. Hero, A.O., Moses, R.L., Patwari, N., Ash, J.N., Kyperountas, S., Correal, N.S.: Locating the nodes: cooperative localization in wireless sensor networks. IEEE Signal Process. Mag. **22**(4), 54–69 (2005)
5. Hofmann-Wellenhof, B., Lichtenegger, H., Collins, J.: Global Positioning System: Theory and Practice (2001)
6. Shubair, R., Merri, A.: Convergence of adaptive beamforming algorithms for wireless communications. In: Proceedings of the IEEE and IFIP International Conference on Wireless and Optical Communications Networks, pp. 6–8 (2005)
7. Tariq, Z.B., Cheema, D.M., Kamran, M.Z., Naqvi, I.H.: Non-GPS positioning systems: a survey. ACM Comput. Surv. (CSUR) **50**(4), 57 (2017)
8. Wagner, B., Timmermann, D., Ruscher, G., Kirste, T.: Device-free user localization utilizing artificial neural networks and passive RFID. In: 2012 Ubiquitous Positioning, Indoor Navigation, and Location Based Service, UPINLBS 2012 (2012)
9. Zhang, Y., Li, X., Amin, M.: Principles and techniques of RFID positioning. In: RFID Systems: Research Trends and Challenges (2010)
10. Soltani, M.M., Motamedi, A., Hammad, A.: Enhancing cluster-based RFID tag localization using artificial neural networks and virtual reference tags. Autom. Constr. **54**, 93–105 (2015)
11. Zafari, F., Papapanagiotou, I., Devetsikiotis, M., Hacker, T.J.: Enhancing the accuracy of iBeacons for indoor proximity-based services. In: IEEE International Conference on Communications (2017)
12. Thaljaoui, A., Val, T., Nasri, N., Brulin, D.: BLE localization using RSSI measurements and iRingLA. In: Proceedings of the IEEE International Conference on Industrial Technology (2015)
13. Zhuang, Y., Li, Y., Qi, L., Lan, H., Yang, J., El-Sheimy, N.: A two-filter integration of MEMS sensors and WiFi fingerprinting for indoor positioning. IEEE Sens. J. **16**(13), 5125–5126 (2016)
14. Chen, Z., Zou, H., Jiang, H., Zhu, Q., Soh, Y.C., Xie, L.: Fusion of WiFi, smartphone sensors and landmarks using the Kalman filter for indoor localization. Sensors **15**(1), 715–732 (2015)
15. Blumrosen, G., Anker, T., Hod, B., Dolev, D., Rubinsky, B.: Enhancing RSSI-based tracking accuracy in wireless sensor networks. ACM Trans. Sens. Netw. **9**(3), 29 (2013)
16. Paul, A.S., Wan, E.A.: RSSI-based indoor localization and tracking using sigma-point Kalman smoothers. IEEE J. Sel. Top. Signal Process. **3**(5), 860–873 (2009)
17. Dong, Q., Dargie, W.: Evaluation of the reliability of RSSI for indoor localization. In: 2012 International Conference on Wireless Communications in Underground and Confined Areas, ICWCUCA 2012 (2012)
18. Abouzar, P., Michelson, D.G., Hamdi, M.: RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture. IEEE Trans. Wirel. Commun. **15**(10), 6638–6650 (2016)
19. Wu, H., Zhang, L., Miao, Y.: The propagation characteristics of radio frequency signals for wireless sensor networks in large-scale farmland. Wirel. Pers. Commun. **95**(4), 3653–3670 (2017)
20. Sarkar, T.K., Ji, Z., Kim, K., Medouri, A., Salazar-Palma, M.: A survey of various propagation models for mobile communication. IEEE Antennas Propag. Mag. **45**(3), 51–82 (2003)

21. Gharghan, S.K., Nordin, R., Ismail, M., Ali, J.A.: Accurate wireless sensor localization technique based on hybrid PSO-ANN algorithm for indoor and outdoor track cycling. IEEE Sens. J. **16**(2), 529–541 (2016)
22. Viani, F., Rocca, P., Oliveri, G., Trinchero, D., Massa, A.: Localization, tracking, and imaging of targets in wireless sensor networks: an invited review. Radio Sci. **46**(05), 1–12 (2011)
23. Coluccia, A., Ricciato, F.: RSS-based localization via bayesian ranging and iterative least squares positioning. IEEE Commun. Lett. **18**(5), 873–876 (2014)
24. Dai, H., Zhu, Z.M., Gu, X.F.: Multi-target indoor localization and tracking on video monitoring system in a wireless sensor network. J. Netw. Comput. Appl. **36**(1), 228–234 (2013)
25. Patwari, N., Hero, A.O., Perkins, M., Correal, N.S., O'Dea, R.J.: Relative location estimation in wireless sensor networks. IEEE Trans. Signal Process. **51**(8), 2137–2148 (2003)
26. Fang, S.H., Lin, T.N., Lee, K.C.: A novel algorithm for multipath fingerprinting in indoor WLAN environments. IEEE Trans. Wirel. Commun. **7**(9), 3579–3588 (2008)
27. Faragher, R., Harle, R.: Location fingerprinting with bluetooth low energy beacons. IEEE J. Sel. Areas Commun. **33**(11), 2418–2428 (2015)
28. Zheng, X., Liu, H., Yang, J., Chen, Y., Martin, R.P., Li, X.: A study of localization accuracy using multiple frequencies and powers. IEEE Trans. Parallel Distrib. Syst. **25**(8), 1955–1965 (2014)
29. Yoo, J., Kim, H.J.: Target localization in wireless sensor networks using online semi-supervised support vector regression. Sensors **15**(6), 12539–12559 (2015)
30. Jiao, J., Li, F., Deng, Z., Ma, W.: A smartphone camera-based indoor positioning algorithm of crowded scenarios with the assistance of deep CNN. Sensors **17**(4), 704 (2017)
31. AlHajri, M.I., Ali, N.T., Shubair, R.M.: Classification of indoor environments for IoT applications: a machine learning approach. IEEE Antennas Wirel. Propag. Lett. **17**(12), 2164–2168 (2018)
32. AlHajri, M.I., Ali, N.T., Shubair, R.M.: Indoor localization for IoT using adaptive feature selection: a cascaded machine learning approach. IEEE Antennas Wirel. Propag. Lett. (2019)
33. Dai, H., Ying, W.-H., Xu, J.: Multi-layer neural network for received signal strength-based indoor localisation. IET Commun. **10**(6), 717–723 (2016)
34. Gogolak, L., Pletl, S., Kukolj, D.: Neural network-based indoor localization in WSN environments. Acta Polytech. Hungarica **10**(6), 221–235 (2013)
35. Mahfouz, S., Mourad-Chehade, F., Honeine, P., Farah, J., Snoussi, H.: Target tracking using machine learning and Kalman filter in wireless sensor networks. IEEE Sens. J. **14**(10), 3715–3725 (2014)
36. Jondhale, S.R., Deshpande, R.S.: Kalman filtering framework-based real time target tracking in wireless sensor networks using generalized regression neural networks. IEEE Sens. J. **19** (1), 224–233 (2019)
37. Jondhale, S.R., Deshpande, R.S.: GRNN and KF framework based real time target tracking using PSOC BLE and smartphone. Ad Hoc Netw. **84**, 19–28 (2019)
38. Kaplan, G.B., Lana, A.: Comparison of Proposed Target Tracking Algorithm, GRNN α, to Kalman Filter in 3D Environment (2013)
39. Kişi, Ö.: Generalized regression neural networks for evapotranspiration modelling, vol. 6667 (2010)
40. Zhong, M., et al.: Gap-based estimation: choosing the smoothing parameters for probabilistic and general regression neural networks. Neural Comput. **19**(10), 2840–2864 (2007)

41. Jondhale, S.R., Deshpande, R.S.: Kalman filtering framework based real time target tracking in wireless sensor networks using generalized regression neural networks. IEEE Sens. J. **19** (1), 224–233 (2018)
42. Rahman, M.S., Park, Y., Kim, K.D.: RSS-based indoor localization algorithm for wireless sensor network using generalized regression neural network. Arab. J. Sci. Eng. **37**(4), 1043–1053 (2012)
43. Jondhale, S.R., Deshpande, R.S.: Modified Kalman filtering framework based real time target tracking against environmental dynamicity in wireless sensor networks. Ad-Hoc Sens. Wirel. Netw. (2018)
44. Yang, Z., Liu, Y., Li, X.Y.: Beyond trilateration: on the localizability of wireless ad hoc networks. IEEE/ACM Trans. Netw. (2010)
45. Uren, J., Price, W.F.: Triangulation and trilateration. In: Surveying for Engineers (2015)
46. Specht, D.F.: A general regression neural network. IEEE Trans. Neural Netw. **2**(6), 568–576 (1991)

Implementation of Automated Aroma Therapy Candle Process Planting Using IoT and WSN

Siti Nor Zawani Ahmmad[1], Muhammad Tarmizi Mokhtar[1], Farkhana Muchtar[2(✉)], and Pradeep Kumar Singh[3]

[1] Instrumental and Control Engineering, Universiti Kuala Lumpur, MITEC, Persiaran Sinaran Ilmu, Bandar Seri Alam, 81750 Masai, Malaysia
sitinorzawani@unikl.edu.my, tarmiziemokhtar@gmail.com
[2] School of Computing, Faculty Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia
farkhana@gmail.com
[3] Department of CSE&IT, Jaypee University of IT, Waknaghat, Solan 17334, Himachal Pradesh, India
pradeep_84cs@yahoo.com

Abstract. Aromatherapy candles with essential oils which can provides a therapeutic treatments have been made to maintain and improve our wellbeing. In this paper, a mini prototype of automated aromatherapy candle process plant using IoT and WSN has been proposed and developed. The main process of producing aromatherapy candle are heating and mixing. To produce the right quality of the aromatherapy candle, the quantity of the raw material is important. Heating process will be control by using ESP8266 based PID controller and monitored by using Open Source Programmable Logic Controller called OpenPLC that run on Raspberry Pi. The software is efficient because can support users over the entire plant and process. Mixing process will mix the raw material evenly using agitator motor with specific temperature. The whole process in this work can be monitored and control through PC via this implementation of software. To obtain the best quality of this work, the set point of temperature need to be control and the plant able to be achieved after second test of the study. As the result, this study able to produces aromatherapy candle with better quality in minimal time. This study also able to control the candle from releasing too many Volatile Organic Compound that can effect human life. Armed with the wealth of relevant information presented in this article, it is hoped that readers will have greatly benefited and gained a thorough understanding on how to develop an automated aroma therapy candle process planting using IoT and WSN. With further research put forth into this study, it is also hope it could be an advantage in innovation development and can be implemented in real life manufacturing industry.

Keywords: Internet of Things · Wireless Sensor Network · Aroma therapy · Candle

1 Introduction

Aromatherapy candle is one of the method used to relief stress. It also can create more soothing atmosphere and did not produce too much smoke [1]. Traditionally, the process of making candle was make manually, especially in controlling the

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 520–545, 2020.
https://doi.org/10.1007/978-3-030-40305-8_25

temperature. Based on previous study, when temperature of melting the wax was not been controlled and monitored, it makes wax released too many type of Volatile Organic Compound (VOC's) to the air and can be harmful [1].

According to Guzialłowska-Tic [2], the suitable temperature for melting and mixing wax is 80 °C which the wax will not release too much VOC's. In addition the suitable temperature to mix with essential oils is 40 °C [3]. Thus it is very important to control specific set point of temperature during the process. However it is very difficult to control using traditional method.

Hence, in order to overcome this problem, automated aromatherapy candle process plant will be developed. The method of controlling and monitoring the temperature of melting wax will be implemented by using Programmable Logic Controller. This method can produce better quality of aromatherapy candle.

The whole process in this study will be controlled and monitored using OpenPLC as human machine interface (HMI) for mini plant. The main process in this work are heating, mixing and cooling process. For the heating process, heating coil will be used to melt the soy wax inside the heating tank until reach the set point which is 71 °C. For mixing process, an agitator motor will be used to mix the raw material. The purpose of cooling process which is to add essential oil at 40 °C.

This paper is organized as follows. In Sect. 1, background information on former research carried out of automated aroma therapy candle process planting is detailed. Section 2 present the literature review. We study and explain about the previous study of raw material of candles that use natural sources. In addition, we also explains about type of candles, benefit using soy wax using natural sources and explain about essential oil in candles making. In Sect. 3, we explains about the process in making the prototype such as the hardware for making prototype and software we have used for programming the prototype. Section 4 presents the result and discussion for mini prototype of automated aromatherapy candle process plant. And finally, in Sect. 5, the research is summarized and the future goals of this work are out lined.

2 Literature Review

In the early phase of this venture, many literatures have been reviewed to get the rough idea about the venture and basic instrument that are reasonable for this study. This section mainly discusses about aromatherapy candles that use natural sources as raw material.

2.1 Candles

Based on national candle association history, in 200 BC the earliest candles originated in Han China that are made from whale fat. After that the candles manufacture became industrialized mass market in the mid-19th century. In 1834 Joseph Morgran from Manchester, England, patented a machine that revolutionised candle making process. He create continuous production of moulded candles by using a cylinder with a movable piston to eject candles as they solidified. At the first half of 20th century, the interest in candles for mood-setters, decorative items and gift become to increase.

Candles are made with different sizes, shapes, colour and scented. The raw material that regularly use is based on soy wax, beeswax, paraffin wax, gel wax and stearin. Today, candles are long way from the purpose of the initial use. Customer less needed a candle as a source of light. Celebration, soothe the senses and accent home decor is now symbolize of the candle. Candles also have the different propose of usage depending on the material of the candles itself. Aromatherapy candles use essential oil as the addition to create therapeutic treatment that are safe to use to humans and environment. Scented candles made by using fragrance to create a good smell. However, a major problem with this kind of material is it release all types of organic compounds that really bad damage for human and environment [4].

2.2 Candles Type

There are several types of aroma candles that widely use nowadays have two different category which is scented candle and aromatherapy candle. There also have different from every types of candle based on their material usage for candle making. Matthai and Petereit [5] state that raw material have different advantages and disadvantages that important to create the candle and purpose of produce the candle.

2.2.1 Scented Candles

Scented Candle usage is to unpleasant odours and give more relaxing ambiance. Scented candle been made by using the raw material of fragrances for the scented aroma. The material to form a candle is different based on their manufacturing company. A recent study by Alsayyad [1] state that scented candle are dangerous both before lighting and when lit. Scented candles release different kinds of Volatile Organic Compounds (VOCs). Several experiment conducted in the lab in order to analyse the distinctive characters of the VOCs emitted from scented candles using six type of candles that have been mention in Table 1 below. From the experiment, some types functional groups that are emitted from scented candles which is alcohol, aldehyde, hydrocarbons and polycyclic aromatic hydrocarbon (PAHs). These result based on research done in [6]. According to The Department of Health and Human Services (DHHS) state that some PAHs can develop cancer when touching candle and breathing candle smoke.

Table 1. Six type of candle test

Name	Code
Clean cotton	CT
Floral	FL
Kiwi melon	KW
Strawberry	SB
Vanilla	VN
Plain	PL

2.2.2 Aromatherapy Candles

Aromatherapy candle have been started to create a therapeutic treatment, designed to maintain or improve our wellbeing. Aromatherapy candle can be made by using any type of wax based on their needs and preferences. Manufacturing company always prefer to use para n wax because para n wax is easily to get and the cost is lower other than other type of wax. The wax itself have different purpose of usage such as gel wax use to create a transparent candle. According to Barnett et al. [7] reason of aromatherapy candles is to replace the aromatherapy technique that widely use nowadays such as aromatherapy massage and di user. Furthermore, according to Baldwin [8] and Siledar [9], aromatherapy candle technique also can help to release anxiety and panic attack.

Then, the main important material to create aromatherapy candle is essential oil. Essential oil is better than synthetic fragrance. Thus, there are extracted from the flowers, barks, stem, leaves, roots, fruits and other part of the plant by various methods [10–12]. Based from this element, the best aromatherapy need to be create by using essential oil that have been extracted from natural sources. Aromatherapy also have many classification such as cosmetic, massage, medical, olfactory, and psycho aromatherapy that use to help surrounding free from disease, bacteria and fungus. Figure 1 below shows the ways of essential oil extraction.

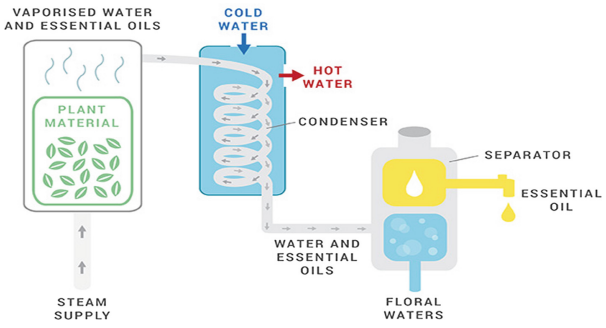
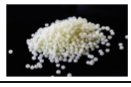


Fig. 1. The extraction of essential oil

2.3 Soy Wax as Raw Material

Wax is the important source to create the candle. Nowadays many type of wax can be founds such as para n wax, beeswax, soy wax that have been illustrated in Table 2 below.

Table 2. Type of wax

Paraffin Wax	Bees Wax	Soy Wax
		

For choosing the right material to create the most safety aromatherapy candle is very important. Paraffin wax appeared in a print is in as early as 1957. Paraffin wax is made from petroleum by dewaxing of light lubricating oil [13–15]. It's also the most popular wax that have been use nowadays. Paraffin wax have been identified had major problems that they were brittle and di cult to remove from moulds [15, 16]. He also stated that para n wax also may produce high concentration of VOCs in air. Paraffin wax is the most popular kind of raw material in candle making nowadays because para n wax is low cost wax with the material performance and burning time. American Chemical Society stated that para n wax also the highest emitted toxic chemical like toluene and benzene. We also say that lighting a para n candle can pose a health threat.

Other source or raw material is beeswax which is natural source of wax that came from bees. Beeswax is the top of highest cost wax because it took sixty pound of honey to produce one pound of beeswax. Beeswax also considered as agricultural product [16–18]. The disadvantages of beeswax to create the aromatherapy candle is, beeswax have their own smell of honey because it's have been create from honey. It is not suitable for using to create aromatherapy candle because when they mix to essential oil, the smell of aromatherapy become bad. Beeswax also a yellowish colour which is not easy to mix with dye to create the colour of what the manufacturer needs.

From the three raw material that have been stated, the best way to create the aromatherapy candle is soy wax. Soy wax is produced from soybeans. It is a pure and natural vegetable. Soy wax also as a nontoxic and biodegradable material. In fact, soy wax is very environmentally friendly and is made from a renewable resource. Candles that are made from soy wax are very clean burning because it's have reduction in soot and the burn time is very high. According to Rezaei, Wang and Johnson [19], soy wax is the most economical candle. In fact, soy wax have their pure white colour that easy for manufacturer to create their own colour of candle by mixing with the dye colour.

2.4 Lavender as Aromatherapy

Lavender (Lavandula officinalis Chaix) (see Fig. 2) is a beautiful herb of the garden belonging to the family of Lamiaceae. It also have a different species that create varies in concentration and therapeutic effects. However, lavender herbs also contain linalyl acetate and linalool that have maximum and great absorbing properties [20]. These will help anxiety patients with sleep disturbance pattern, improving the feeling of wellbeing, supporting mental alertness and suppressing aggression and anxiety according to the study of Koulivand, Ghadiri and Gorji [10]. Then, from the study, they also mention that lavender oils shows its antibacterial and antifungal properties against many species of bacteria especially when antibiotics fail to work. When taking to the aromatherapy technique, it is well performed for the treatment of abrasions, burns, stress, headaches and boosting an immune system that have been state in study from Tisserand and Young [21] and Karaman et al. [22]. This herb is good for our raw material to create the aromatherapy candle compared to other fragrance that widely use nowadays.

Based on the study of Alsayyad [1], Liu et al. [23] and Lucattini et al. [24], fragrance release many type of volatile organic compounds (VOCs) that can cause indoor pollution. Graham, Janssen and Sanders [25] reported that one of five people in

the U.S are adversely affected from exposure to fragrance. Fragrance is a known respiratory irritant and neurological toxin. For many people such as those exposed to asthma, exposure to perfume can pose serious health risk such as migraines, nausea, and respiratory impairment. From this result, the company that claim they are creating aromatherapy candle by using fragrance as a natural raw material is not safe for the user as long-term effect.

Fig. 2. Lavender (Lavandula officinalis chaix)

2.5 Process Controlling Method

Temperature control method is widely use in process plant. In candle making, heating process will be involved to make the raw material of wax to melt for creating the shape of candle itself. Many industry of candle making are not using temperature control because they just melt the wax from solid to liquid formation. The important of controlling the temperature is for the safety of controlling concentration of VOCs in air. Previous study have shown [2] that the boiling point of candle at 800 C is the best for melting the candle wax because it doesn't release high concentration of VOCs in the air. Hence, for this project temperature at 710 C will be selected to melt the wax for the safety purpose of the manufacturing plant.

From other side of study conducted by Cooke and Ernst [3], ash point of essential oil such as lavender is 500 C to 600 C. Based on this study, our project will conduct the controlling method of 2 different temperature which is at 800 C for the melting of soy wax and 400 C for mixing of the essential oil in the soy wax. From this study, we know that we can control the safety issue of manufacturing candle for the safety purpose. The main controlling method that will be choose by using Programmable Logic Controller (PLC) because it more efficient and easy for monitoring. PID controller will be add to control the heating process.

2.5.1 Heating Control

Temperature controlling is important in this study. For this study, heating need to use PID controlling method which is to control the set point of the heating process. PLC have that type of controlling method but need to use temperature transmitter that give an input 4–20 mA to the PLC [26]. In this study, low budget on for construct the prototype, temperature transmitter cannot be used because the price is too high. The type of sensor will be replace with thermocouple and the PID controller will be use ESP8266. According to Knospe [27], PID control can control the temperature in desired set point which is heating is fast response to the current temperature.

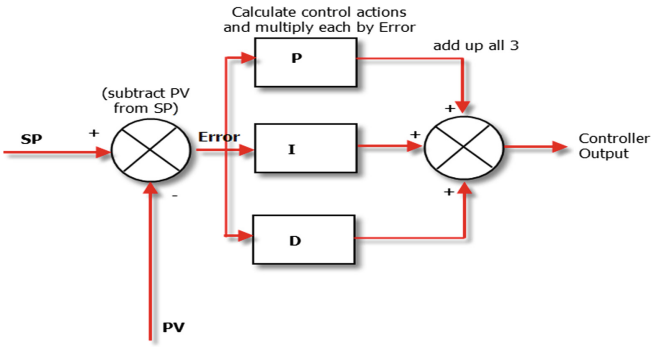


Fig. 3. PID controlling method

Figure 3 shows the type of PID controlling method which is use Proportional, Integral and Derivative. Study from Åström and Hägglund [28] by using three of the control will eliminate more error for the controller to reach the set point od controller. The feedback of the control temperature will be more effective and the heating process will take less time. The lowest time of production of making candle is very important because when the time taken is low, the cost of production can be decrease. Production cost is important to the company to gain more profit [29].

From other side of study from Wu et al. [30], designing the PID controlling method and tuning is needed when the process have to control the set point. Set point need to be accurate and less error to get the good result of production.

2.6 Literature Review Summary

Table 3 shows the literature review of the summary from journal that have been discussed in this section.

Table 3. Summary of literature review

Author	Review	Proposed Method
Matthai & Petereit (2004) [5]	Different wax have different advantages and disadvantages of the own usage. GSM and GPRS module	Soy wax have been choose from this study. Soy wax have long lasting burning and great soothing of the candle
Koulivand et al. (2013) [8]	Lavender plant have the great usage to create the aroma that can relief stress	Lavender essential oil will be use as raw material to create aromatherapy candle because of their great usage
Alsayyad (2016) [1]	Scented candles create high VOCs when melting of the wax are not safe to manufacturing and user	Essential oil will be use to avoid harmful for the manufacturing and user
Guzialłowska-Tic (2013) [2]	Wax need to be melt at specific temperature to avoid over melting of the wax	Development of temperature control and monitoring in this work will be applied

3 Design, Process Flow and Development of Prototype for This Study

3.1 Overview of Prototype Development

This section will explain about the project specifications and the project operates. In this section also will explain in details the process of developing and contract this project. The material and component used in this project will also explain in details. The project design will be also explain in this section.

3.2 Project Specification

See Table 4.

Table 4. Project specification

Item	Specification
Name of project	Automated aromatherapy candle process plant
Main process	Heating process
Operation mode	Auto and manual
Raw material	Soy wax, Lavender essential oil, Dye
Types of controller	PLC
Total process	Heating process, Mixing process
Inflow	Soy wax/Lavender Essential Oil/Dye
Product	Aromatherapy Candle

3.3 Project Flow

Figure 4 shows the major process involved in our aromatherapy candle process plant. The process starts with filling the raw materials which is soy wax into heating tank. After the raw material put into the main tank for heating process. The heating process will take place for 30 min with temperature 710 C and agitator for mixing the wax. After heating the raw material for 30 min, the heater will turn off to process the next stage which is cooling to 400 C. When the temperature reach at 400 C the essential oil and dye colour will be adding to the heating tank and mixing process will take place to make sure the raw material merge perfectly together. The mixing process will take 15 min. After mixing process, the end product will be produced.

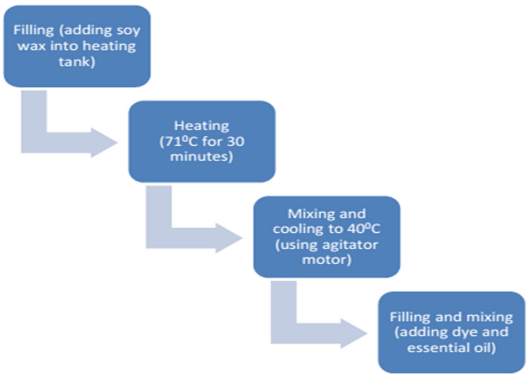


Fig. 4. Diagram for overview of process

3.4 Project Flowchart

Figure 5 shows the flowchart of the total process to create aromatherapy candle from start to the end of process.

3.5 P&ID Diagram of This Study

Figure 6 and Table 5 below shows the P&ID diagram for the aromatherapy process plant.

Figure 6 show the P&ID diagram for the aromatherapy candle process plant. Tank 1 used for soy wax, tank 2 for dye colour and tank 3 for the essential oil. Motorized ball Valve have been used because powder of soy wax need fully opened valve for efficiency flowing. Double boiler for heating tank have been used because the wax cannot directly heated. If the soy wax directly heated, the melting of wax is taking longer time. Motor pump have been used because easy to calculate the ratio of the raw material to create the good quality of the candle. Agitator motor used for mixing of the raw material to create the best colour and aromatherapy for the candle. Temperature transmitter used as the sensor of temperature that need to be control in this process. All of the electrical component have been connected to the Programmable Logic Controller for the controlling method of the process plant. Table 5 shows the legends for the P&ID diagram.

3.6 Hardware Development

This section will discuss about the components used in hardware implementation, which involved Programmable Logic Controller, temperature sensor, solenoid valve, heating element (coil), dc motor 12v for mini prototype of automated aromatherapy candle process plant.

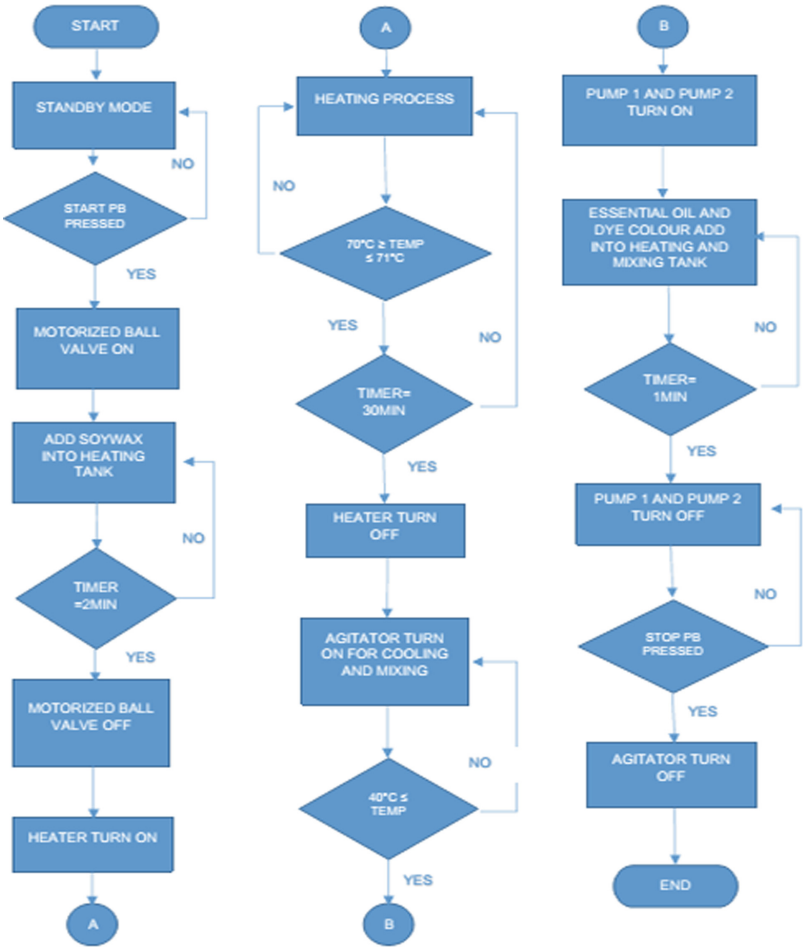


Fig. 5. Flowchart diagram

3.6.1 Programmable Logic Controller

PLC is the one of the most important equipment that need to have in our study because programmable logic controller use to run and control the process that involve in our study and without programmable logic circuit we cannot process our plant automatically.

3.6.2 Thermocouple Temperature Probe

Table 6 show thermocouple type K temperature probe that will be used in this study to sense and monitor the temperature in process. Thermocouple consist of 2 wire legs made from different metals. The wires legs are welded together at one end, creating a junction. This junction is where the temperature is measured. When the junction experiences a change in temperature, a voltage is created. This sensor will be used because have a wide temperature range, great precision and this relationship is around straight over a little range.

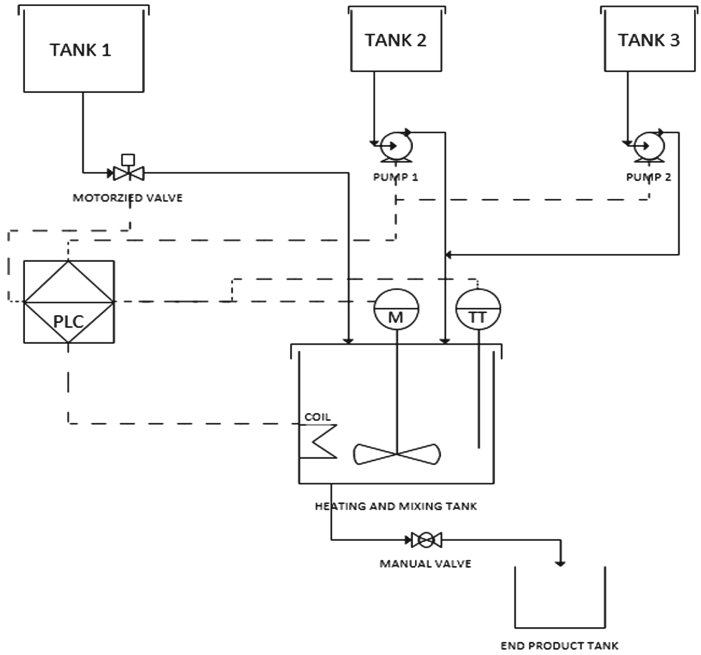


Fig. 6. P&ID diagram

Table 5. Legends for P&ID diagram

Legends	Description	Ratio
Tank 1	Soy Wax Tank (Raw Material)	5 L
Tank 2	Dye Storage Tank (Raw Material)	2 L
Tank 3	Essential Oil Tank (Raw Material)	2 L
End Product Tank	Product Tank (Aromatherapy Candle)	8 L
Heating and Mixing Tank	Heating and Mixing Process Tank	8 L
Pump 1	Water Pump 1	1.5–2/Liter per minutes
Pump 2	Water Pump 2	1.5–2/Liter per minutes
Manual Valve	Manual Ball Valve	10 L per minutes
Motorized Valve	Motor Operated Ball Valve	10 L per minutes
M	Agitator Motor (Power Window Motor)	85 Rpm
COIL	Immersion Heating Coil (Heater)	2500 W
PLC	Programmable Logic Controller	–
TT	Temperature Transmitter	–

3.6.3 Solenoid Valve

An electrical motorized ball valve in Table 6 is controlled by an electric current and an electromechanically worked valve. Usually an electrical ball valve has two conditions such as normally open and normally closed, the condition worked depend on the process. Fluids always be a control element for ball valve. Their main functions are to stop, discharge, and measurements, disperse or blend liquids. Electrical motorized offer quick and safe exchanging, high dependability, long administration life, good medium similarity of the materials utilized, low control power and minimal outlines.

3.6.4 Agitator Motor

An Agitator motor in Table 6 used in industries that process food, chemical, cosmetic product and pharmaceutical. There are several reasons to use this agitator motor such as to mixing the product and to promote the reaction of chemical substances. The main function this agitator motor to mix fluids, liquids specifically.

3.6.5 Immersion Heating Coil

Immersion heating coil in Table 6 will be used to heat up the water for heating process. This heating coil is an electrical device that converts electric current to heat. The heating element inside every electrical resistor, and works on the principle of joule heating, an electric current passing through a resistor will convert that electrical energy into heat energy. Most modern electric heating devices use nichrome wire as the active element and the heating element, depicted on the right, uses nichrome wire supported by ceramic insulators.

3.6.6 Water Pump

DC motor pump in Table 6 is DC powered pumps use direct current from motor, battery, or solar power to move fluid in a variety of ways. Motorized pumps that have been use id 12VDC. DC pump consume low power voltage and very efficient. The price also affordable then other pump. This pump has been choose because the pump flow for 1.5–2/L per minutes.

3.6.7 PID Controller as Temperature Controller

For temperature controller purposes, combination of ESP8266 microcontroller and Solid State Relay (SSR) are used to replace traditional REX-C100 PID controller in original design. The purpose is to make the machines we develop more modular and flexible using IoT and WSN (Wireless Sensor Network) methods at low cost.

ESP8266 microcontroller is a cheap and reliable IOT and WSN solution that can replaces traditional PID controller like REX-C100 as a temperature controller by providing additional features needed to create a more autonomous and modular system. The components for temperature controller that we recommend can be seen in Table 6.

IoT and WSN technology allows mixing and heating tank modules to be in different locations with main controller modules. At the moment we can increase the number of units for the mixing and heating tank module according to current requirements without going through complex wiring and setup. Addition of serial socket and serial cable is not required, on the contrary on PLC only need to add new serial port based on IP address for new temperature controller.

Programming logic in ESP8266 still acts like the original PID Controller with the addition of PLC intercepts wirelessly for monitoring purposes. We maintain a PID controller approach though using ESP8266 for robustness and simplicity of PID controller approach in implementing autonomous process for manufacturing machine.

Temperature controller on mixing and heating tank is connected to PLC wirelessly with serial over Wi-Fi method without requiring serial cable connecting temperature controller and PLC to be connected physically. SSR is used to replace power regulator because SSR provides the same function as power regulator at a lower costs.

The use of IoT and WSN technologies through ESP8266 also allows configuration to be done wirelessly using the web console without having to physically work on the PID component. This is to simplify the configuration process through a smartphone or laptop without having to go to the physical location of the heating and mixing tank itself.

Table 6. Temperature controller components

			
Programmable Logic Controller	Thermocouple Temperature Probe	Solenoid Valve	Agitator Motor
			
Immersion Heating Coil	Water Pump	PID Controller as Temperature Controller	

3.7 Software Development

OpenPLC Editor is used in this project for programmable logic circuit in OpenPLC on Raspberry Pi. This software is efficient because can support users over the entire life cycle of machine or plant. This software also permits a high degree data consistency through the entire engineering process.

3.8 Control Loop

3.8.1 Heating Process

Figure 7 and Table 7 shows the control element of heating process Temperature indicator controller used to control the temperature of the heating process in manual mode, for the auto mode it will be used PLC and ESP8266 (internal temperature controller) to control the temperature. To control the temperature we used an immersion coil (FCE) and heating process is a continuous process. We used continuous process because we want to heat our product continuously.

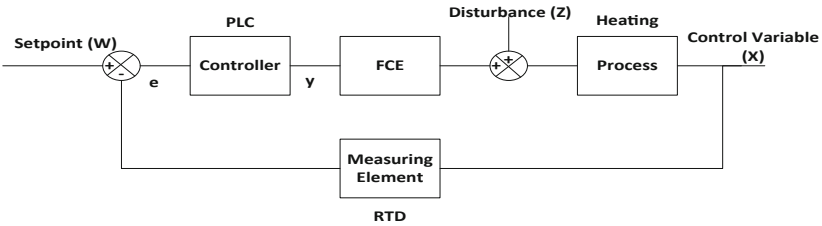


Fig. 7. Heating process

Table 7. Specification of heating process

Controller	OpenPLC on Raspberry Pi and ESP8266
Final Control Element (FCE)	Heating element (immersion coil)
Process	Heating
Transducer	Resistance Temperature Detector (PT 100)

3.9 Prototype

3.9.1 Actual Prototype

The development of prototype is the first objective for this project. The development of this project include hardware and software. Hardware of this project include plant manufacturing and electrical wiring diagram.

Fig. 8. Actual aromatherapy candle process plant

Figure 8 show that the development of this plant using 70% of metal, 20% of plastic and 10% of stainless steel material. The main tank which is heating tank is using stainless steel because the maximum temperature of the stainless steel is 500 C. Stainless steel material have its own advantages and physical properties, the most popular advantage is its resistance to corrosion [31]. For the piping system of aromatherapy candle process plant is using PVC because of the ease to find the type of piping and easy for installation.

3.9.2 Wiring Diagram (Electrical Control Circuit)

Electrical control circuit is main control for electrical equipment. Figure 10 show that the control circuit for start, stop and emergency push stop button for equipment that use 230 V supply. There also for the controlling the heater and PID control because the equipment use 230 V supply. Figure 11 show the electrical circuit 12 V supply for every instrument that use 12 V supply. Each equipment must have their own control circuit with different voltage that use by the equipment to run the plant (Fig. 9).

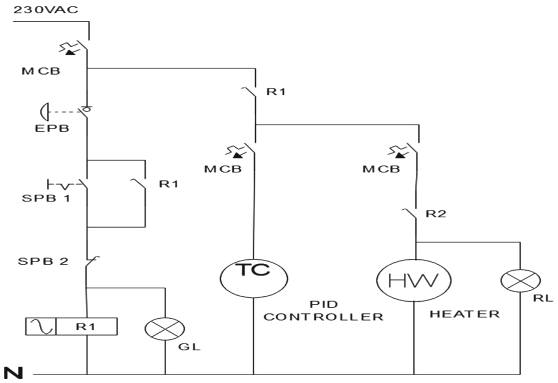


Fig. 9. Electrical control circuit for 230 V

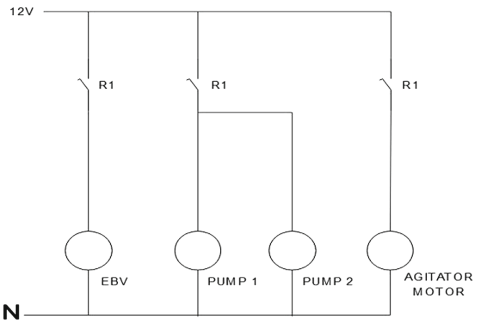
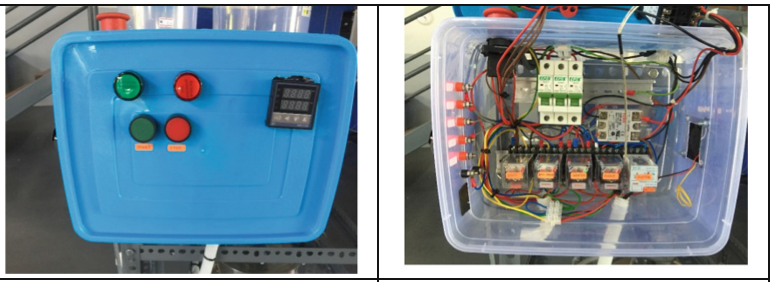


Fig. 10. Electrical control circuit for 12 v

3.9.3 Actual Electrical Control Panel

Figure 12 show the actual wiring for electrical control circuit. Control panel for electrical control circuit is using plastic box for easy installation of the electrical component. The control panel contain ESP8266, MCB, Relay, SSR, cooling fan, start and stop push button with light indicator.



Electrical Control Panel	Electrical Wiring

Fig. 11. Actual wiring for electrical control circuit

3.10 Control and Monitoring Program

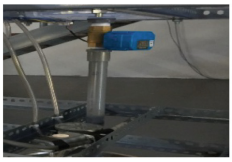
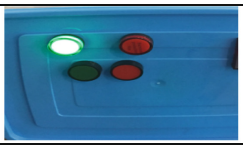
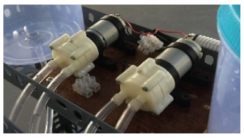
To develop innate food colouring plant, the control system is the main and compulsory part in the project. It is used to control the process parameter such as water temperature when heating, water level in the tank and liquid mixing. This plant will be controlled by using Open Source Programmable Logic Controller, OpenPLC on Raspberry Pi with communication to temperature controller using serial over Wi-Fi. The programming architecture was built using ladder programming method that involved normally open (NO), normally closed (NC), Timer (TIM), Holding, Interlock and also Memory function for analogue or digital input. The operation of this project can be controlled at the plant by easily pressing the push button. Temperature controller is used to control and monitor the temperature for this project.

This work involve to create software to run the hardware. In this project, we use ladder diagram for PLC to run this work. To make automated process plant, automation is important to run every process in sequence.

3.11 Actual Process Sequence

The sequence of this work is important to make a good aromatherapy candle. Set point of heating need to be at 71 °C. The sequence is important because the essential oil and dye colour cannot be add at the higher temperature that make the essential oil will be evaporate. The aroma of the candle will be low and the quality of the candle not in good condition. Table 8 show the process sequence of running the automated aromatherapy candle process plant.

Table 8. Actual process sequence

Step 1		Prepare the material to start the process. 1.Soy wax as main raw material 2.Essential Oil for aromatherapy 3.Dye colouring for colouring the candle
Step 2		Turn on the main supply for 240V and 12V and the process ready to start.
Step 3		Turn on the electrical control circuit by push the start button. Green indicator will indicate that the plant in ON MODE. The controller show the ambient temperature at 33°C.
Step 4		Run the program in PLC and process will start in sequence. Motorized ball valve will on at 1st sequence to add soy wax.
Step 5		After that, the heater will turn on until the 71°C to start heat the soy wax from solid to liquid phase. The red indicator indicate that heater in on mode.
Step 6		Then, the agitator will turn on after 5minutes. Heating and mixing the soy wax will happen at this process sequence.
Step 7		After 20minutes heating the soy wax at 71°C, heater will turn off and red lamp will turn off but agitator still turn on to cooling the soy wax before adding the essential oil and dye colour.
Step 8		When temperature goes down at 40°C, pump 1 and 2 will turn on to add the essential oil and dye colour. Mixing process will continue for 10minitues to mix the material evenly.
Step 9		The process will stop and the end product can be collect by open the manual ball valve.

4 Result and Discussions

4.1 Controlling the Heating

4.1.1 Result for 1st Running Test

Figure 12 show the graph of time vs temperature for the data analysis of the controlling temperature at desired set point. For the 1st run of the heating process. The temperature is start increasing from 32 °C until 58 °C in 5 min. Then the temperature is decreasing to 55 °C because the agitator is start to turn on from sequence of the process. The temperature decreasing because there are heat loss in the tank from mixing process of agitator.

At minutes 6, the temperature start to increase back to reach the set point at 71 C. It takes 10 min to reach to the set point but the temperature do not stop at desired set point which is 71 C. The temperature is overheating until 78 C at minutes 23. Emergency stop button have been push to stop the process to avoid the raw material from damage.

After stop the process plant, problem that have been encountered is the heating is over heat. Troubleshooting for the PID Controller to get the desired value is done. According to Crenganis et al. [32], Zigler-Nicols tuning method for PID can encountered the overheating of the temperature.

Setting of PID controller should be change to follow the heating of process that have been made. This countermeasure is follow according to the Saleh et al. [33] that state the PID controller can be used in auto tuning. After changing the default setting to

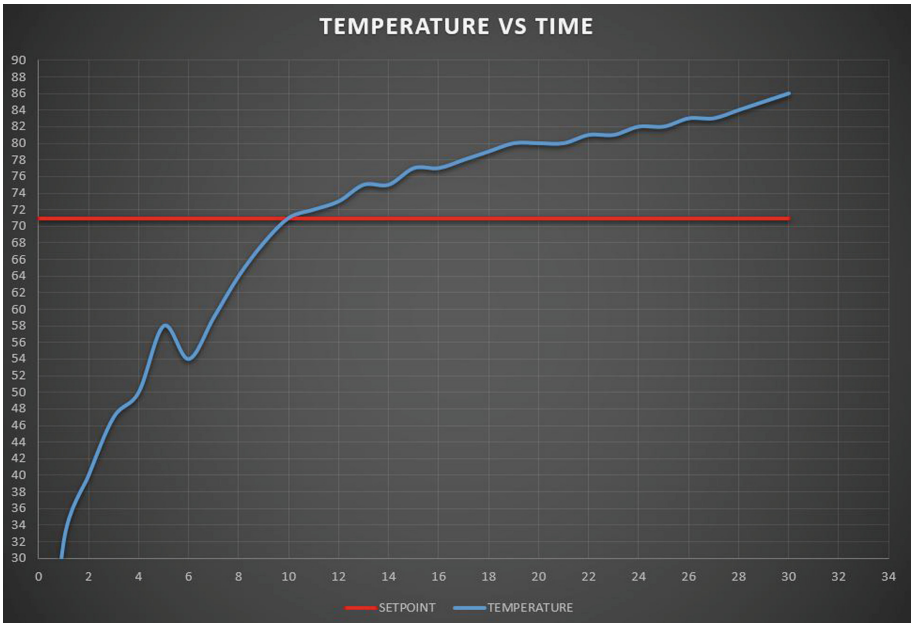


Fig. 12. Graph 1st test

the follow setting, auto tuning of the PID controller can be use, second test will be run to get the desired set point of heating.

PID controlling method is very efficiency because its tune by Proportional, Integral and Derivative. By using the PID controller it can be set to auto tune the value of PID by itself. Auto tuning is easier way because its tune follow to the type of liquid that sensor detect. The controlling is more accuracy [34].

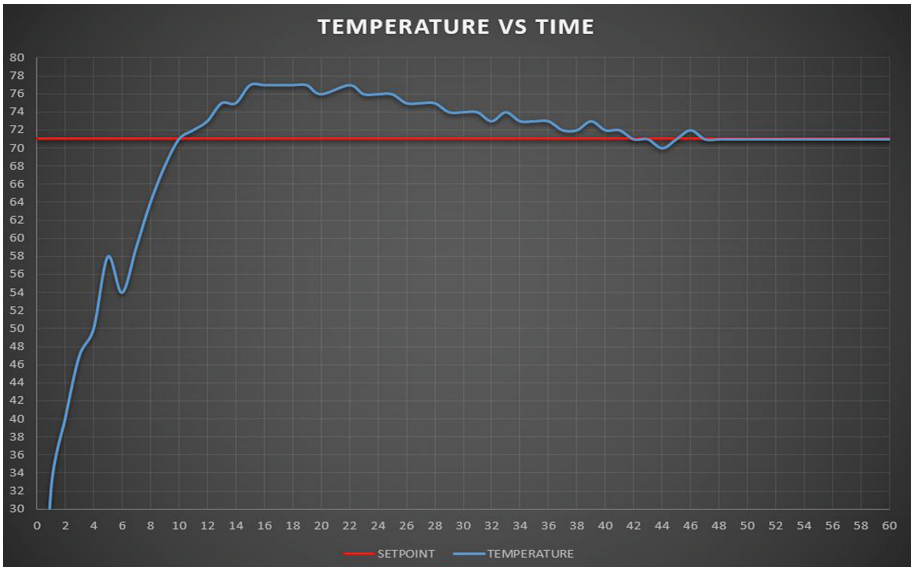


Fig. 13. Graph for 2nd test

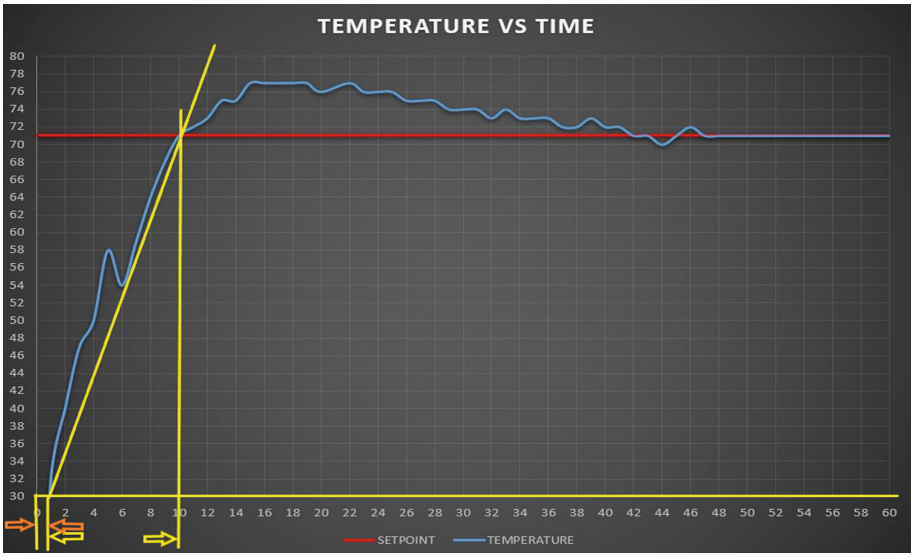


Fig. 14. Open loop tuning graph

4.1.2 Result for 2nd Running Test

Figure 13 show the result for the 2nd test. The result of temperature for heating until 55 °C as the same as the 1st test which is 5 min heat reach to temperature and temperature decreasing because of agitator turn on at minutes 5. The problem that happen in 1st run which is heater in overheat to 78 °C and desired set point is not reaching. After setting the PID controller. As we can see in the Fig. 13, the temperature is increasing until 75 °C but in slow time. The temperature stop increasing at 75 °C and start to decreased slowly.

After 20 min, the temperature decreasing to the desired set point which is 71 C. According to Vega, Sanz and Abascal [35], longer time is needed to decrease the temperature. The heating process is continue to maintain at 71 C until 20 min to get the right quality of aromatherapy candle.

4.1.3 PID Tuning Graph

Figure 14 above show the closed loop tuning graph where the process of heating candle is tuned by setting the PID controller. To set the proportional (P), integral (I) and derivative (D) the process plant need to be run to get the data analysis. The data can be analysed and do calculation to get the best PID value for the process plant. Using Ziegler-Nicholas closed loop tuning method, the value of the proportional gain (Kp), integral gain (Ki) and derivative gain (Kd). After the step input is triggered the heating process is started at minute 0, the temperature start to rise at 1st minute. The delay time (Tu) is can be measured and after the temperature is reach the set point, 71 °C (Table 9).

The value of proportional (P), integral (I) and derivative (D) are set to 0.13, 2 and 0.5 respectively at the PID controller. This is the best tune for the heating of candle as the data is measured and calculate.

Table 9. PID tuning formula

	Kp	Ki	Kd
PID Formula	1.2/(Tg/Tu)	2Tu	½ Tu
Tu = 1 − 0 = 1 Tg = 10 − 1 = 9	Kp = 1.2/(9/1) = 0.13	Ki = 2*(1) = 2	Kd = 0.5 (1) = 0.5

4.1.4 Ratio of Raw Material

Table 10 show the result for 4 test of experiment have been done get the correct amount of ratio for the best quality of the candle. Test no 1 show the essential oil have been use 10% from the quantity of the wax and 5% of dye colour. The result show that the candle is good for the emission of candle soot because does not produce any emission but the smell and candle colour is in low point. The burning time of the candle is good for the quality. For the test no 2, the quality of raw material test have been done by using the recipe that stated by author in [5]. 20% of essential oil and 10% of dye colour have been use. The result of the candle is no emission of soot which is good for the candle. Burning time of the candle also as a high which is long lasting but the candle smell and candle colour is in medium which mean the candle cannot produce the

good aromatherapy. For the test no 3, the ratio of raw material have been increase 10% for essential oil and 5% for dye colour each test. The result shows the candle produce the emission of soot in low condition for test no 3 and high emission for test no 4. Emission of soot for candle is not good for the health of users. Burning time of candle will be decrease because the ratio of essential oil and dye colour have been add more. For the result, the burning time of the candle is depending on the ratio of two raw material which is essential oil and dye colour. Candle smell is not enough for test no 3 but in good smell for test no 4. Candle colour is high when the ratio of dye colour exceed 15% from the wax ratio. For this result, the quality of candle is determine by the burning time of candle and the smell of the candle. Test no 2 have been in good quality to create the best aromatherapy candle process plant.

Table 10. Ratio Test

Test No	1	2	3	4
Wax (kg)	2 kg	2 kg	2 kg	2 kg
Essential oil (ml)	200 ml (10%)	400 ml (20%)	600 ml (30%)	800 ml (40%)
Dye Colour (ml)	100 ml (5%)	200 ml (10%)	300 ml (15%)	400 ml (20%)
Emission of candle soot	No emission	No emission	Low emission	High Emission
Burning time of candle	High	High	Medium	Low
Candle Smell	Low	Medium	Medium	High
Candle colour	Low	Medium	High	High

4.1.5 Flow of the Raw Material

Table 11 shows the data for flow rate. The flow rate of raw material have been test for 10 s. Table 11 show the result of flow rate from the test. From this test, the timer in the program can be determine for the actual ratio of the raw material need to be used. The flow rate of the pump 1 and pump 2 is different because of the viscosity of the raw material. The pump have been use is the same pump which the flow is 1.5-2 Litre per minutes. Essential oil have higher viscosity than dye colour that's make the flow rate of the essential oil slower than dye colour. The flow rate for the wax is 1000 g in every 10 s and 100 g per second. To determine the right ratio for the candle, timer of the program should be depending on the result of this flow rate.

Table 11. Flow rate

	Pump 1 (Essential Oil)	Pump 2 (Dye Colour)	Ball Valve (Wax)
Opening time (s)	10 s	10 s	10 s
Flow	250 ml	300 ml	1000 g
Flow rate (s)	25 ml	30 ml	100 g

4.1.6 Melting Time of the Wax

Table 12 shows the data melting time of the wax.

Table 12. Melting time of the wax.

Temperature (°C)	Melting time of the wax (minutes)
67	28
69	26
71	20
73	18
75	16
77	14
79	12
81	10
83	10
85	10

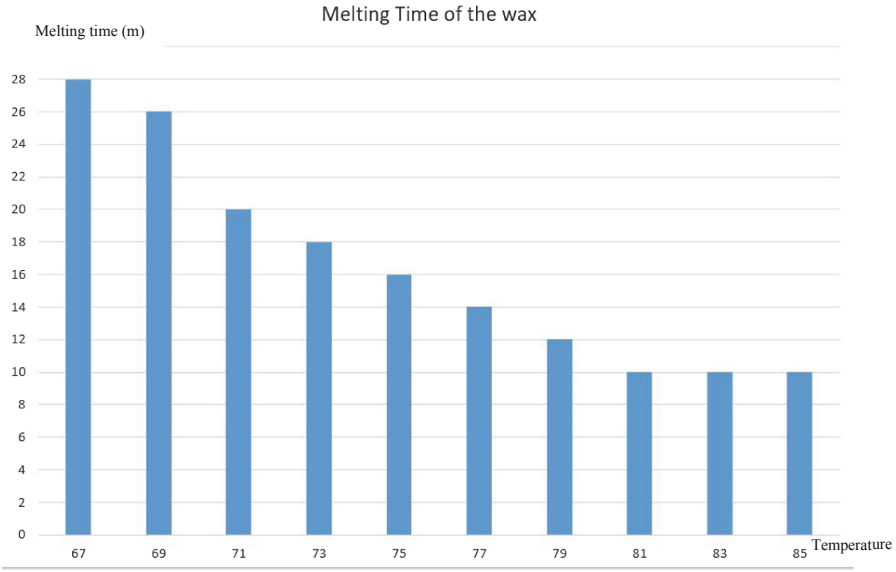


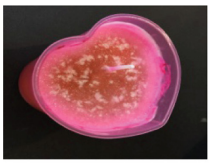
Fig. 15. Bar chart for melting time of the wax

Melting time taken per kilogram for the wax to be melt vs temperature. The temperature have been test from 67 °C because below than 67 °C the wax cannot be melt as shown in Fig. 15. The time for the wax to be melt is decreasing follow to increasing temperature of the heating. The graph show when the wax is melting over 81 °C the time taken for the wax to be melt is same as 10 min. From the study, the wax

cannot be melt over 80 °C because the wax can create more Volatile Organic Compound that not good for the user health.

4.2 End Product (Aromatherapy Candle)

Figure 16 show the result of end product that has been made by automated aromatherapy candle process plant. The end product has been test in and the candle successfully create the aromatherapy of the lavender. Based on this evidence, this automated process plant can be used to create the aromatherapy candle (Fig. 16).



Aromatherapy Candle (End Product)

Test the End Product

Fig. 16. End product of this study

5 Conclusion and Future Work

This section presents the conclusions and suggestion of future work of the study described in this article.

5.1 Conclusion

The work in this article has been successfully completed and the objectives of this article has been met. Automated aromatherapy candle process plant has been designed and implemented in this article. A reasonable finding with conclusion is reported by the design of experiment and prototype development result also has been explained. Through the successful development of work in this article, this study has found in generally that the temperature for making the candle can be control according to the set point by using external temperature controller. This result of investigation show that the temperature reading is overheat at first test but the temperature controller able to reach and maintain the set point after tuning the controller.

The mixing of the raw material completely can be done by automated process. The system also able to control overall process using. Program has been created and downloaded into PLC to automate the process for this plant to monitor the process. This plant also can make variety of aromatherapy and colour by using the right combination reaction. This process would have a great potential to be commercialized in line with the rapid growth of study in automated process industry.

5.2 Future Work

The complete final prototype and testing of this study have arisen some disadvantage of the system. Thus, a suggestion of future work for this study is listed as below:

i. Control and monitoring temperature using PLC by installing the temperature transmitter.
ii. Customize a bigger glass product tank
iii. Install motorized ball valve for easy collecting end product
iv. Install level sensor to get the accurate amount of raw material.

References

1. Alsayyad, S.: The danger of scented candles. In: Natural Sciences Poster Sessions, vol. 99 (2016)
2. Guzialowska-Tic, J.: Description of raw materials for manufacturing candles and grave candles and their influence on the environment. Chemik Science-TechniqueMarket **67**, 1007 (2013)
3. Cooke, B., Ernst, E.: Aromatherapy: a systematic review. Br. J. Gen. Pract.: J. Roy. Coll. Gen. Pract. **50**(10962794), 493–496 (2000). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1313734/
4. Li, B., SauvØ, G., Iovu, M.C., Jeries-EL, M., Zhang, R., Cooper, J., Santhanam, S., Schultz, L., Revelli, J.C., Kusne, A.G., Kowalewski, T., Snyder, J.L., Weiss, L.E., Fedder, G.K., McCullough, R.D., Lambeth, D.N.: Volatile organic compound detection using nanostructured copolymers. Nano Lett. **6**(8), 1598–1602 (2006). https://doi.org/10.1021/nl0604980
5. Matthai, M., Petereit, N.: The quality candle. Sofw. J. **130**, 69–82 (2004)
6. Ahn, J.H., Kim, K.H., Kim, Y.H., Kim, B.W.: Characterization of hazardous and odorous volatiles emitted from scented candles before lighting and when lit. J. Hazard. Mater. **286**, 242–251 (2015). https://doi.org/10.1016/j.jhazmat.2014.12.040. http://www.sciencedirect.com/science/article/pii/S0304389414010243
7. Barnett, J.E., Shale, A.J., Elkins, G., Fisher, W.: Aromatherapy. In: Complementary and Alternative Medicine for Psychologists: An Essential Resource, pp. 181–191. American Psychological Association, Washington, DC (2014). https://doi.org/10.1037/14435-013
8. Baldwin, J.: Aromatherapy as an Adjunctive Support for Trauma in Pastoral Care and Counseling. Sensing Sacred: Exploring the Human Senses in Practical Theology and Pastoral Care, p. 169 (2016)
9. Siledar, S.: Aromatherapy for anxiety: a guide for the average adult user to reduce symptoms of anxiety. Ph.D. thesis, Alliant International University (2018)
10. Koulivand, P.H., Khaleghi Ghadiri, M., Gorji, A.: Lavender and the nervous system. Evid.-Based Complement. Altern. Med.: eCAM **2013**(23573142), 681304–681304 (2013). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3612440/
11. Worwood, V.A.: The Complete Book of Essential Oils and Aromatherapy, Revised and Expanded: Over 800 Natural, Nontoxic, and Fragrant Recipes to Create Health, Beauty, and Safe Home and Work Environments. New World Library (2016)
12. Stiles, K.: The Essential Oils Complete Reference Guide: Over 250 Recipes for Natural Wholesome Aromatherapy. Page Street Publishing (2017)
13. Bacon, M.M., Romero-Zern, L.B., Chong, K.K.: Determining wax type: para n or naphthene? SPE J. **15**(04), 963–968 (2010). https://doi.org/10.2118/124799-PA

14. Menon, A., Waller, N., Hu, W., Hayhurst, A., Davidson, J., Scott, S.: The combustion of solid para n wax and of liquid glycerol in a uidised bed. Fuel **199**, 447–455 (2017)
15. Miller, A., Smith, R., Dufresne, B., Mahmoudkhani, A., et al.: Out with the old: developing a new test methodology for para n wax dispersion and inhibition testing. In: SPE International Conference on Oil eld Chemistry. Society of Petroleum Engineers (2019)
16. Hawcroft, M.: New light on candles on the seventeenth-century french stage. French Stud. **68**(2), 180–192 (2014). https://doi.org/10.1093/fs/knt301
17. Harriet, J., CampÆ, J.P., Grajales, M., LhØritier, C., Pajuelo, A.G., MendozaSpina, Y., Carrasco-Letelier, L.: Agricultural pesticides and veterinary substances in uruguayan beeswax. Chemosphere **177**, 77–83 (2017)
18. Perugini, M., Tulini, S.M., Zezza, D., Fenucci, S., Conte, A., Amorena, M.: Occurrence of agrochemical residues in beeswax samples collected in Italy during 2013–2015. Sci. Total Environ. **625**, 470–476 (2018)
19. Rezaei, K., Wang, T., Johnson, L.A.: Combustion characteristics of candles made from hydrogenated soybean oil. J. Am. Oil Chem. Soc. **79**(8), 803–808 (2002). https://doi.org/10.1007/s11746-002-0562-y
20. López, V., Nielsen, B., Solas, M., Ram rez, M.J., Jäger, A.K.: Exploring pharmacological mechanisms of lavender (lavandula angustifolia) essential oil on central nervous system targets. Front. Pharmacol. **8**, 280 (2017)
21. Tisserand, R., Young, R.: Essential Oil Safety: A Guide for Health Care Professionals, 2nd edn. Elsevier Health Sciences (2013)
22. Karaman, T., Karaman, S., Dogru, S., Tapar, H., Sahin, A., Suren, M., Arici, S., Kaya, Z.: Evaluating the efficiency of lavender aromatherapy on peripheral venous cannulation pain and anxiety: a prospective, randomized study. Complement. Ther. Clin. Pract. **23**, 64–68 (2016)
23. Liu, T., Liu, Q., Li, Z., Huo, L., Chan, M., Li, X., Zhou, Z., Chan, C.K.: Emission of volatile organic compounds and production of secondary organic aerosol from stir-frying spices. Sci. Total Environ. **599**, 1614–1621 (2017)
24. Lucattini, L., Poma, G., Covaci, A., de Boer, J., Lamoree, M.H., Leonards, P.E.: A review of semi-volatile organic compounds (SVOCS) in the indoor environment: occurrence in consumer products, indoor air and dust. Chemosphere **201**, 466–482 (2018)
25. Graham, C.A., Janssen, E., Sanders, S.A.: Effects of fragrance on female sexual arousal and mood across the menstrual cycle. Psychophysiology **37**(1), 76–84 (2000)
26. Hambali, N., Saat, S., Ahmad, M.A., Ramli, M.S., Ishak, M.A.: Computer-based system for calibration of temperature transmitter using RTD. In: 2010 3rd International Conference on Information Management, Innovation Management and Industrial Engineering, vol. 3, pp. 332–336 (2010). https://doi.org/10.1109/iciii.2010.400
27. Knospe, C.: PID control. IEEE Control Syst. Mag. **26**(1), 30–31 (2006). https://doi.org/10.1109/mcs.2006.1580151
28. Astrom, K., Hagglund, T.: The future of PID control. Control Eng. Pract. **9**(11), 1163–1175 (2001). https://doi.org/10.1016/S0967-0661(01)00062-4. http://www.sciencedirect.com/science/article/pii/S0967066101000624. PID Control
29. Larsson, S., Fantazzini, D., Davidsson, S., Kullander, S., Höök, M.: Reviewing electricity production cost assessments. Renew. Sustain. Energy Rev. **30**, 170–183 (2014). https://doi.org/10.1016/j.rser.2013.09.028. http://www.sciencedirect.com/science/article/pii/S1364032113006990
30. Wu, H., Su, W., Liu, Z.: PID controllers: design and tuning methods. In: 2014 9th IEEE Conference on Industrial Electronics and Applications, pp. 808–813 (2014). https://doi.org/10.1109/iciea.2014.6931273
31. Lula, R.A.: Stainless steel (1985)

32. Crenganis, M., Breaz, R.E., Racz, G., Bologa, O.: Zigler-nicols PID tuning method for position control of a mobile robot. In: Recent Tendency in Aerospace, Robotics, Manufacturing Systems, Energy and Mechanical Engineering, Applied Mechanics and Materials, vol. 841, pp. 221–226. Trans Tech Publications Ltd (2016). https://doi.org/10.4028/www.scientic.net/AMM.841.221
33. Saleh, A., Sakaka, A., Arabia, S., Mosa, M.: Analysis of control strategies and simulation of heating systems using Simulink/Matlab potential. J. Therm. Eng. 2(5), 921–927 (2016)
34. Ho, W., Hong, Y., Hansson, A., Hjalmarsson, H., Deng, J.: Relay auto-tuning of PID controllers using iterative feedback tuning. Automatica **39**(1), 149–157 (2003). https://doi.org/10.1016/S0005-1098(02)00201-7. http://wwwsciencedirect.com/science/article/pii/S0005109802002017
35. Vega, C., Sanz, E., Abascal, J.L.F.: The melting temperature of the most common models of water. J. Chem. Phys. **122**(11), 114507 (2005). https://doi.org/10.1063/1.1862245

Implementation of Automated Retractable Roof for Home Line-Dry Suspension Area Using IoT and WSN

Siti Nor Zawani Ahmmad[1], Muhammad Abdul Ghaffar Eswendy[1], Farkhana Muchtar[2(✉)], and Pradeep Kumar Singh[3]

[1] Instrumental and Control Engineering, Universiti Kuala Lumpur, MITEC, Persiaran Sinaran Ilmu, Bandar Seri Alam, 81750 Masai, Malaysia
sitinorzawani@unikl.edu.my, mabdghaffareswendy@gmail.com

[2] School of Computing, Faculty Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia
farkhana@gmail.com

[3] Department of CSE & IT, Jaypee University of IT, Waknaghat, Solan 17334, Himachal Pradesh, India
pradeep_84cs@yahoo.com

Abstract. Weather in Malaysia are hot and humid throughout the year thus having a sudden rain can disrupt the drying of laundries and make them wet. In this study, an automated retractable roof system was developed to overcome this problem. The development and implementation of this study enables user to monitor the parameters at the laundry suspension area by using their smartphone and prevent the laundries getting wet from rain. This study uses humidity sensors, Ultraviolet (UV) sensor, rain sensor, and temperature sensor to detect parameter such as humidity, UV intensity, presence of water and temperature respectively. Data from the sensors were collected and analysed to determine the values of parameters when rains occurred. These parameters were indicated as part of weather prediction study. From experiment, the retractable roof will open and close depended on condition met by the system. In addition, the system can communicate with the user's phone through using Internet connection. The Blynk application in the smartphone allows the user to monitor and control the system through internet connection between the application and microcontroller. This study will be helpful for non-commercial use and can be expanded to commercial use as with further improvement.

Keywords: Internet of Things · Wireless Sensor Network · Retractable roof

1 Introduction

Malaysia is a country located near equator being hot and humid throughout a year. Thus, Malaysia have occasional rainfall and more during the monsoon seasons. During May to September, Malaysia faced Southwest monsoon while Northeast Monsoon from October and March [1, 2]. The formation of rain occurred when water from water body such as

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 546–565, 2020.
https://doi.org/10.1007/978-3-030-40305-8_26

lakes, streams, or ocean evaporates into the air when it is heated up by the sunlight. When the water vapor rises up in the air, it condenses, and condenses into clouds. A clouds is made up of small drops of water or ice crystals which depends on the height and how cold is the surrounding air. The water will start to fall back if the particles is having too much water condenses around it, or if there is drops in the temperature. The liquid particles that fall in which is called rain, if fall while frozen it is called as snow. The water will ow into rivers and lakes when the rainfall either seeps into the ground or become runoff once it falls on the land. Then the water from rivers flows into the ocean. Then, the cycle of evaporating of water from water body to rain fall continues. This is the common cycles of rain, which become the basis of the formation of rain [3–5].

As Malaysia weather is uniform throughout the year, peoples in Malaysia do their laundries and leave it to dry at the suspension area, which usually open and expose to sunlight. This method of drying laundries called as line dry which clothes are left on a line suspension made of wires or ropes. This is common method used in countries located in equator such as Philippines, Thailand, Singapore, Indonesia, etc. Line-drying are prefer even it is ineffective as such it depends on sunlight (UV) intensity, temperature, and wind speed. However, it also are cheaper than doing laundries and using cloth dryer to dry the clothes as it consume a lot of electricity and the machine itself are expensive. Thus, having sudden rain while leaving the laundries to dry at the suspension area can become a problem especially when away from home [6–8].

The other method in which to dry laundries, which is common in the West, is by using the clothes dryer. Most of the western household have a clothes dryer instead of line-dry which is common in the East. In comparison, by using clothes dryer, it is faster compare to line-dry. This is because line-dry method need sunlight and drying by evaporation took a lot of times. Another differences of culture for drying laundries is that in the west, it is considered unsightly to hang laundries and its more space e Efficient, as there is no need to use a space to hang the clothes if using the clothes dryer. However, the power consumption for the dryer is higher while line-dry use natural energy, which is sunlight [6–8].

In this study, apart from developing the automated retractable roofing system, the possible parameters, which can predict the rainy weather, were identified. Thus, a few sensor has been integrated such as humidity sensor, temperature sensor, and UV sensor. Data obtained in real-time were sent to the microcontroller and the data were transmitted through wireless network to the user's smartphone. The smartphone application shows the parameters from the sensor and some calculation were made to decide whether the weather is going to be rainy or clear. Additionally, instead of using the computers to monitor and actuate the system, smartphone was used as alternative monitoring devices for users. With smartphone application the system can be monitored anywhere and instructions can be send wirelessly to the system at home immediately [9–11].

2 Literature Review

In this study, apart from developing the automated retractable roofing system, the possible parameters which can predict the rainy weather were identified. Thus, related work to this study will look at three branches, namely (i) the development of retractable roof system, (ii) weather forecasting parameter, and (iii) rain sensor.

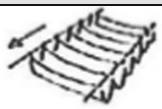
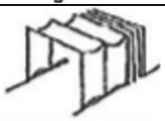
2.1 Existing Literature of Retractable Roof System

Retractable roofing systems have been used throughout the world since the 1930, in form of one or another. That is only until recent decades that the roofing systems have been applied or installed by large structures especially stadia. Despite that, retractable roofing systems also have been used for medium structures such as houses and restaurants in the recent years. At the early of millennium, there were approximately 25 large-span retractable roofs used for stadia in the world, and approximately half of the total were located in Japan, according to Ishii [12], Zablocki [13] and Liu et al. [14].

Though the number is increasing in the past years with the major sports events that leads to construction and remodeling of stadia. In 1961, Pittsburgh Civic Arena was the first large retractable roof built for a sporting venue. The name was later changed to the Mellon Arena, USA [15]. For a large retractable roof, there are multiple methods for opening and closing. These methods can be brie y explained by classifying their movement as: parallel, circular, vertical and their method of stowing the retracted roof as: overlapping, non-overlapping, or folding. In addition to the existing method, there are also the utilization of combination if any of these methods as described by Kassabian et al. [16], Jensen [17], Korkmaz [18] and Fenci and Currie [19].

For the objective of this work, the method that is preferred is the folding systems. A research has been executed to use the folding membranes as retractable roofs. Montreal Olympic Stadium was the first stadium that applied a folding membrane roof in 1976. However, the folding roof itself was not finished until the mid-eighties and were put back due to wind-induced failures of the structural membrane. The following were the method of opening and closing of membrane structures in accordance to the Institute for Light Weight Structure (1972) [20] (Table 1).

Table 1. Type of movement of opening and closing of retractable roofing.

Type of Movement	Parallel	Central	Circular
Membrane (Stationary supporting structure)	 Bunching	 Bunching	 Bunching
	 Sliding		
Supporting Membrane (moveable supporting structures)	 Rolling	 Folding	 Folding
	 Folding		

(*continued*)

Table 1. (*continued*)

	Most of the large retractable roofs are based on parallel movement due to its direct motion and ease of repair. The membrane or the support structure move horizontally at the same time until reach at one end of the structure.	This type of method of opening and closing involved usually involve d in vertical movement in which the membranes or panels move vertically at same time while expanding the folded or overlapped membranes.	This method of opening and closing of the roof by pivoting a fixed point allowing them to be stowed in overlapping or folding of the panels or membranes.

2.2 Weather Forecasting Parameters

For many centuries that weather conditions and change of climate has been observed and researched throughout the globe. In order to determine the environmental changes that happened, various parameters have been observed. As climate played a huge important role in human life, scientist are motivated to develop more ways to observe and do research to observe the subject of climate and weather. Nowadays, there are many automated observatories and weather forecasting system has been developed all around the world collecting the environmental parameters continuously for some other applications. With weather forecasting, data can be used for other field such as agricultures, transportation, construction etc.

According to VivekBabu et al. [21], the study said that weather forecasting has to be reliable and accurate regardless of its application. Thus, in their study, they developed a prototype system that employs Embedded System using Raspberry Pi for observing the weather changes. The systems monitored various parameters related to weather conditions which are humidity, temperature, soil moisture, rainfall and light intensity. The data collected from the system can be applied to agricultural. The prototype system was develop using open source hardware Raspberry Pi and Wi-Fi. The sensors gather the data of various environmental parameters then provide it to Raspberry Pi that act as base station. The Raspberry Pi transmits the data using Wi-Fi and the processed data will be displayed on laptop.

In this study, ESP32 and ESP8266 was used as base station and microcontroller. ESP8266 collects the data from sensors and ESP-Mesh connection which connected to ESP32, then data were transmitted to the user's smartphone using bluetooth. In addition, the objectives of the study are to develop automated roof system that can be control and monitored by the user instead of monitoring and data collection.

2.3 Rain Sensor

Rain sensor is part of the important components in this work. By measuring conductivity, it may detect whether the component is wet or dry in water. The resistor will raise the sensor trace value high until a drop of water shorts the sensor trace to the grounded trace. This pulse width information is read into a software counter in the microprocessor to determine the degree of rainfall [22–24]. The circuit works with the digital I/O pins of ESP8266 or the analog pins detect the amount of water-tempted contact between the grounded and sensor traces. The improvement of makes some work and innovation more safety and customers need requirement. For example, rain sensor as a part of innovative product to improve some common product in the market. The expanding disk rain sensor is the most commonly used in the market. The rain sensor used when a raindrop falls through the running board [25, 26]. During period of significant rainfall, an electromechanical actuating device designed employs the rain sensor to cause a circuit interrupt temporarily disable the irrigation controller. After a period of time subsequent to the rainfall, the device automatically restored the controller to a normal operating condition. The rain sensor has several features and benefits are automatic rain shutoff prevents the overwatering due to natural precipitation. Besides that, the moisture sensing disks works in a variety of climates.

2.4 IoT

The Internet of Things (IoT) is a system of interrelated computing with either anything as mechanical and digital machines, object, animals, human that provided with unique identifiers and ability to transfer data over a network independently without the involvement of human-to-human or human to-computer interaction. In other word, any devices connected to the Internet that has switches are to be considered as Internet of Things. This includes almost anything a person can think of, ranging from cellular phones to the jet engine of an airplane, to a building maintenance.

In this work, the retractable roofing system is connected to an ESP32 microcontroller that embedded with Wi-Fi and Bluetooth functions. Bluetooth is required to communicate with user's smartphone. For a sensor node, we are using ESP8266 microcontroller that only embedded with Wi-Fi function, enough for Wi-Fi mesh communication using ESP-Mesh library. We will discuss about ESP-Mesh in the next subsection.

The creation of Internet of Things which influenced by the rapid increase of these in a communicating-actuating networks. We can see that around our environment, sensors and actuators blend in seamlessly in the recent time. With information is shared across the platform in order to establish a common operating picture (COP). With the advancement of wireless technologies such as RFID tags, embedded sensors and actuators node in the recent years, the Internet of Things has stepped out of its infancy and is becoming the next revolutionary technology in altering the Internet into a fully integrated Future Internet [28–31].

2.5 Wireless Sensor Networking (WSN) Using ESP-Mesh

To facilitate the setup process and integration process between sensor nodes and retractable roof, ESP32 NodeMCU unit and ESP8266 NodeMCU units are linked to each other by ad-hoc as a mesh network group using ESP-Mesh.

The purpose is to enable automatic retractable roofs to be installed without the need to provide wireless network infrastructure before use. Instead, the retractable roof controller and wireless sensor nodes can be installed directly as each unit communicates wirelessly ad-hoc.

In addition, the use of ESP-Mesh also allows the node sensor to be installed modularly which can be installed at the desire (Table 2).

Table 2. Summary of related work

Authors	Title	Method	Proposed method
Ishii (2000) [12]	Retractable Roof Structures	Various type of opening and closing movement of retractable roof	Sliding method is used as a movement of opening and closing of retractable roof
VivekBabu et al. (2017) [21]	Weather Forecasting Using Raspberry Pi with Internet of Things	Using Raspberry pi for weather forecasting and monitoring the parameters only. The hardware is Raspberry pi 2 board	Arduino is used as microcontroller while Blynk application for monitoring and control the roof system
Jadhav et al. (2016) [27]	Environment Monitoring System using Raspberry-Pi	Using Raspberry-Pi for weather monitoring the environment with parameters such as humidity, temperature, vibration, and gas changes	The parameters used for monitoring and control purposes. The parameters used for this study were humidity, temperature and UV intensity
Madankar (2011) [22]	Intelligent Rain Sensing using Automatic Wiper System	Developing an Automatic Wiper System by using the Rain Sensor application	The retractable roof was the structure that was actuated. The rain sensor was used as a switch in the system

3 Development of Our Work in This Study

3.1 Process Flow

The process flow of this work starts when the user switches on the system. The sensors of the system will start to collect data of parameters and sends the signal to the user in real time. Hence, the sensors will transmit the signal to the Arduino microcontroller and it will do the conditions set when it receives the signal from the sensors based on the programming language download to the device. Next, it will transmit the signals to the Android application via internet connections (Figs. 1 and 2).

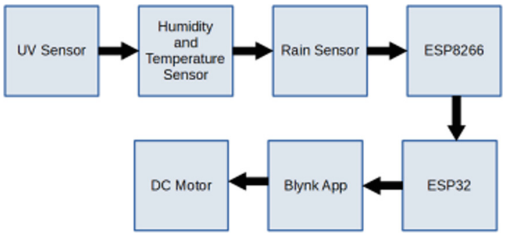


Fig. 1. Process flow

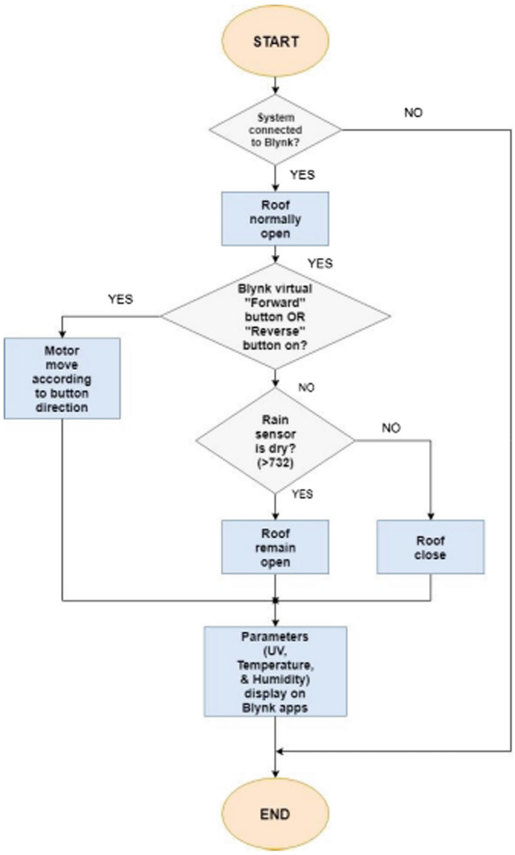


Fig. 2. Flowchart of retractable roof operation

3.2 Research Tool

The research tool applied in this study can be divided by two categories. The major part is the hardware and the second part is the programming software development.

3.2.1 Hardware Development

ESP32 NodeMCU
ESP32 is a series of low-cost, low-power system on a chip (SoC) microcontrollers with integrated Wi-Fi and dual-mode Bluetooth. ESP32 packaging can be obtained in various forms primarily for prototype and development purposes. The ESP32 NodeMCU board is selected for use in this work as it is among the most popular ESP32 development board used and has a smaller size than any other ESP32 development board. ESP32 is used as a main controller for the retractable roof and allows remote control over the smartphone using Bluetooth. ESP32 receives data sensors from ESP8266 inside the mesh network.

ESP8266 NodeMCU
The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability produced by manufacturer Espressif Systems in Shanghai, China. ESP8266 is used as a controller module for node sensors and at the same time transmits data sensors from sensors to ESP32 microcontroller inside the mesh network.

Humidity Sensor
In this study, humidity sensor is used to measure the moisture and the air temperature. The sensor detect the relative humidity of the immediate environment in which they are placed.

Ultra Violet Sensor
UVM-30A is an Ultraviolet (UV) sensor which can acquire the UV intensity indoors or outdoors. It converts photo-current or voltage depends on the UV intensity by internal amplifier equipped in it.

ESP32 Devkit Motor Shields
ESP32 Devkit Motor Shields contains one 74HC595 shift registers and two of L293D motor drivers and. Direction of the motor drivers can be control by using the 8 pins of the shift registers. PWM outputs of the ESP32 is connected directly to the output enable of the L293D. The Motor shield is able to drive 4 full H-bridge motor outputs or drive 2 servo motors or a combination.

Table 3 provides readers with a quick glimpse on the types of hardware component that is used in this study.

Table 3. Summary of hardware component used in this study

Component name	Function
ESP32 NodeMCU Microcontroller	Main controller of retractable roof
ESP32 NodeMCU Motor Shield	Motor driver to control DC motor for retraction mechanism of the roof
ESP8266 NodeMCU Microcontroller	As serial over Wi-Fi bridge between sensors and main controller in mesh network
Humidity Sensor	Humidity measurement input
UVM-30A Ultraviolet sensor	Ultraviolet radiation measurement input
Rain Sensor	Rain detector

3.2.2 Software Development

There are three software that have been used in this study; Arduino IDE 1.8.2, Blynk Application, and Fritzing.

Arduino IDE 1.8.2

The Arduino Integrated Development Environment or Arduino Software (IDE) contains a text editor too for composing code, a message zone, a content area, a toolbar with catches for basic capacities and progression of menus. It associates with the Arduino and Genuino equipment to transfer programing codes for the microcontroller to work. The code created must aligned with the system for this study. Arduino IDE also can be use to program ESP32 and ESP8266 microcontrollers.

Blynk Application

Blynk is a smartphone application that can be used to design an application for the Internet of Things. It can remotely control hardware, it also can display and store the sensor data. Blynk application for smartphone has three major components in the platform. It allows user to create interfaces for works using the various widget provided. Secondly, Blynk server where it liable for all the communication between the hardware and smartphone. There is also Blynk Cloud or run user's own public Blynk server locally. Lastly, the Blynk Libraries, where all the popular and commonly used hardware platforms that enable the communication with the server and process all the incoming and out coming commands from all various controller.

Fritzing

Fritzing is an open source software for the design of electronics hardware, to support creators to move from experimenting with a prototype to building a more permanent circuit. The software was created to document the user's Arduino-based prototype and create a PCB layout for manufacturing. Furthermore, this software can develop a prototype electronic circuit before applying to actual work. The circuit design for this study is as shown in Fig. 3.

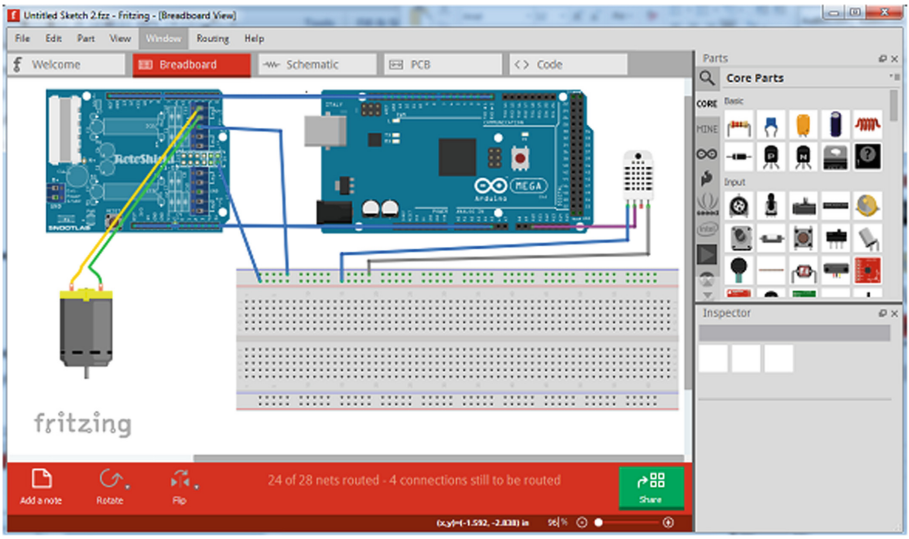


Fig. 3. Circuit design in fritzing for this study

3.3 Project Illustration

The draft idea for this work was roughly designed. It was separated by two parts which were design of the wiring and design of hardware.

3.3.1 Design of Wiring Diagram

A proper design and wiring was needed so that the components such as sensors, actuators, and microcontrollers can work as intended. Figure 4 shows the wiring diagram of our work in this study made by using Fritzing software.

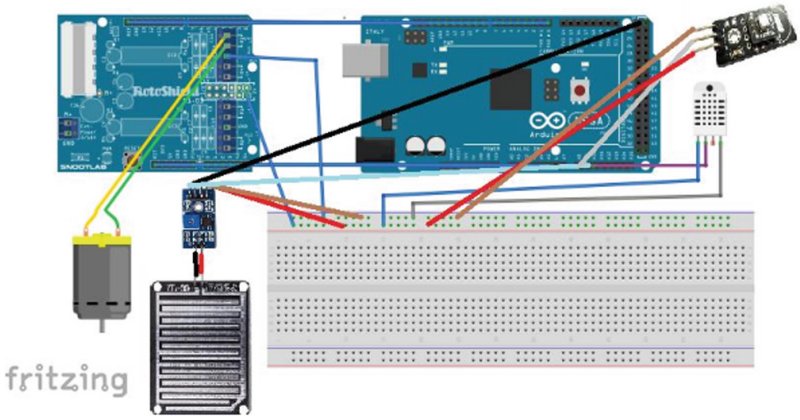


Fig. 4. Design of wiring diagram

3.3.2 Design of Hardware

The idea of this work is to attach all the sensors and the actuator, DC motor to the microcontroller and it shield. The sensors detect the parameters such as relative humidity, temperature, presence of water and UV intensity of the surrounding. Figure 5 shows the illustration of the hardware.

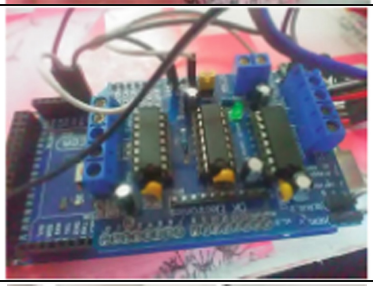
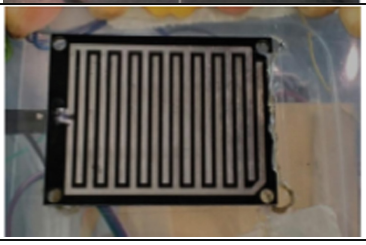
Table 4 briefly explains the functions of each component that involves in actuating the system to opening or closing the retractable roof.

Table 4. Device interface in the automated retractable roof system.

No.	Device/interface	Condition
1		Asus Zenfone Go is the smartphone that has been used in this work. The Android operating system in this device is used to create the system interface to control the automated retractable roof system.
2	 	Blynk is the application that has been used in the smartphone. This application need to identify the microcontroller, type of connection, and authentication code to use the automated retractable roof system.

(*continued*)

Table 4. (*continued*)

3		The microcontroller that had been use for this work is Arduino MEGA. The microcontrollers are used to get the information from the sensors and give instruction to the output.
4		The L293D Motor shield has been used in this work to control the movement of motor to open and close the automated roof system.
5		The output in this work is DC motor. It pulls or releases string that tied to the motor roller between the retractable roof. It close the roof by pulling the retractable roof and open the roof by releasing the retractable roof.
6		The retractable roof had been used to cover the laundry suspension area.
7		This is the rain sensor. It has been put on top of the cases to expose it to rain and water. When water detected on the rain sensor it will send signal to microcontroller to close the roof. Basically, the rain sensor acts as the switch to open and close the roof automatically.

3.3.3 Hardware Setup

The hardware was setup based on laundry suspension area in a moderate size and design. The main function of the design was to represent the roof in the suspension area it can be control either automatically by the system itself or instructions from the user from the smartphone application, Blynk. The system will run a conditional case in which the operation of motor to open and close the roof based on the sensors reading. Figure 5 shows the hardware setup of the prototype.

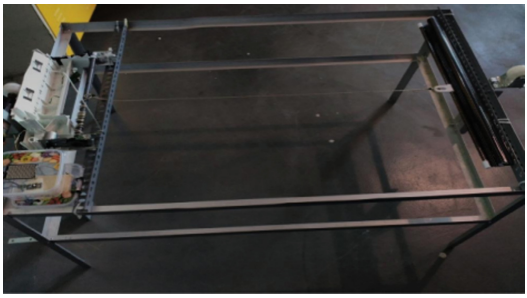


Fig. 5. The prototype design

3.4 Device Output Interface

Device Output Interface Fig. 6 illustrate the coding of ESP32 NodeMCU that have been created by IDE software with Blynk and sensors libraries. The coding is used to read sensors data, actuates the motor, and connects to the smartphone.

Fig. 6 arduino mega 2560 coding design

The program of blynk-ser.bat need to run in the PC to progress the coding and being connected to smartphone IP address. First of all, the program started the Blynk server connection to send and retrieve the data from the hardware. If the Blynk ser.bat is not running or connected to Blynk server, the system will not run. Figure 7 shows the program blynk-ser.dat connection status while running our project.

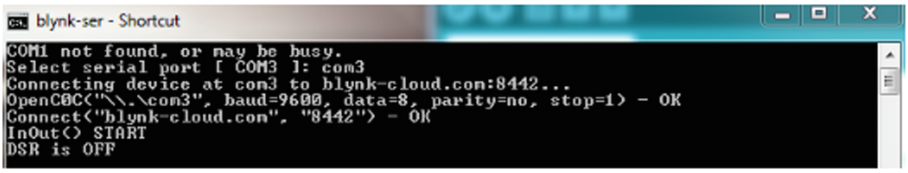


Fig. 7. Connection status to blynk server

The design for this work is completed after user turn on Blynk application in smartphone to monitor the parameters and control the actuator. Figure 8 shows the design of the work in this study when the roof is open and Fig. 9 shows the result when the roof was closed.

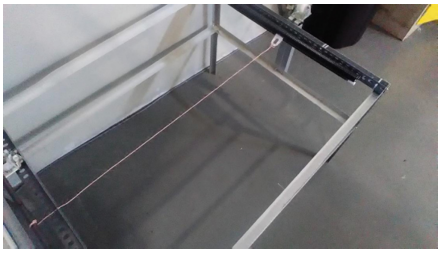


Fig. 8. Roof in open state

Fig. 9. Roof in close state

4 Result Analysis

The result shows the device and interface for the automated roof system.

4.1 System Testing

Figure 10 illustrates the first setup for the Blynk application in the smartphone by choosing the microcontroller and its connection and to log into the system using the author token address. In the hardware model option, user can choose many option of microcontroller such as Arduino models, Raspberry Pi models, RedBearLab models, Samsung models. Once the hardware setup has been set, user has to choose the connection type of microcontroller so it can communicate with smartphone. Connection type in the option consists of Ethernet, Wi-Fi, USB, GSM, Bluetooth, and BLE connection. Once, the two option have been selected, Blynk application issued an Auth token which used to connect the system to the user's project interface. In this project, the microcontroller was ESP32 NodeMCU and the connection type was Bluetooth wireless connection.

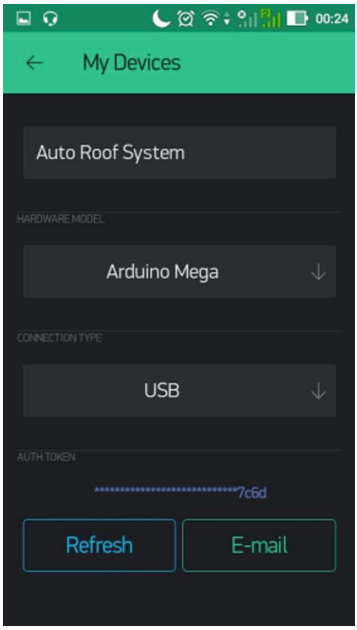


Fig. 10. Setup option of hardware model and connection type

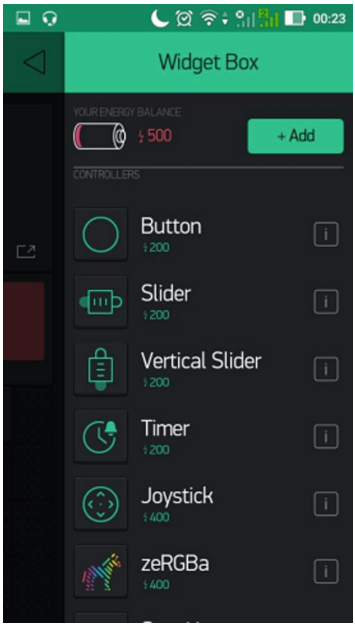


Fig. 11. List of widget in Blynk application

Fig. 12. User interface of the our work in this study

The configuration setup for the Blynk application in the smartphone using the proper widgets to the system was shown in Fig. 11. User can choose many option of widget such as button, slider, chart, joystick, and notification widget to name a few.

Figure 12 illustrate the user interface will be displayed in the Blynk application. It shows after the setup with the widgets when two output to be control, one lcd display widget, four value display to monitor the parameters and one graph plotter to show the parameters in graphs against time.

When the setup on the application completed, the Arduino IDE coding was designed based on the function related to application monitor and control interfaces and function of actuator. The coding then uploaded to microcontroller and connection to the Blynk server was established. Figure 13 shows that the coding of Arduino IDE assigned the virtual pins in the Blynk application to the sensor used.

The coding was then uploaded into microcontroller and connects to the smartphone. After running the system calibration, the output can be controlled and monitored by the application in the smartphone.

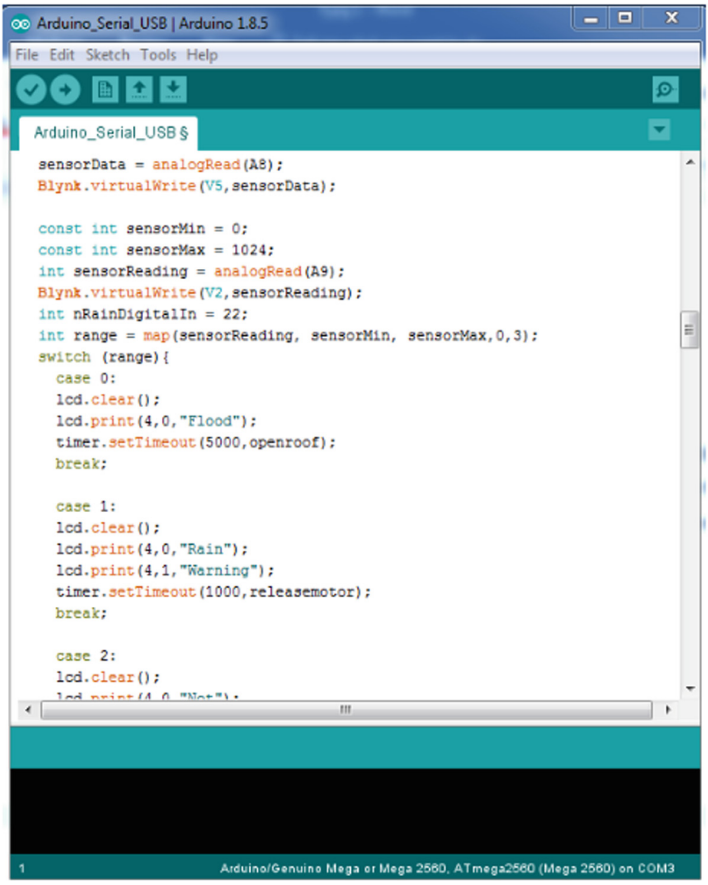


Fig. 13. Virtual pins assigned in the Arduino IDE coding

The coding was then uploaded into microcontroller and connects to the smartphone. After running the system calibration, the output can be controlled and monitored by the application in the smartphone.

4.2 Analysis of Results

The Table 5 shows the collected data from the sensors to determine value of parameters which will indicates rain weather for the weather prediction. The data collected is categorized into 2 table which is Table 5 which consists of data in which rainy weather occur while Table 6 consists of data in which clear weather.

Table 5. Rain weather data

Time	UV index	Average temperature	Humidity	Rain sensor	Status
Day 1 (1200–1359)	5	30.67	70	335	Flood
Day 1 (1400–1559)	3	31.53	76.67	321.04	Flood
Day 1 (1600–1759)	1	31.27	70.68	614.4	Rain warning
Day 2 (1200–1359)	0	31.33	67.33	593.92	Rain Warning
Day 2 (1400–1559)	5	31.45	70.67	111.24	Flood
Day 2 (1600–1759)		29.75	79.54	317.44	Flood
Day 3 (1200–1359)	4	31.88	61.32	931.4	Not raining
Day 3 (1400–1559)	1	32.79	59.67	741.33	Not raining
Day 3 (1600–1759)	9	30.13	71.67	303.6	Flood

The data in the Table 5 is collected during 3 days of when the weather is raining in a period of 3 h which is from 12 a.m. until 6 p.m. During rains, the UV index and surrounding temperature drops as the cloud cover the sun and rains cools the surrounding area meanwhile the humidity increased during rains. The value of the rain sensor drops when the raindrops detected on the rain sensor.

Table 6. Clear weather data

Time	UV Index	Average TEMPRATURE	Humidity	Rain sensor	Status
Day 1 (1200–1359)	7	31.95	58.33	1024	Not raining
Day 1 (1400–1559)	6	33.65	52.47	1024	Not raining
Day 1 (1600–1759)	3	30.56	60.98	1023	Not raining
Day 2 (1200–1359)	5	31.64	59	1024	Not raining
Day 2 (1400–1559)	5	30.13	53	1024	Not raining
Day 2 (1600–1759)	3	29.75	63	1021	Not raining
Day 3 (1200–1359)	9	31.68	61.35	1022	Not raining
Day 3 (1400–1559)	9	32.77	56.78	1023	Not raining
Day 3 (1600-1759)	9	29.54	66.23	1023	Not Raining

The data in the Table 6 is collected during 3 days of when the weather is clear in a period of 3 h which is from 12 a.m. until 6 p.m. During clear, the UV index is usually more than 5 showing and only drops when the weather is moody. The surrounding temperature are slightly above the room temperature and in range of 29 to 30 C. Meanwhile, the humidity recorded are in range of 50% to 60%. The humidity decreases in sunnier weather. The readings of rain sensor are constant at 1023 and 1024 since there is no raindrops or water detected on the rain sensor.

From the data analysis, parameters that can be assumed for rain weather prediction are when the UV index is below 3 meanwhile for temperature is that below 29.0 C. For humidity, the value is above 60%. In this work, rain sensor act as switch, however parameters for its cases already set such as for Flood, the value is below 341 while for Rain warning is at 732 and Not raining is above 732 value.

5 Conclusion

The work in this article has been successfully completed and the objectives of this article has been met. The work has two conditions and it can be considered a success in implementing each part and combining them together to make one working system. The prototype of automated retractable roof for home line-dry suspension area was successfully developed. After a few experiment, data collection and data analysis were done, the system of the automated retractable roof had accomplished the steps and conditions in the flow chart process.

This article is important because it is based on observation to improve and upgrade the system to be much better in future. The automated retractable roof for home line-dry suspension area was successfully developed, but there are a few limitations in application hardware and software. This recommendation can be used for references for future work or innovation such as:

i. Give user more options when taking action through the process.
ii. The connection in this work is bluetooth which are limited to bluetooth signal range (50–100 m). Thus, connection based on Wi-Fi are preferable so that the microcontroller can connect to the Internet without connecting it with bluetooth.
iii. Replace all the power supply with solar panel which can save the energy.
iv. Add retractable automation that collects the laundry suspension line.
v. Add notification function in the user interface to notify the user for weather in the Blynk application.

References

1. Tangang, F.T., Liew, J., Salimun, E., KwanMeng, S., LohJui, L., Muhamad, H.: Climate change and variability over Malaysia: gaps in science and research information. Sains Malaysiana **41**(11), 1355–1366 (2012)

2. Mei, N.S., Wai, C.W., Ahamad, R.: Environmental awareness and behaviour index for Malaysia. Proc. – Soc. Behav. Sci. **222**, 668–675 (2016). https://doi.org/10.1016/j.sbspro.2016.05.223. http://www.sciencedirect.com/science/article/pii/S1877042816303019
3. Hamlin, M.: The significance of rainfall in the study of hydrological processes at basin scale. J. Hydrol. **65**(1), 73–94 (1983). https://doi.org/10.1016/0022-1694(83)90211-1. http://www.sciencedirect.com/science/article/pii/0022169483902111. Scale Problems in Hydrology
4. Hasan, M.A., Pradhanang, S.M.: Estimation of ow regime for a spatially varied Himalayan watershed using improved multi-site calibration of the soil and water assessment tool (swat) model. Environ. Earth Sci. **76**(23), 787 (2017)
5. Adams III, T.E.: The use of central tendency measures from an operational short lead-time hydrologic ensemble forecast system for real-time forecasts. Ph.D. thesis, Virginia Tech (2018)
6. Pink, S., Mackley, K.L., Moroşanu, R.: Hanging out at home: laundry as a thread and texture of everyday life. Int. J. Cult. Stud. **18**(2), 209–224 (2015)
7. Yates, L., Evans, D.: Dirtying linen: re-evaluating the sustainability of domestic laundry. Environ. Poli. Gov. **26**(2), 101–115 (2016)
8. Madgwick, D., Wood, H.: The problem of clothes drying in new homes in the UK. Struct. Surv. **34**(4/5), 320–330 (2016)
9. Chunjiang, Y.: Development of a smart home control system based on mobile internet technology. Int. J. Smart Home **10**(3), 293–300 (2016)
10. Stojkoska, B.L.R., Trivodaliev, K.V.: A review of internet of things for smart home: challenges and solutions. J. Clean. Prod. **140**, 1454–1464 (2017)
11. Mao, X., Li, K., Zhang, Z., Liang, J.: Design and implementation of a new smart home control system based on Internet of Things. In: 2017 International Smart Cities Conference (ISC2), pp. 1–5 (2017). https://doi.org/10.1109/isc2.2017.8090790
12. Ishii, K.: Structural design of retractable roof structures. Computational Mechanics (2000)
13. Zablocki, W.: Mobility in sport architecture. In: International Symposium on Lightweight Structures in Civil Engineering, pp. 99–106. Jan B Obrebski, Warsaw (2002)
14. Liu, M., Li, Q.S., Huang, S.H., Shi, F., Chen, F.: Evaluation of wind effects on a large span retractable roof stadium by wind tunnel experiment and numerical simulation. J. Wind Eng. Ind. Aerodyn. **179**, 39–57 (2018). https://doi.org/10.1016/j.jweia.2018.05.014. http://www.sciencedirect.com/science/article/pii/S0167610518300308
15. Mahovič, A.: Typology of retractable roof structures in stadiums and sports halls. IGRA USTVARJALNOSTI (IU)/CREATIVITY GAME (CG) Theor. Pract. Spat. Plann. **3**, 90–99 (2015)
16. Kassabian, P., You, Z., Pellegrino, S.: Retractable roof structures. Proc. Inst. Civil Eng.-Struct. Build. **134**(1), 45–56 (1999)
17. Jensen, F.V.: Concepts for retractable roof structures. Ph.D. thesis, University of Cambridge (2005)
18. Korkmaz, S.: A review of active structural control: challenges for engineering informatics. Comput. Struct. **89**(23), 2113–2132 (2011). https://doi.org/10.1016/j.compstruc.2011.07.010. http://www.sciencedirect.com/science/article/pii/S0045794911002070
19. Fenci, G.E., Currie, N.G.: Deployable structures classification: a review. Int. J. Space Struct. **32**(2), 112–130 (2017). https://doi.org/10.1177/0266351117711290
20. Otto, F., Burkhardt, B.: IL Five: Convertible Roofs. Information of the Institute for Lightweight Structures Series. George Wittenborn Incorporated (1972). https://books.google.com.my/books?id=wb3iAAAACAAJ
21. VivekBabu, K., Reddy, K.A., Vidhyapathi, C., Karthikeyan, B.: Weather forecasting using raspberry pi with internet of things (IoT). ARPN J. Eng. Appl. Sci. **12**, 5129–5134 (2017)

22. Madankar, S.B., Khanapurkar, D.M.M.: Intelligent rain sensing using automatic wiper system. In: 2nd National Conference on Information and Communication Technology (NCICT), pp. 27–29 (2011)
23. Lai, B., Deng, Z., Wang, X., Yan, J.: A kind of rainfall sensor design without mechanical structure. In: International Conference on Education, Management, Computer and Society. Atlantis Press (2016)
24. Chacon-Hurtado, J.C., Alfonso, L., Solomatine, D.P.: Rainfall and streamow sensor network design: a review of applications, classification, and a proposed framework. Hydrol. Earth Syst. Sci. **21**(6), 3071–3091 (2017)
25. Prabhakar Hegade, S.N., Alagundi, P., Kiran, M.: Automatic protection of clothes from rain. Int. J. Adv. Res. Comput. Commun. Eng. **5**(04), 363–366 (2016)
26. Oktawiani, P.I., Putra, I.K.G.D., Wibawa, K.S.: Sistem penjemur pakaian otomatis menggunakan raspberry pi berbasis android. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi), pp. 225–233 (2018)
27. Jadhav, G., Jadhav, K., Nadlamani, K.: Environment monitoring system using raspberry-pi. Int. Res. J. Eng. Technol. (IRJET) **3**(04), 1168–1172 (2016)
28. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gen. Comput. Syst. **29**(7), 1645–1660 (2013). https://doi.org/10.1016/j.future.2013.01.010. http://www.sciencedirect.com/science/article/pii/S0167739X13000241
29. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutorials **17**(4), 2347–2376 (2015). https://doi.org/10.1109/comst.2015.2444095
30. Vashi, S., Ram, J., Modi, J., Verma, S., Prakash, C.: Internet of Things (IoT): a vision, architectural elements, and security issues. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 492–496. IEEE (2017)
31. Lee, I., Lee, K.: The internet of Things (IoT): applications, investments, and challenges for enterprises. Bus. Horiz. **58**(4), 431–440 (2015)

Advancements on Wireless Sensor Networks

IoT Enabled Air Pollution Monitoring in Smart Cities

Vrinda Gupta(✉)

National Institute of Technology Kurukshetra,
Kurukshetra 136119, Haryana, India
vrindagl6@gmail.com

Abstract. Every country is working towards transforming their cities into smart cities. The cities are to be developed and sustainable solution to be provided more so as concern towards the issue of air pollution is ever increasing. The hazardous gases emitted from combustion of vehicles has been the major cause of it and it has led to increase in number of deaths year by year. For addressing this urban cities air pollution problem, an attempt has been made in the present chapter by building a low cost and real time monitoring system using Internet of Things technology. The system uses gas sensor to detect pollutants such as ammonia, carbon dioxide, aromatic compounds etc. and consequently transfer the sensed data to microcontroller. The data is then transmitted through Internet to server using Wi-Fi module. The air quality in the vicinity of sensor can thus be recorded and proper counteraction could then be taken in case of high level of pollution. By using Internet of Things and recording sensor data to a remote server, one can overcome the memory limitations and also collection of data manually from installed devices. Policy makers can use the live data via Internet of Things in implementing a smart city and thereby improve the quality of citizens lives.

Keywords: Smart cities · Internet of Things · Air pollution monitoring

1 Introduction

Due to industrialization and rapid population growth, need for a comfortable living in urban areas grew hastily, leading to the urbanization. In these urban cities, a number of systems and sub-systems are networked in such a way that one influences the other to a great extent. These systems e.g. food, water, housing, transport, health, education, governance, maintenance and law enforcement are interlinked and interdependent which impacts the human's life in one way or other. In a comprehensive view, the urban city needs sufficient supply of water, electricity, housing, good means of transport, and ultimately the sense of safety. The urbanization has impacted the environment of these cities, the climate and its natural resources. There is an urgent need of the hour for an urban city that has the capability to manage these interdependent systems in such a way to make it to smarter city and finally lead to a smarter life [1]. These smart cities need to fulfil the following amenities to be named as given below:

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 569–591, 2020.
https://doi.org/10.1007/978-3-030-40305-8_27

- Smart energy generation and maintenance (smart grid, smart lighting)
- Smart environment (water management, weather, smart waste)
- Smart transportation (traffic monitoring, smart parking)
- Smart buildings (office, residential buildings).

All the above things/processes are said to be smart if a very less or no human intervention is required or demanded besides producing accurate results. The objective of smart city development is to make it sustainable and ensure its citizens a high quality of life by providing a clean environment [2]. Central to the development of smart cities is a sensor as it collects vital data which in turn can ensure smooth functioning of a city. Sensors are of various types such as meteorological sensor, pollution sensor, smart building sensor, medical sensor, or human sensors. These sensors are required to be connected wirelessly through next generation technologies such as 5G which are emerging and are being developed quickly [3]. These sensors are integrated with real time monitoring systems and lead to reduction in carbon dioxide emissions. The sensor network technology has enabled the Internet of Things (IoT). The Internet of Things in recent days witnessed a wide range of application in different fields connecting 0.3 billion devices during 1990 and is expected to comprise a total of 1 trillion by the year 2025, as foreseen by Hewlett Packard. IoT makes the access and interaction with different types of devices which are connected to the Internet. The goal of IoT is to make sensors/devices (things) communicate with each other. Sensor devices sense the environment and communicate without applying human intervention and the data collected can be analyzed to make human life easier and comfortable. The term 'Internet of Things' was coined in 1999 by Ashton [4] to describe this vision of Internet connected things which is now a reality. This vision of IoT has made possible the next generation devices to be embedded with sensing and communicating capabilities. With the integrated sensors systems in smart cities, the authorities can easily monitor the environment and improve it by providing new services and sustainable solutions to its citizens. For instance, an urban IoT can make available the resources to monitor air quality in parks, or other public places. The sensed data about air quality and pollution levels can be made available to the city dwellers.

Now-a-days the health of mankind has been completely wedged by pollution. Pollution, in general, means introduction of contaminants into environment which in turn disturbs and harms the ecosystem. There are different types of pollution in environment, such as air pollution, water pollution, noise pollution etc. being faced by cities. According to Economic Survey of Delhi (2018–19), under the head environmental concerns, the main cause of environmental degradation in Delhi was found to be air pollution [5]. The causes of such outdoor air pollution are the emissions caused from automobile exhausts, biomass burning and use of fossil fuels. World Health Organization (WHO) has stated that about ninety percent of world's urban population is being affected by air pollution [5]. As per a survey by Lancet, in India 1.2 million deaths were due to air pollution in the year 2017 [6]. Even cities of US which is the most powerful nation is facing the issue of air pollution mainly caused due to contaminants like lead, ozone, particulate matter. Particulate matter (PM_{10}) comprises small particles that arise from traffic and combustion. $PM_{2.5}$ is of great concern as these small diameter particles affect our lungs, and even blood vessels. Occupational

exposure to respirable quartz dust causes silicosis and lung cancer. Air pollution is created due to different hazardous contaminants those are present in the air which are being generated from gas emissions of vehicles. Nitrogen oxide (NO_2) gas mainly arises from combustion which causes bronchitis, and asthma attacks. Ozone gas (O_3) formed by combination of various pollutants cause eyes irritation, respiratory and heart diseases. Thermal power generation is producing lot of CO_2, thereby causing global warming and leading to rise in temperature of 2–3 °C by the end of century. The rate of air pollution is increasing day by day due to increase of usage of vehicles and other changes taking place in the atmosphere. Besides it, air quality fluctuates more rapidly than the weather, during the course of the day, and therefore requires long term monitoring data and including real-time data [7].

The smart city is an application of IoT. Therefore, underlying technology used in building of smart cities is inherited from IoT. The smart city can be well thought-out as a 4-layer model, with infrastructure layer at the bottom comprising of devices, sensors, a second layer as a management layer for managing the complex infrastructure such as granting access to all available resources, then on its top comes the application layer that provides all smart cities applications, and final top is the stakeholder layer that includes all the entities for e.g. citizens, officers, vehicles etc. [8]. The four layer stack for smart city has been shown Fig. 1. In a smart city, variety of large number of sensors are deployed. Sensing equipment could be Zigbee, Bluetooth, RFID sensor, GPS terminals, etc. These sensors feed the big data city management systems. In a sustainable smart city, data management is central to all the services that smart city provides. The process of data management could be further categorized into data analysis, data fusion, data processing, data storage decision management. For performing data fusion, the authors have reported use of Kalman filtering technique at data management layer [9]. This in turn provides the real-time information to citizens about traffic flows, parking space availability, air quality, etc. This process of generation, processing, analysis, sharing and storing the big data requires protection and security during different steps [10, 11].

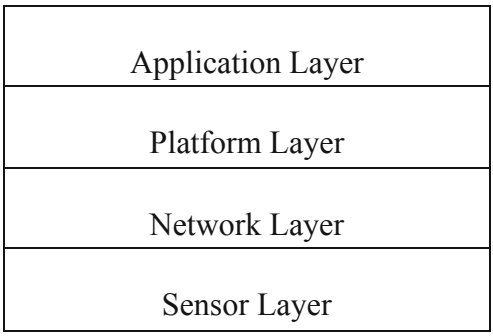


Fig. 1. Technology architecture for smart cities.

The smart cities are built up of few main attributes viz. sustainability, quality of life, urbanization etc. And under sustainability, comes the pollution issue [1, 12]. Our urban cities will be deteriorating if the pollution is not taken care of. This situation is because of the industrial developments, rise in vehicles and buildings because of the industrial developments, or rise in vehicles and buildings in urban cities. Governments of various nations have taken it up as a challenge. As the population is growing, it is becoming more difficult to achieve sustainable environment with smart solutions i.e. sustainable transport in cities, solid waste management, industrial emissions reduction and access to renewable energy etc. It can be best achievable with utilization of Internet of Things (IoT) [1]. IoT is being used in smart cities as it offers the information of the CO_2 levels and other data at the right time for decision making and thus assuring the life quality of their citizens. There is no doubt that IoT is playing a key role as a networking technology in sustainable development of smart cities. By sustainability issue, the meaning is that the city should be able to maintain balance of eco system while performing it's all operations. Significant literature on Internet of Things-enabled smart cities giving state of the art and future trends is presented [13, 14]. A practical implementation of an IoT realized smart city can be seen at an urban Padova in Italy which has developed a benzene (C_6H_6) sensor for monitoring air quality [15]. Another project known as Green IoT for development of smart city, has been established in Uppsala, Sweden [16]. The authors in [17] suggest an opportunistic approach using taxi cabs for data collection. Even though certain smart cities have developed and has increased the quality of life of its inhabitants, the challenge still lies with them i.e. concerning security and privacy issue. This issue has occurred because of the increase in interdependency, connectivity, and complexity and if not taken care of, may lead to bad and insecure implementation of smart city [18].

The vision of the smart city differs according to geographic location and its current infrastructure and technological deployments. For e.g., the goal of a city located in a developed country would be promoting efficiency of services, and creating sustainability, whereas the main goal of a city located in a developing country would be managing economic transitions in an urban environment [19, 20]. Many applications make collection of more data than that is essentially required. This information can be leaked to third parties, thus threatening the privacy of the user. Therefore, IoT based smart city also has the challenge called as data over-collection [21]. Another challenge lies in cloud based smart cities which integrated the IoT and cloud computing. In this, the data is managed by cloud service providers (CSPs). But this again, requires to check integrity of outsourced data [22]. Moreover, it is found that no two cities have the same characteristic features, viz. geography, demographical, social, cultural context. It requires involvement of different stakeholders in the development of smart city because of the diversity that exists. Therefore, better solution is to empower its citizens toward creation of sustainable cities [23]. It is found that monitoring of air pollution in urban areas and smart cities is very challenging, as there are large number of factors which affect air quality, such as urban structures, traffic volume, meteorology, land use [24].

1.1 Air Quality Monitoring Overview

Pure air consists of mixture of gases in fixed proportion, i.e. 78% nitrogen, 21% oxygen, and about 1% argon. If the composition alters, it is called air pollution which leads to hazardous effects on living creatures' health and environment. And it is evident from the data, that most of the urban areas are facing severe problem of air pollution, meaning that air quality is no longer pure, but is deteriorating and deviating from the standard. A number of contaminants are introduced into the air that is referred to as air pollution. These emissions have altered the chemical composition of the atmosphere. The concentration of greenhouse gases viz. carbon dioxide, methane, and nitrous oxide has increased which cause harm when in high concentrations. The main source for generating atmospheric pollutants is vehicles and industries [25]. It has also been determined that not only vehicular emissions, & industries emissions, but domestic pollution, garbage burning are also adding to the total pollution load. The data of environmental components in smart cities can be taken from various international and national/local agencies like, National Aeronautics and Space Agency (NASA), Central Pollution Control Board (CPCB), Meteorological Department, etc. Now, air quality is being specified by using a color coded tool called Air Quality Index (AQI). It is indicated by a number which lies in the range 0–500. Larger value of AQI shows that air is of poorer quality. Moreover, there are areas and hours during the day, where air quality fluctuates and changes dramatically. The indicators used for air quality monitoring are ozone, Green House Gases (GHG); Particulate Matter (PM); Pb, Aerosol, Air Quality Index (AQI). To tackle air pollution problem at Delhi, few low-cost air quality sensors prototype one of MIT have been deployed on the ground. They are reporting data to a remote server every 30 s. There is another regulatory sensor co-located with it for calibration. As spatial coverage is required, one of the sensor is made mobile too by moving it on rickshaw. So, governments of various developing countries are working towards meeting this challenge, like Government of India has checked indoor air pollution remarkably by providing smoke free kitchen through 'Pradhan Mantri Ujjwala Yojna'.

1.1.1 Air Pollutants Classification

The pollutants can be classified into various categories on various basis. There are two types of pollutants, primary pollutants and secondary pollutants. The pollutants that are directly emitted into the atmosphere are called primary pollutants, whereas secondary pollutants are formed in the atmosphere from primary pollutants. Compounds of carbon, nitrogen, sulphur, halogen, and particulate matter fall under the category of primary pollutants. And ozone, sulphuric acid, droplets, sulphates, nitrates, and organic particles comprise secondary pollutants. Now-a-days, a new type of smog is recognized that is composed of secondary pollutants such as ozone, and lead (Pb). Other classification could be gaseous (SO_2, NO_x, O_3, CO etc.) and particulate air pollutants (PM_{10}, $PM_{2.5}$, $PM_{1.0}$). Air Pollution could also be classified into indoor and outdoor pollution based upon the place where the pollution activities take place. Improper ventilation in buildings can make pollutants concentrations high than those found outside. NO, CO, SO_2 emissions from dirty cook stoves and furnaces are major contributors to indoor pollution. According to WHO, in India, about 5 lakh deaths occur due to indoor

pollution caused by unclean cooking fuels. The indoor pollutants include nitrogen oxides, sulphur dioxides, carbon monoxide, hydrocarbons and different particulate matter. Indoor air pollution also causes acute respiratory diseases in young children. It is said that burning of fuel openly in kitchen is like burning 400 cigarettes an hour. Furthermore, while doing air quality measurements of gases, there are two ways, that is, mobile measurements and stationary measurements. Mobile measurements can be carried out at random locations and it will determine the ambient spatial distribution of pollutants, whereas, stationary measurements aid in continuously recording the temporal distribution at fixed points which could be representative ones for the investigating area.

1.1.2 Air Quality Indexing

Air Quality Index (AQI) tool is used to monitor air quality in urban cities of the world on a real-time basis. Number of pollutants are considered for determining AQI viz, PM_{10}, $PM_{2.5}$, CO, O_3, NO_2, SO_2, NH_3 and Pb. The AQI bands are color coded like orange (101–150), red (151–200), purple (201–300), and maroon (301–500) for citizens' look-up for enabling them to learn about their health and decide further course of action if required. Recently only, The Economic Times on May 9, 2019 reported that India's capital city of Delhi's air quality index as recorded by the System of Air Quality and Weather Forecasting and research (SAFAR) is 408 because of the sudden rise in particulate matter concentration. It may be noted that an AQI in the range 0–50 is considered 'good', 51–100 'satisfactory', 101–200 'moderate', 201–300 'poor', 301–400 'very poor', and 401–500 'severe'. So there is a need to control the contaminants those are responsible for causing pollution.

This article is an attempt to monitoring of the air pollution continuously and make the data available to the world using IoT, so that necessary counter action can be made before it gets hazardous. For this design project study, a sensor based prototype for detecting the air pollution in a pilot site in Kurukshetra, India has been created and examined. The remainder of this article is laid out as follows. The Sect. 2 throws challenges on that occur during continuous air pollution monitoring in smart cities. Section 3 presents the related works available in literature. Section 4 mentions the system architecture with its software and hardware description. Section 5 provides the implementation details and discusses the results obtained. Last section draws the conclusion and future scope of work.

2 Challenges During Continuous Air Pollution Monitoring in Smart Cities

Monitoring refers to measurement over a required period together with recording of the measurements data and continuous monitoring refers to measurement without interruption during the period of interest and displaying the measurements result nearly instantaneously. There are several challenges during air pollution monitoring of smart cities, which are being discussed in this section.

1. Defining the measurement plan
   For air quality measurement in real time scenario, the measuring plan should be defined precisely. This is important, as the measurement result would be different with mobile measurement than with stationary one.
2. Choice of site location and sampling
   The site location where air quality measuring station is being located is significant especially during real time monitoring as proper spatial coverage is required, especially in populated areas such as busy roads, school, hospital or city centres. In this scenario, the data is continuously transferred to a central station. Here, selecting the site location means that sample is representative of the area. There are guidelines for site locations to be chosen up. So it is important to follow these standardized criteria while planning this real time monitoring. Moreover, there are certain violent pollutant gases like NO, which must be continuously measured at locations having high concentration profile.
3. Accuracy of Measurements
   The correctness of measurement is of paramount importance. In air pollution measurements, calibration and adjusting a measuring instrument is required. The measuring station must be equipped with calibration gases. Moreover, the environment of the monitoring station must be controlled for maintaining a constant temperature for instruments as parameters like humidity, temperature affects the accuracy of measurements results.
4. Methodology adopted
   For providing air quality data in real time, various methods can be adopted. There is a traditional way of passive sampling to the most sophisticated ones i.e. with use of remote sensing devices. The monitoring methodology adopted should be appropriate as it would affect the cost, reliability, and complexity of operation.
5. Consistency of power supply
   As pollution monitoring requires continuous data collection, there is a need of an on-board power source. Inconsistent power supply and voltage fluctuations affect monitoring; therefore, continuous source of energy is constantly required. In case of IoT devices, prolonging the battery life is a research challenge.
6. Real time continuous monitoring
   If data is reported in real-time, it helps the authorities to formulate action plan and issue daily alerts. But, there is time-lag in reporting of the collected data in air quality monitoring systems. Moreover, data transfer between the sensor node, the core component, and the cloud requires reliable channels. And for transferring data in real-time, appropriate approach is required to be used, like cellular networks or Wi-Fi hotspots.
7. Development of air quality emissions inventories
   It is essential to understand the type of air pollutants being emitted from various sources and ambient locations. The authorities need to understand the profile of city's air pollution i.e. not only the sources, but also the emission rates and trends. Therefore, air quality management requires to develop emissions inventories for effective implementation of air pollution control method. It is important to generate specialised data in order to safeguard public health and the environment beyond the routine monitoring.

8. Cost efficiency
   Continuous ambient air quality monitoring stations that report data in real-time are costing a lot. It comprises of meteorological instrumentation, calibration systems, analysers, sensors, display units etc. Therefore, low cost communication is a challenge.
9. Sensing technology
   Data collected by the sensors should be reliable, then only it will be suitable for urban sensing. So the low-cost sensors which are being used must perform appropriate calibration. So calibration methods are to be developed and more so for providing accuracy because hardware components and signal drifts over time or environmental factors like humidity, temperature affects sensitivity.
10. Security and privacy
    Smart cities are providing internet connectivity to number of devices. This makes security issue a critical challenge. In smart cities, software protection, authorization, communication protocols are some of the important concerns which are vulnerable to attacks. IoT based smart city poses a challenge of privacy by doing over-collection of data than that is required, and by leaking the collected data to third parties.

3 Related Work

There is a phenomenal growth in low-cost sensors due to advancements in VLSI technology, micro-electromechanical systems and wireless communication. In this section, an insight to air pollution study has been made using such low-cost sensors. Table 1 lists typical air pollutants of interest and presents their issues of concern during measurement. Issues such as interference, cross-sensitivity, correction etc. must be overcome during design and development of air pollution systems. Furthermore, in the following paragraphs, recent research efforts towards air pollution monitoring in smart cities is discussed.

A number of researchers have already come up with different solutions to solve air pollution monitoring. Each of them have their own approach. An analysis of sensor network deployment for air pollution monitoring systems has been given in Reference [26]. A practical implementation of 3D air quality sensing has been done in Peking University and Xidian University [27]. It is using spatial fitting and short term prediction as data processing technique, deployment based on aerial and ground sensing, and power control technique to balance between power consumption and data accuracy. The air quality sensing system is fine grained and made real time using large number of tiny sensors. With this system, big data can be collected and analyzed and information of pollution level can be timely provided to the citizens. Another approach with graphical signal model is used by authors of [28] for inferring or predicting air quality in New York City. Community of buildings having large $PM_{2.5}$, and NO_x have been identified. Each building is considered to be an element in a data set which is then analyzed based on Louvain method using a complex network system. The surrounding air quality could be quantified with the data collected and the trend of air quality can be

obtained in big cities with this approach. Indoor pollution which is the contamination of closed places like homes, offices etc. is monitored successfully in [29]. The system is implemented using an Arduino microcontroller, Raspberry Pi processor and a semiconductor ozone sensor has been used particularly targeting ozone gas level indoors. The IoT devices collect data periodically at an interval of 5 min [29].

Indoor air quality (IAQ) parameters are crucial as people spend most of their time in indoor environment. A research work using Internet of things technology has been developed for CO_2 monitoring [30]. It may be noted that CO_2 levels above 1000 ppm indicates indoor air pollution environment. Other than detecting air pollution, the monitored data can be used for medical purpose. In another study, a system based on wireless sensor network is realized for monitoring indoor air pollution [31]. It takes into account stationary nodes realized in a specific location and switches to mobile nodes in a city using mobile phones. This is done to ensure quality of service by monitoring full coverage area. In [32], research work improved indoor air quality by controlling particulate matter (PM) like dust, bacteria using an atmospheric pressure plasma. The study used two types of electrodes, disc-type, and needle-type reactor for particle collection and formaldehyde removal. The electrodes operated at low voltages as compared to other electrostatic precipitators being used to remove particulate matter from gases. In this, the electrodes were designed to have a small discharge gap, thereby reducing the discharge voltage.

Research work [33] has classified the low cost sensors into two groups i.e., sensors that measure pollution in inner city areas and sensors that measure pollution in outer city areas. This is based on the fact that pollutants concentration is usually uniform during night in inner city which is due to traffic variations and is uniform during afternoon in outer city locations. So calibration of these sensors should be done accordingly. The state of the art of the low-cost portable air pollution sensors has been published in [34]. These potable sensors have enabled air pollution monitoring at high spatiotemporal resolution whereas the conventional air pollution monitoring systems resulted in low spatial resolution and sparse coverage, as they are bulky, costly, and therefore deployed in few numbers at representative locations only [35]. However, because data provided by these low-cost sensors is not so reliable [36], research works have been done for providing appropriate sensor calibration and thereby made them suitable for urban sensing [37]. Furthermore, these low cost sensors were classified on the basis of the target pollutant as PM and gaseous sensors [35]. Such PM sensors are mostly based on optical sensing principle, and thereby can also differentiate sizes of particles. The majority of such gaseous sensors are based on electrochemical principle. Poor measurement accuracy of these portable sensors has been found to be because of internal errors such as signal drift over a long time [38] or external errors such as environmental factors like increase of humidity or external errors such as environmental factors like increase of humidity decreases the sensitivity of electrochemical sensors [39]. So these sensors need to be calibrated. Some calibration methods are developed and research works performed in both labs [36] and fields [40]. A low-cost implementation has been examined for estimating $PM_{2.5}$ concentrations in a roadside urban traffic scenario with a mobile test run [41]. High accuracy was obtained and certain delay in observations were noted due to limitations of equipment employed.

In a smart city monitoring, the idea of crowd sensing has been in use for many applications for example, not only for estimating air quality, providing traffic information, structure health monitoring etc. Crowd sensing idea implies outsourcing the sensing tasks to the crowd. Now-a-days, Smart phones are popular and they are integrated with on board sensors like, GPS, camera, accelerometers, microphones, compass [42]. So a study in [43] has been done to use smart phones to estimate air quality and PM 2.5 concentration in cities.

Table 1. Typical air pollutants and their limitations with their sensor types

Air pollutant	Type	Source	Issues/effects
Ozone (O_3)	Secondary	Formed via UV (sunlight) and pressure of other key pollutants	Relative Humidity (RH) Temperature Cross-sensitivity of oxidizing gases e.g. NO_2, H_2S, Cl_2 Long term stability (ageing or drift)
Carbon monoxide (CO)	Primary	Fuel combustion-mobile sources, industrial processes	Relative humidity Temperature Cross-sensitivity of reducing gases (e.g. SO_2, H_2S) Long term stability(ageing or drift)
Sulfur dioxide (SO_2)	Primary	Fuel combustion-electric utilities, industrial processes	Relative humidity Temperature Cross-sensitivity of reducing gases (e.g. NO_2, H_2S) Long term stability(ageing or drift)
Nitrogen dioxide (NO_2)	Primary and Secondary	Fuel combustion-mobile sources, electric utilities, off-road equipment	Relative humidity Temperature Cross-sensitivity of oxidizing gases (e.g. O_3, H_2S, Cl_2) Long term stability(ageing or drift)
Carbon dioxide (CO_2)	Primary	Fuel combustion-electric utilities, mobile sources	Relative humidity Temperature Cross-sensitivity of reducing gases (e.g. CO)
Volatile organic compounds (VOCS)	Primary and Secondary	Fuel combustion(mobile sources, industries) gasoline evaporation; solvents	Relative humidity Temperature
Particulate matter ($PM_{2.5}$, PM_{10})	Primary and Secondary	Fuel combustion(mobile sources, electric utilities, industrial processes), dust, agriculture, fires	Relative humidity High humidity and high temperature decreases the accuracy of the sensors.

One of the smart city solution is being envisaged in the city of Porto, Portugal. A city-scale IoT deployment has been made to monitor air quality, namely *UrbanSense* and to acquire some other data namely *SenseMyCity* and *BusNet* [44].

The study proposed in [45] suggests that the pollution monitor is installed at a location which has an ability to monitor about five different kinds of environmental

parameters, and each installation point costs about $10000. Herein, IoT has been combined with environmental protection to make a real time "air" pollution monitoring and forecasting system. To analyze the forecasting, the system uses neural network technology. In this implementation the whole system is divided into three layers namely Perception layer, Network and Application layers.

A different implementation can be found in [46] using a ZigBee module and a wired internet connection (Ethernet) for connectivity. The drawback of using ZigBee module is that the data is available only in the locations near to the device. A real time pollution monitoring system was proposed in [6] using pollution sensors MQ 135, MQ 7 and PIC microcontroller. The pollution data is transferred to servers which is then made accessible by traffic control stations. The use of PIC microcontroller is a kind of unnecessary for this simple task of collecting and uploading the pollution data.

A prototype based on an IoT based notification for air quality monitoring in respect of particulate matter and carbon monoxide has been designed for Manila city of Philippines [47]. The system is developed with the use of Raspberry Pi, Gizduino microcontroller, MQ-7 toxic gas sensor, and dust sensor.

The work proposed by Sarun et al. [48] have developed smart multi-sensor based air pollution detection system using NB-IoT network for city of Bangkok, Thailand. The real-time data such as that of CO, O_3, PM_{10}, NO_2, SO_2 can be measured for determining the AQI of a particular location. Another research group used electro-chemical sensors MQ4, MQ9, and MQ135 to detect pollutants in public transport routes of districts of Lima so that pedestrians could be made aware of it for further action at their end [49]. At Inverleith, Scotland, an IoT based air pollution campaign has been conducted to encourage people for cycling habit. IoT devices were utilized to perform data analysis, physical data visualization for creating awareness among people related to air pollution issues [50].

A hierarchical air quality monitoring system prototype based on IoT technology has been developed at Beijing University of Technology to monitor air pollution of Beijing city [51]. The findings have confirmed that automobile emission is the major pollutant source in Beijing city of China. The IoT sensors such as CO, SO_2, NO, NO_2, $PM_{2.5}$ were deployed hierarchically in each floor inside the buildings. The sensed data was sent to information processing center through ZigBee wireless protocol for carrying out real time monitoring of air quality.

In other study, in UAE [52], researchers have integrated IoT technology to remotely detect pollution without human interaction. An IoT system has been described that monitors real-time data and alerts when pollutants exceed a given threshold. This system comprises of Waspmote microcontroller, gas sensors, and wireless gateway which can communicate with cellular mobile system, Xbee/RF radio.

Similar work on Air Pollution Index (API) monitoring system has been devised using IoT technology and Sigfox low power wide area network (LPWAN) communication technology at University of Limerick [53]. This method is an attempt to overcome the problems being faced by earlier methods viz. limited communication distance, high maintenance cost, large energy consumption and short life. The IoT devices need network connectivity for their operation. A number of networking and communication technologies are used, some of which are Sigfox, Low power personal area network (6LowPAN), low range wireless area network (LoRaWAN) [54]. In smart

cities, it is expected that with availability of such low power technologies, like LoRa, large number of sensors can be connected and interconnectivity can be provided. In fact, this wireless technology has been developed keeping in mind IoT and smart cities. Moreover, it has the capability to connect smart cities' various sub-systems, for example parking, waste management, lighting etc. This advantage can be realized in a way, that the average time required by a vehicle to be parked can be reduced with it and thereby CO_2 emissions can be reduced. The air pollution monitoring application or service of smart city requires long range and low data rate communications. The comparative performance of current IoT access technologies (LP-WAN) is available in literature in reference [55].

The authors in [56] have developed edge computing based IoT architecture prototype for low-cost air pollution monitoring systems. In this, edge computing device performs operations and analysis on the sensed air quality data gathered by sensors in real-time. The prototype was developed with Arduino platform and it monitors particulate matter and gases together with humidity and temperature. This work has taken into account temporary errors that may occur in low cost sensors and cross–sensitivity

Table 2. IoT based projects in smart cities

S. no.	Smart city project	City	Country	Application remarks
1	Padova Smart City	Padova	Italy	Collects CO level, air temperature, humidity and benzene measurement level in the air
2	Green IoT Smart city	Uppsala	Sweden	Uses CO and NO_2 sensors on Bus for air quality, and $PM_{2.5}$, PM_{10} sensors on Lampposts for dust particle monitoring
3	CityVerve	Manchester	England	CityVerve is based on an open data principle that incorporates a "platform of platforms". Monitors air quality at different heights and locations
4	Connecting Copenhagen	Copenhagen	Denmark	Working with Google and installed monitoring equipment in their street view cars to produce a heatmap of air quality
5	Opensense	Zurich, Lausanne	Switzerland	Integrating air quality measurements from heterogeneous mobile and crowdsensed data sources
6	Everyaware	Lower Saxony	Germany	An affordable low-cost sensor with a smartphone and a web service have been developed
7	Citi-sense-MOB	Oslo	Norway	Bicycle-based air quality measurement
8	Air View	Oakland	California	Google Street View cars travelled around West Oakland for taking air samples
9	Friends of the Earth	London	England	Govt. supplying citizens with testing kits, so they can learn more about the quality of the air in their local areas

problem. In order to ensure the accuracy of reported data, automatic calibration was applied. The authors in [57] have framed a near real-time smart city application. It supports IoT data collection, event detection and data analytics. For obtaining cleaner air across the UK, its cities having some worse pollution in Europe, the solution provided was to move to electric cars. But recently, it has been determined that they still deliver about three quarters of the pollution through their tyres and brakes. So the answer to obtain clean air is more cycling and walking.

Table 2 summarizes certain existing air quality monitoring projects in IoT enabled smart cities all over the world. Although different implementations of the pollution monitoring problem based on Internet of Things have been proposed in recent years, not many are implanted at lesser installation and maintenance cost. The data obtained by many of those implementations is not accessible in real time. Some of the solutions are not provided with internet connectivity making the data accessible only to those in the near vicinity or just to the authorities. Although the conventional pollution monitoring system followed by various governments is accurate, it demands a huge immobile setup.

This makes the data unavailable remotely and is unauthorized too. Unlike these systems, the proposed system can be installed at any remote location with a very low cost as compared to other existing ones. Furthermore, it does not require any local servers or databases as the device is connected to the internet, and system updates the data directly. Efforts are being made by the authorities to deploy sensors in the urban cities of today to monitor air quality, water, waste, and traffic. Still there is a requirement to provide information in near real time by processing the raw data gathered and interpreting it into actionable information.

4 The System Design

As viewed from literature, IoT has been widely applied in smart cities to accomplish a number of environmental monitoring applications, in particular air pollution monitoring. It is seen that with the introduction and application of Internet of Things, many IoT based air monitoring systems have been proposed by a number of researchers. The central component of air pollution monitoring system is a pollutant detector (sensor) that can detect any dangerous elements in the air that shall decrease the air quality. The main advantage of IoT implementation for air pollution monitoring is availability of low cost hardware. In this section an Internet of Things based system is being discussed in detail which can be used to monitor the air pollution in real time. Table 3 lists different kinds of sensors that are used for implementing IoT based air pollution monitoring systems, viz. humidity, temperature, light intensity in addition to air quality sensors.

Table 3. Sensors used for IoT

S. no.	Parameters		Sensors	Range
1	Gas	NH_3, CO_2, S, C_6H_6,N_2S, alcohol	MQ-135	10–300 ppm (NH_3) 10–1000 ppm (C_6H_6)
		NO_2	MiCS-2714	0.05–10 ppm
		CO	MQ-7	10–10000 ppm
		O_3	MiCS-2614	10–1000 ppb
2	Fine Particulate Matter ($PM_{2.5}$)		SPS30	over 0.3 µm
3	Particulate Matter (PM_{10})		PPD42	over 1.0 µm
4	Humidity & Temperature		DHT-11, DHT-22	Detect 20–80% (DHT-11) 0–100% (DHT-22)
5	Light intensity		LDR	5 mm, 8 mm, 12 mm and 25 mm
6	Pressure		BMP-180	300–1100 hPa
7	Rain		FC-37	–
8	Total Volatile compound (TVOC)		ZMOD4410	5 ppm–20 ppm
9	Volatile Compound (VOC)		CCS811	400–8192 ppm

A. The System Architecture

Hardware impacts IoT product's value, experience of user and application abilities. There are basically 4 building blocks of IoT hardware for any application and can be understood by block diagram given in Fig. 2.

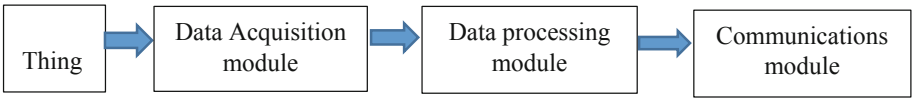


Fig. 2. The IoT system architecture

In air pollution monitoring these blocks shown in Fig. 2 could be namely:

(i) Thing – controlling of pollution levels.
(ii) Data acquisition module – Gas sensor MQ135
(iii) Data processing module – Arduino UNO
(iv) Communication module - ESP8266 Wi-Fi module.

The architecture of Arduino based IoT solution for air pollution monitoring system is illustrated in Fig. 3. The Arduino microcontroller takes the input of pollution level from the Pollution Sensor (MQ-135) and processes the data to find the pollution in ppm (parts per million) after initial calibration. The value is then uploaded to a server named ThingSpeak so that the pollution levels can be accessed from any place via an Application or a website.

The device thus developed can be installed near any Wi-Fi hotspot in a smart city. The Arduino board can load the required libraries as soon as the board is powered and fetches sensed data from MQ-135 sensor which is in the form of analog output voltage. The value of the voltage generated is proportional to the amount of pollutant gas in parts per million (ppm). The analog voltage obtained at the analog pin of the Arduino is digitized by built-in analog to digital converters (ADC's) which takes the value between 0 to 1023. This value is later sent to the Wi-Fi module in the form of string as an input. The sensor can be calibrated so that its analog output voltage is proportional to the concentration of polluting gases in ppm.

The Wi-Fi module is connected with the ThingSpeak which is an IOT platform which provides analytics service that allows to visualize and analyze live data streams in the cloud. The connection between Wi-Fi module and ThingSpeak server can be established by using AT Commands. Initially "AT" command is sent by controller to Wi-Fi module using software serial function. 'OK' response appears if cloud service is running. If 'AT+GMR' command is made, Wi-Fi module responds to it with the version information. After this, the parameter in command, 'AT+CWMODE', is set to 3. With this setting, Wi-Fi module is configured to softAP as well as station mode. It sends back the string as an output indicating that its connection mode is set.

For restart of the Wi-Fi module, 'AT+RST' command is made. Command 'AT +CIPMUX' is set to '1' for setting multiple connections or made '0' for setting single connection.

To take SSID of the registered cloud service on ThingSpeak and password to login the cloud service, command, 'AT+CWJAP' is used. For sending back the local IP address of the Wi-Fi connection, command 'AT+CIFSR' is used.

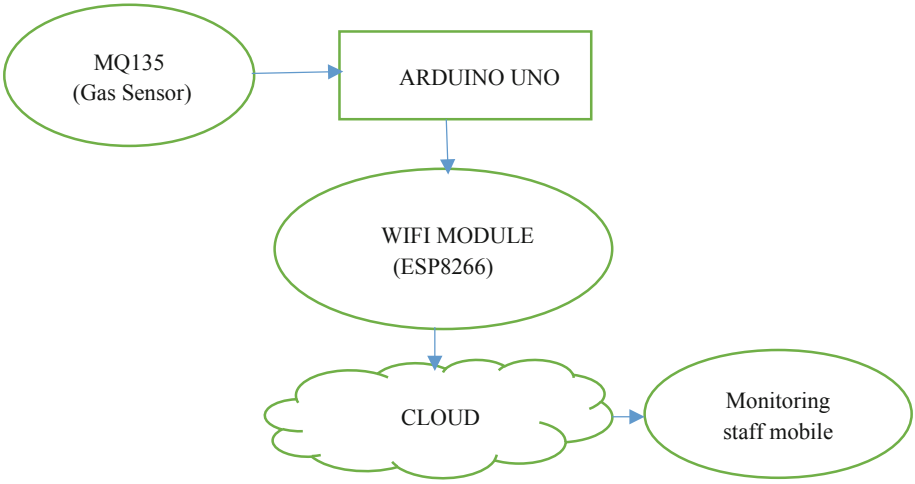


Fig. 3. Architecure of IoT based air pollution monitoring system

'AT+CIPSTART' command is used to establish a TCP connection, register an UDP port or establish an SSL connection. For TCP connection to be established, this command takes four number of parameters. First parameter is link ID i.e. a number between 0–4, second parameter is connection type, 'TCP' or 'UDP', third parameter is remote IP address or IP address of the cloud service to connect with and last parameter is to enable or disable TCP keep alive feature and for setting detection time interval. If it is set to '0', it would be disabled, otherwise time interval in seconds ranging from 1 to 7200 can be passed. The server response is 'OK' if connection is successfully established, otherwise it responds with 'ERROR' message.

In this study project, a string containing the URL having API key and the sensor value as the field value is passed. The passed field and its value are logged on the cloud server. It is important to pass the API key in this URL as one of the field value in order to connect with the registered cloud service. The air quality measured by sensor can now be monitored and recorded through the ThingSpeak IoT platform. Using 'AT +CIPSTART' command, the Wi-Fi module accesses the link given below with the actual pollution level value for updating the same to the server.

https://api.thingspeak.com/update?api_key=UZMM5BU15GWAVK2I&field1=0.

Here, if the value at the end is any integer, then that is updated to the server.

B. The System Hardware

The hardware components used are discussed briefly in this sub-section.

(i) **Arduino Uno**

It is open source microcontroller and can be programmed using C/C++ with some specified library. It is small in size and easy to use with many built in libraries to code. It acts as a data processing module. This system uses an Atmega 328 microcontroller. The specifications of Arduino Uno are as follows. It contains14 digital I/O pins and 06 analog input pins [58]. The operating voltage is 5 V DC with the clock speed of 16 MHz. The MQ-135 sensor is connected to it through an analog input pin and two pins are utilized to interface the ESP 8266 Wi-Fi Module.

There are many microcontrollers out there in the market but still Arduino rules the market because of its simplicity and other advantages. It is inexpensive (under 50$), cross platform, easy to program and supports large number of actuators and sensors [59].

(ii) **MQ-135 Gas Sensor**

In the architecture presented in Fig. 3, a low cost semiconductor gas sensor MQ-135 has been used which detects ammonia (NH_3) and carbon dioxide (CO_2). The gas sensor forms front end of the IoT based monitoring system. Hence is called "things" of the system. The main purpose of these things is to accumulate data from environment (Sensors) or provide data to the surroundings (Actuators) [60].

MQ-135 gas sensor uses tin dioxide (SnO_2) as the gas sensitive material. It increases its conductivity with increase in concentration of pollution in air. In case of clean air, it has low conductivity. It is ideal choice for monitoring of harmful gases and smoke. The advantage of using this sensor is its low

manufacturing and maintenance cost, reduction in energy consumption and node volume. For cost efficient pollution monitoring system, semiconductor sensors are suitable and are required to be used in array form [60]. In addition to it, some other type of sensors for pressure, temperature, and humidity measures can also be incorporated into the system.

(iii) **ESP8266 Wi-fi module**
The Wi-Fi module, ESP8266 is a less power consuming, high performing, Wi-Fi network control module designed by Espressif [61]. It meets the different IoT requirements and used vastly in different IoT applications like smart home, industrial automation, biotechnology etc. The ESP8266 is having capabilities of UART and pulse-width modulation. The ESP8266 can support automatic power save delivery for Internet Protocol applications and Bluetooth interfaces. This acts as the communication unit and is required for communicating the acquired data to cloud. The ESP8266 is chip based.

5 Implementation and Analysis

The system was developed as discussed in Sect. 4 and made running continuously. For the purpose of analysis, experimental readings were noted for four consecutive days i.e. 22–25 November, 2018. A total of 444 readings were noted. It was observed that the values noted are in agreement with the real time situations while representing different conditions of air. Different environmental conditions were created with different concentrations of pollutants in the air by use of aerosols, fire and smog, viz. generating smoke by burning of paper, spraying deodorant etc. The readings of such contaminated conditions can be seen in the graph with increased value of pollution levels than that of normal conditions. It may be noted that in the proposed system, the gas sensor output being analog gives an output ranging from 0 to 1023 which is a proportional value to the actual ppm value of NH_3 and CO_2 present in surrounding environment. In normal situations, i.e. when the air pollution is under control or human tolerable level, then the value of air pollution recorded with the proposed system is in the range of 25–30. In Fig. 4, each dot represents individual reading that is updated to the server. It can be observed that when a constant value has been updated repeatedly as on 25 Nov. 2018, the dots appear too close to each other. It shows that the pollution level remained almost constant as the same value has been updated repeatedly. The pollution level of fresh air has been observed to be almost constant for the whole observation period as shown in Fig. 4. In fresh air, the value is observed to be 31 on an average out of a large number of readings. The situation when pollution environment was created manually, the readings recorded by the system is 164 (i.e. at least above 100, depending upon the extent of pollution present in the atmosphere in the vicinity). It is represented by peaks in the plot shown in Fig. 4, that is on 22nd and 25th Nov. 2018. The increased value of air pollution on 22nd Nov. 2018 is due to the smoke generate in the atmosphere near to the device. The increased reading of air pollution on 23rd Nov. 2018 is because of the smog that was present in the atmosphere on that night. And the peaky reading observed on 25 Nov. 2018 is 116, which was because of spray of aerosol in the surrounding.

Figure 5 shows a bar chart depicting air pollution measurement result for a day i.e. 22nd November, 2018 at different time. In addition, Fig. 6 shows the minimum and maximum value of air pollution levels observed during observation period, that is 22–25 Nov. 2018.

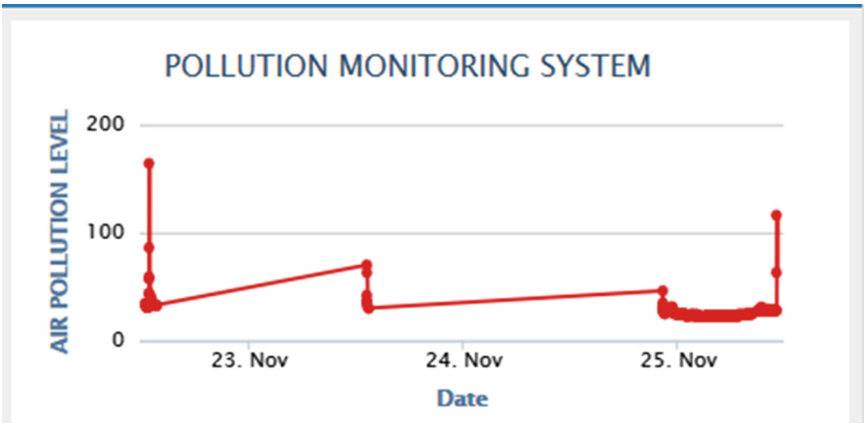


Fig. 4. Air pollution recorded data

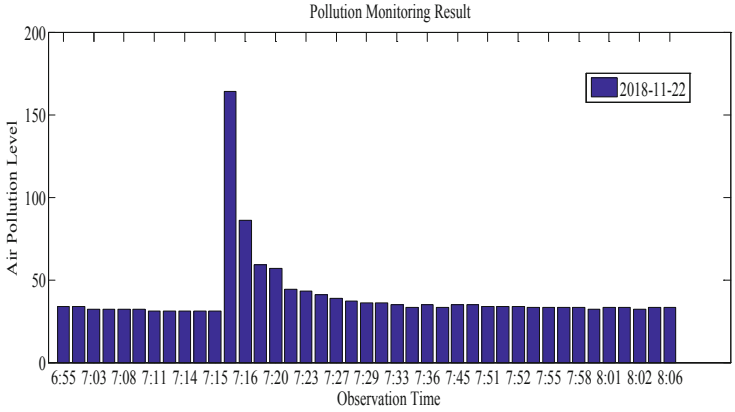


Fig. 5. Air pollution measurement result of one day

The results shown above clearly agree with the created environment of pollution in the vicinity of the Sensor. One thing that is noticeable is that the range of the device is in need of continuous internet supply and any discontinuity would result in loss of the data. However, as the developed system uploads data at every instant, loss of some data would not cause any damage since the pollution levels doesn't increase drastically.

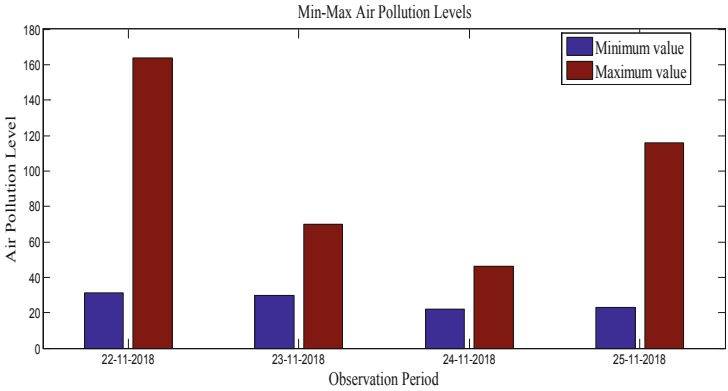


Fig. 6. Minimum and maximum values of air pollution observations

6 Concluding Remarks

Air pollution is a major threat to our ecosystem and the planet as a whole. It has been on the rise due to industrialization and combustion. As the population is growing, this challenge of air quality monitoring becomes more complicated and the cities need to prioritize it. More people means more waste, more congestion, and more pollution. Pollution data can impact the mobility of people and the decisions required to be taken about the working hours, and more. There is a dire need to monitor it in order to preserve the smart city environment, and thereby work upon improving its quality. The governments all over the world are taking measures to control it, and doing urban planning by using the field data. Many countries are trying to switch to electric vehicles instead of petrol and diesel vehicles for reducing air pollution. Thus, air pollution can be reduced by using green transport, more green-belt areas, more renewable energy, separate paths for bicycles, and decreasing burning of agricultural wastes.

The elements that impact air quality can be connected and incorporated with IoT and big data. The proposed IoT in this article included the conventional modules in minimal configuration. The device developed is a pilot project. A low cost semiconductor gas sensor MQ-135, which detects gases such as ammonia (NH_3) and carbon dioxide (CO_2) was applied. The results plotted provides air pollution recorded data without gas decomposition and the value output by sensor MQ-135 used is an average of the different air pollutants like ammonia or carbon dioxide in in the range of 0–1023 depending on the pollution levels.

In this work, only gas sensor was taken into account. But as discussed in Sect. 3, it is not sufficient to measure air quality index. In order to improve the accuracy of measurement and for providing better analysis, in addition to gas sensor, other few sensors viz. humidity and temperature sensor etc. needs to be added. An IoT based air pollution monitoring system can thus be made helpful in determining the degree to which the air is polluted. IoT methodology can hence be used to develop cost effective solution to monitoring of air pollution. This work demonstrated real-time and location based air quality monitoring. This information provision to citizens will enable them to

make better choice of spending their time either indoor or outdoor. The people will be less exposed to harmful air pollutants.

The device can further be developed in such a way that depending on the pollution levels at that location, the device itself can take some counter action to control the same. Furthermore, one can create store data and by creating own database run the system on their own Server. The system at present is capable of detecting the air pollution of the surrounding and updating the recorded data at the server. This stored data can be analyzed using some techniques like Machine Learning and Deep Learning to forecast the future pollution trends at that location. Based on this data, many recommendations can be made for suggesting locations as to where new industries can be located without having any hazard to mankind, or a pollution source could be detected which is a threat to living beings.

Another modification in the proposed architecture could be made, that is the inclusion of an alert system. Alert messages may be sent to concerned pollution boards whenever pollution level of a particular location is observed to be increasing drastically, so that the authorities can take proper measures. For example, in case of pollution caused on busy roads due to heavy traffic, the authorities can control the road traffic of that particular area in order to reduce the pollution [62].

References

1. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything you wanted to know about smart cities: the Internet of Things is the backbone. IEEE Consum. Electron. Mag. **5**(3), 60–70 (2016)
2. Angelidou, M., Psaltoglou, A., Komninos, N., Kakderi, C., Tsarchopoulos, P., Panori, A.: Enhancing sustainable urban development through smart city applications. J. Sci. Technol. Policy Manag. **9**, 146–169 (2018)
3. Ge, X., Tu, S., Mao, G., Wang, C.X., Han, T.: 5G ultra-dense cellular networks. IEEE Wirel. Commun. **23**, 72–79 (2016)
4. Ashton, K.: That Internet of Things thing: in the real world, things matter more than ideas. RFID J. **22**, 97–114 (2009)
5. WHO: Ambient air pollution: a global assessment of exposure and burden of disease. World Health Organization, Geneva, Switzerland (2016)
6. Muthukumar, S., Mary, W.S., Jayanthi, S., Kiruthiga, R., Mahalakshmi, M.: IoT based air pollution monitoring and control system. In: Proceedings of International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, pp. 1286–1288 (2018)
7. Dwevedi, R., Krishna, V., Kumar, A.: Environment and big data: role in smart cities of India. Resources **7**(4), 1–10 (2018)
8. Bruneo, D., et al.: An IoT service ecosystem for smart cities: the #SmartME project. Internet Things **5**, 12–33 (2019)
9. Khan, B.N., Khan, M., Han, K.: Internet of Things: a comprehensive review of enabling technologies, architecture, and challenges. IETE Tech. Rev. **35**(2), 205–220 (2017)
10. Zhang, K., et al.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)

11. He, Y., Yu, F.R., Zhao, N., Leung, V.C.M., Yin, H.: Software-defined networks with mobile edge computing and caching for smart cities: a big data deep reinforcement learning approach. IEEE Commun. Mag. **55**(12), 31–37 (2017)
12. Gharaibeh, A., Salahuddin, Md.A., Hussini, S.J., Khreishah, A., Khalil, I., Guizani, M., Fuqaha, A.A.: Smart cities: a survey on data management, security, and enabling technologies. IEEE Commun. Surv. Tutor. **19**(4), 2456–2501 (2017)
13. Alavi, A.H., Jiao, P., Buttlar, W.G., Lajnef, N.: Internet of Things-enabled smart cities: state-of-the-art and future trends. Measurement **129**, 589–606 (2018)
14. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., Guizani, M.: Internet-of-Things based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel. Commun. **23**(5), 10–16 (2016)
15. Cenedese, A., Zanella, A., Zorzi, M.: Padova smart city: an urban Internet of Things experimentation. In: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Sydney, pp. 1–6 (2014)
16. Ahlgren, B., Hidell, M., Ngai, E.: Internet of Things for smart cities: interoperability and open data. IEEE Internet Comput. **20**(6), 52–56 (2016)
17. Bonola, M., Bracciale, L., Loreti, P., Amici, R., Rabuffi, A., Bianchi, G.: Opportunistic communication in smart city: experimental insight with small-scale taxi fleets as data carriers. Ad Hoc Netw. **43**, 43–55 (2016)
18. Sookhak, M., Tang, H., He, Y., Yu, R.: Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun. Surv. Tutor. **21**(2), 1718–1743 (2019)
19. An, J., Yang, K., Wu, J., Ye, N., Liao, Z.: Achieving sustainable ultra-dense heterogeneous networks for 5G. IEEE Commun. Mag. **55**(12), 84–90 (2017)
20. Wu, J., Guo, S., Huang, H., Liu, W., Xiang, Y.: Information and communication technologies for sustainable development goals: state of the art, needs, and perspectives. IEEE Commun. Surv. Tutor. **20**(3), 2389–2406 (2018)
21. Li, Y., Dai, W., Ming, Z., Qui, M.: Privacy protection for preventing data over-collection in smart city. IEEE Trans. Comput. **65**(5), 1339–1350 (2016)
22. Hou, L., Zhao, S., Xiong, X., Zheng, K., Chatzimisios, P., Hossain, M.S., Xiang, W.: Internet of Things cloud: architecture and implementation. IEEE Commun. Mag. **54**(12), 32–39 (2016)
23. Gutierrz, V., et al.: Empowering citizens toward the co-creation of sustainable cities. IEEE Internet Things J. **5**(2), 668–676 (2018)
24. Ang, L.M., et al.: Big sensor data systems for smart cities. IEEE Internet Things J. **4**(5), 1259–1271 (2017)
25. Rushikesh, R., Sivappagari, C.M.R.: Development of IoT based vehicular pollution monitoring system. In: Proceedings of International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, pp. 779–783 (2015)
26. Boubrima, A., Bechkit, W., Rivang, H.: Optimal WSN deployment models for air pollution monitoring. IEEE Trans. Wirel. Commun. **16**(5), 2723–2735 (2017)
27. Hu, Z., Bai, Z., Yang, Y., Zheng, Z., Bian, K., Song, L.: UAV aided aerial-ground IoT for air quality sensing in smart city: architecture, technologies and implementation. IEEE Netw. **33** (2), 14–22 (2019)
28. Jain, R.K., Moura, J.M.F., Kontokosta, C.E.: Big data + big cities: graph signals of urban air pollution. IEEE Sig. Process. Mag. **31**(5), 130–136 (2014)
29. Firdhous, M.F.M., Sudantha, B.H., Karunaratne, P.M.: IoT enabled proactive indoor air quality monitoring system for sustainable health management. In: Proceedings of 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, pp. 216–221 (2017)

30. Marques, G., Ferriera, C.R., Pitarma, R.: Indoor air quality assessment using a CO_2 monitoring system based on IoT. J. Med. Syst. **43**(3), 1–10 (2019). Article number 67
31. Naziha, A., Fu, L., Elamine, G.Md., Wang, L.: A method to construct an indoor air pollution monitoring system based on a wireless sensor network. Sensors **19**(967), 1–15 (2019)
32. Shimizu, K., Kurokawa, Y., Blajan, M.: Basic study of indoor air quality improvement by atmospheric plasma. IEEE Trans. Ind. Appl. **52**(2), 1823–1830 (2016)
33. Mueller, M., Meyer, J., Hueglin, C.: Design of an ozone and nitrogen dioxide sensor unit and its long term operation within a sensor network in the city of Zurich. Atmos. Meas. Tech. **10** (10), 3783–3799 (2017)
34. Maag, B., Zhou, Z., Thiele, L.: A survey on sensor calibration in air pollution monitoring deployments. IEEE Internet Things J. **5**(6), 4857–4870 (2018)
35. Rai, A.C., Kumar, P., Pilla, F., Skouloudis, A.N., Di Sabatino, S., Ratti, C., Yasar, A., Rickerby, D.: End-user perspective of low-cost sensors for outdoor air pollution monitoring. Sci. Total Environ. **607–608**, 691–705 (2017)
36. Castell, N., Dauge, F.R., Schneider, P., Vogt, M., Lerner, U., Fishbain, B., Broday, D., Bartonova, A.: Can commercial low-cost sensor platforms contribute to air quality monitoring and exposure estimates? Environ. Int. **99**, 293–302 (2017)
37. Thompson, J.E.: Crowd-sourced air quality studies: a review of the literature & portable sensors. Trends Environ. Anal. Chem. **11**, 23–24 (2016)
38. Kim, J., Shusterman, A.A., Lieschke, K.J., Newman, C., Cohen, R.C.: The BErkeley atmospheric CO_2 observation network: field calibration and evaluation of low-cost air quality sensors. Atmos. Meas. Tech. **11**(4), 1937–1946 (2018)
39. Paang, X., Shaw, M.D., Lewis, A.C., Carpenter, L.J., Batchellier, T.: Electrochemical ozone sensors: a miniaturized alternative for ozone measurements in laboratory experiments and air-quality monitoring. Sens. Actuators B Chem. **240**, 829–837 (2017)
40. Spinelle, L., Gerboles, M., Villani, M., Alexandre, M., Bonavitacola, F.: Field calibration of a cluster of low-cost commercially available sensors for air quality monitoring. Part B: NO, CO and CO_2. Sens. Actuators B Chem. **238**, 706–715 (2017)
41. Genikomsakis, K.N., et al.: Development and on-field testing of low-cost portable system for monitoring PM2.5 concentrations. Sensors **18**(4) (2018)
42. Du, R., Santi, P., Xiao, M., Vasilakos, A.V., Fischione, C.: The sensible city: a survey on the deployment and management for smart city monitoring. IEEE Commun. Surv. Tutor. **21**(2), 1533–1560 (2019)
43. Liu, X., Song, Z., Nagi, E., Ma, J., Wang, W.: PM2.5 monitoring using images from smartphones in participatory sensing. In: Proceedings of IEEE Conference on Computer Communications Workshops, pp. 630–635 (2015)
44. Santos, P.M., et al.: PortoLivingLab: an IoT-based sensing platform for smart cities. IEEE Internet Things **5**(2), 523–532 (2018)
45. Chen, X., Liu, X., Peng, X.: IOT-based air pollution monitoring and forecasting system. In: Proceedings of International Conference on Computer and Computational Sciences (ICCCS), Noida, pp. 257–260 (2015)
46. Wang, D., Jiang, C., Dan, Y.: Design of air quality monitoring system based on Internet of Things. In: Proceedings of 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Chengdu, pp. 418–423 (2016)
47. Caya, M.V.C., Babila, A.P., Bais, A.M.M., Im, S.J.V., Maramba, R.: Air pollution and particulate matter detector using Raspberry Pi with IoT based notification. In: Proceedings of International Conference on Humanoid, Nano-Technology, Information Technology, Communication and Control, Environment and Management, pp. 1–4 (2017)

48. Sarun, D., Takarn, A., Jamjareegulgarn, P.: A development on air pollution detection sensors based on NB-IoT network for smart cities. In: Proceedings of International Symposium on Communications, and Information Technologies, Bangkok, Thailand, pp. 313–317 (2018)
49. Medina-De-La-Cruz, M., Mujaico-Mariano, A., Soto-Cordova, M.M.: Implementation of an evaluation system to measure air quality on public transport routes using the Internet of Things. In: Proceedings of Congreso Argentino de Ciencias de la Informatica y Desarrollos Investigacion, Buenos Aires, Argentina, pp. 1–4 (2018)
50. Budiarto, A., Febriana, T.: IoT device used for air pollution campaign to encourage cycling habit in inverleith neighborhood. In: Proceedings of International Conference on Information Management and Technology, Yogyakarta, Indonesia, pp. 356–360 (2018)
51. Ma, Y., Yang, S., Huang, Z., Hou, Y., Cui, L., Yang, D.: Hierarchical air quality monitoring system design. In: International Symposium on Integrated Circuits, Singapore, pp. 284–287 (2015)
52. Alshamsi, A., Anwar, Y., Almulla, M., Aldohoori, M.: Monitoring pollution: applying IoT to create a smart environment. In: Proceedings of International Conference on Electrical and Computing Technologies and Applications, Ras Al Khaimah, United Arab Emirates, pp. 1–4 (2018)
53. Feng, Y., et al.: API monitor based on Internet of Things technology. In: Proceedings of International Conference Sensing Technology, pp. 213–216 (2018)
54. Ibrar, Y., Ahmed, E., Hashem, I.A.T., Ahmed, A.I.A., Gani, A., Imran, M., Guizani, M.: Internet of Things architecture: recent advances, taxonomy, requirements, and open challenges. IEEE Wirel. Commun. **24**(3), 10–16 (2017)
55. Ikpehai, A., et al.: Low power wide area network technologies for Internet of Things: a comparative review. IEEE Internet Things **6**(2), 2225–2240 (2019)
56. Idrees, Z., Zou, Z., Zheng, L.: Edge computing based IoT architecture for low-cost air pollution monitoring systems: a comprehensive system analysis, design considerations, & development. Sensors **18**, 1–23 (2018)
57. Puiu, D., et al.: CityPulse: large scale data analytics framework for smart cities. IEEE Access **4**, 1086–1108 (2016)
58. Pan, T., Zhu, Y.: Getting started with Arduino. In: Designing Embedded Systems with Arduino. Springer, Singapore (2018)
59. Adriansyah, A., Dani, A.W.: Design of small smart home system based on Arduino. In: Proceedings of Electrical Power, Electronics, Communications, Control and Informatics Seminar (EECCIS), Malang, pp. 123–127 (2014)
60. Parmar, G., Lakhani, S., Chattopadhyay, M.K.: An IoT based low cost air pollution monitoring system. In: Proceedings of International Conference on Recent Innovations in Signal Processing and Embedded Systems (RISE), Bhopal, pp. 524–528 (2017)
61. Zinca, D., Popa, M.O.: Development of a ZettaJS driver for the ESP8266 IoT hardware. In: International Symposium on Electronics and Telecommunications, Timisoara, Romania, pp. 1–4 (2018)
62. Khanna, A., Goyal, R., Verma, M., Joshi, D.: Intelligent traffic management system for smart cities. In: Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies. Communications in Computer and Information Science, vol. 958. pp. 152–164 (2019)

Data Mining and Fusion Techniques for Wireless Intelligent Sensor Networks

Ritika(✉), Nafees Akhter Farooqui(✉), and Ankita Tyagi(✉)

Department of Computer Applications, DIT University, Dehradun, UK, India
{hod.mca, nafees.farooqui, ankita.tyagi}@dituniversity.edu.in

Abstract. The Intelligent Wireless sensor networks (WSNs) are autonomous sensing devices that can quickly sense or monitor physical or environmental conditions from the distributed networks. WSN is an integral part of the research area for the real-time system. The Intelligent wireless sensor networks are to accomplish the vast volume actual-time data to take agreement making process that improves the computational technology. That inclines the analysis of the state to traverse the data mining and fusion proficiencies concerning obtaining perception from vast sustained approaching data from intelligent wireless sensor networks. In recent years the intelligent system had been implemented on various techniques similar to data mining and fusion, potency alive routing, task scheduling, reliability, and restriction. In this chapter, we explain the data mining and data fusion technique based on the different types of intelligent wireless sensor networks that detect forest fire. The suggested model is based on the rate of data fusion and the level of information fusion. Information resources are gathered from the intelligent heterogeneous sensors from the forest at the data fusion stage. The fire can be identified in the stage of information fusion by calculating the probabilities of data fusion. The process of fire detection in the forest will be completed with the help of the data that is collected from intelligent wireless sensors. Afterward, it is implemented by the data mining algorithm. We examined the performance of the scheduled data fusion access radically and analyzed it with other measured approaches. Finally, we got the performance of the data mining and data fusion techniques as an intelligent wireless sensor network has improved as compared to others. Besides, we explain the advantages and disadvantages of data mining and data fusion techniques over traditional WSN and intelligent WSN.

Keywords: Intelligent wireless sensor networks · Data mining · Data fusion · Computational technology · Heterogeneous

1 Introduction

In recent years, there is a drastic change in technology as sophisticated devices give the accelerations in communication technology. Wireless technology is used to communicate and provide connectivity back to the wired world. The wireless sensor node detects, senses, computes, transfers, and responds to input from the physical environment, which is required for communication.

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 592–615, 2020.
https://doi.org/10.1007/978-3-030-40305-8_28

Wireless sensor networks are a meshwork that consists of tiny detector stalks, which act as both generators and network relays. It is not only sensing components but also has on-board, processing, communication, and storage capabilities. With these enhancements, a sensor node is often not only responsible for data collection, but also used in-network analysis correlation and fusion of its sensor data and data from other sensor nodes. Each node of the wireless sensor network have three subsystems: the first subsystem is a sensor subsystem that precipitates the habitat, the second subsystem is organizing the structure that accomplishes the calculus on the sensor data, and the third subsystem is communication subsystem that is responsible for exchanging the information between the different sensors nodes. Nodes are either participate as a source junction; the source junction is accountable for the procurement of facts and communication to the sink node through more than one hop routing. Sink node processed that data and delivered it to the end-user.

Wireless sensor networks play a vital role in the development of military communication technology. In 1978, the Defense Advanced Research Projects Agency (DARPA) organized the Distributed Sensor Nets Workshop (DAR 1978), backing on sensor networks research summons acting as sensor networking automation, signal transformation techniques, and distributed designs. (DARPA) Also regulated the Distributed Sensor Networks (DSN) strategies in the early 1980s, which was later suspended by the Sensor Information Technology plans. The Rockwell Science Center and the University of California at Los Angeles prefers the completion of Wireless Integrated Network Sensors or WINS (Pottie2001). After then, Wireless sensor networks are broadly used in academics as well as in the different arena of society.

Forest engages the first part in the global, ecological environment and diversified structure. It massively impacts the proportion of ozone hurting substances, barometrical carbon maintenance, and decreases soil breaking down. It can coordinate the temperature and oversee precipitation. A forest fire is a catastrophe which comprises of a flame that lashes the enormous territory secured for the most part with trees and undergrowth and a significant risk for the untamed life. The spreading fire is one of the certifiable issues for the woods that ought to be controlled, which can cause enormous mischief. The general explanation behind the woodland flames is lightning, yet it can likewise be brought about by the carelessness of human arsonist tendencies. Throughout the mid-year, the drying leaves, parts of trees incite the flame. Subsequently, fire develops excessively ignitable. Consistently around 4 million hectares of forests are consumed, and a large portion of the backwoods has a place with the Mediterranean belt. The smoke that radiated from the destroyed forests can create genuine medical problems, for example, sickness, psychological instability, queasiness, heart assault, and even passing.

The traditional strategies for the anticipation of flame are very little powerful dependent on this. It is highly required to mindful individuals in this issue, all the more especially for the individuals who live in woods zones. It extremely impacts the proportion of ozone hurting substances, barometrical carbon maintenance, and decreases soil breaking down. Along these lines, in this section, we utilize the intelligent remote sensor organizes for the flame discovery at the beginning time with the assistance of information mining and information combination method. Early discovery is the essential route for lessening the harms of forest fires. Intelligent wireless sensor

systems, in comparison to satellite-based methods, can rapidly acknowledge and screen forest fires. These sensor nodes collect data as far as temperature, mugginess, smoke, and various parameters are concerned and send it to the specific group head; from that stage on, these bunch heads send the data to the supervisor hub creating a network. In request to direct the investigation, we survey the current methodology for the accumulation of information through the sensor [1–3]. The prior expectation of flame in the backwoods will help in the (FMS) Fire Management System and the forests chiefs' inappropriate asset distribution, for example, giving enough air tankers and ground groups.

The overall chapter is divided into eight sections namely the first section is intelligent wireless sensor network. The second section is application of wireless sensor networks. Fourth section is, data mining in wireless sensor networks. The fifth section is, data fusion. In Section six, Forest Fire Monitoring Systems dependent on Data mining and Data combination techniques. Discussion and conclusions are accounted for in section seven and eight individually.

2 Intelligent Wireless Sensor Networks

An intelligent sensor is a sensor that has advance learning, adjustment, and development capacities. Sensors are astute when it is equipped for adjusting mistakes that happened during the estimation of both at the information and yield closes. A perfect sensor ought to have a direct association with the deliberate amount. Be that as it may, there are a few variables that are presented in the non-linearity framework that are required in canny sensors. A wise sensor makes some predefined moves when it detects suitable information (light, heat, sound, movement, contact, etc.). They can repay the information worth with the end goal that it has all the earmarks of being immaculate. Remuneration is the capacity to distinguish and react to changes in nature through indicative schedules, self-alignment, and adjustment. Keen sensors can assess the legitimacy of gathered information, contrast them and that of different sensors and affirm the exactness of any information variety. A perfect sensor ought to be so that it quantifies the touchy property just as to any obtuse property. Along these lines, it ought not to impact the deliberate property. Perfect sensors are encircled to be direct. The yield sign of such sensors is relatively straightforward to the estimation of the deliberate property. On the off chance that sensors are not perfect, the number of deviations can happen and may contrast from the worth indicated in the estimation of affectability; the yield sign isn't zero when the deliberate information is zero. Notwithstanding, such sensors are non-direct. Non-linearity assumes a crucial job when the affectability of a sensor isn't consistent over a range. On the off chance that nonlinear sensors are to be utilized, at that point, such calculations are intended to ensure that mistake substance is to be diminished Insight is characterized as the ability to supporting unique impromptu self-designing ongoing sensor organizes that can adjust shortcomings while keeping up estimation precision and worldly honesty. Remote sensor systems comprise sensor hubs, which are observed by unique situations that change quickly every once in a while. With the progression of the innovation, remote correspondence, and systems administration are combined with the

accessibility wise and minimal effort factor gadgets that are ground-breaking in the calculation and have correspondence abilities [14].

Remote sensor Networks are involved in countless sensor gadgets that can speak with one another through remote channels, with constrained vitality and processing abilities. WSN are worked under exacting vitality controlled, and the power that is provided is the most costly parts of the hub being planned. The insightful sensor hubs that are decked with different kinds of sensor, for example, warm, acoustic, substance, weight, climate, and optical sensors. Because of the assorted variety, WSN has the enormous potential for structure incredible applications in wellbeing observing framework, Traffic Controlling, Space Satellite Monitoring, Modern Agriculture, and so forth.

2.1 Architecture of Wireless Intelligent Sensor Network (WISN)

The planning of the Wireless Intelligent Sensor Network (WISN) comprises three sections: insightful sensors, microcontrollers, and radio interfaces. It is appeared as in Fig. 1, where smart sensors are utilized as detecting gadgets and actuators also for info and taking activities to give yields separately, the microcontroller controls the sensors and actuators through the ongoing working framework, radio interface used for accepting and transmitting the sign over the entire condition where it will deploy. Intelligent Sensor is a brilliant little gadget that has a microsensor innovation, low power sign handling, prepared to do quick information procurement, having critical vitality requirements, no constant support, dependable, and exact. The principle errand of a sensor in a sensor field is to recognize occasions, perform snappy neighborhood information handling, and transmit the information through the radio interface gadgets [16].

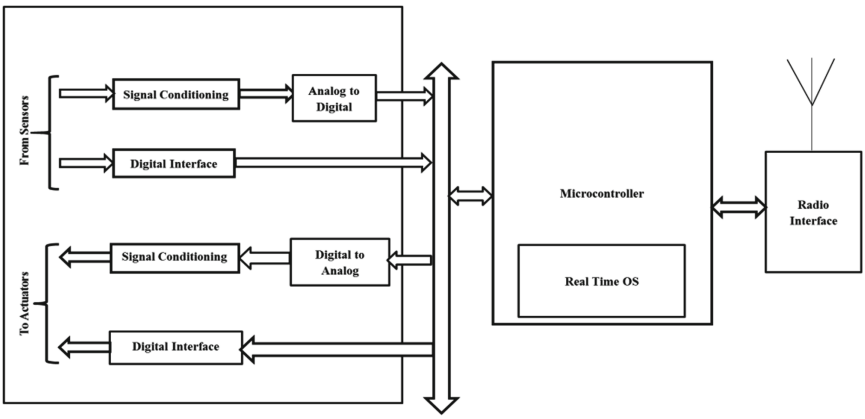


Fig. 1. Block diagram of a WISN

3 Application of Wireless Sensor Networks

There are various sorts of sensors, for example, seismic, attractive, warm, visual, infrared, acoustic, and radar, which can screen the temperature, moistness, weight, speed, bearing, development, light, soil cosmetics, commotion levels, the nearness or nonattendance of particular sorts of items, and mechanical feelings of anxiety on connected articles and so forth; along these lines, different uses of sensors are conceivable. This range of utilizations incorporates country security, checking of space resources for potential and human-made dangers in space, ground-based observing of both land and water, ecological observing, climate and atmosphere investigation and expectation, insight gathering for resistance, urban fighting, combat zone checking and reconnaissance, research of the Solar System and past, observing of seismic increasing speed, strain, temperature, wind speed and GPS information and some more. Distribution centers can improve their exhibition by introducing the sensors on the items to follow their area. The utilization of remote sensor systems are constant. Presently days, WSN's are being utilized in numerous potential application regions that are military data, water observing framework, natural checking of air and soil structure checking for structure and extensions, new machine finding, process checking resource following, and so forth [11] (Fig. 2).

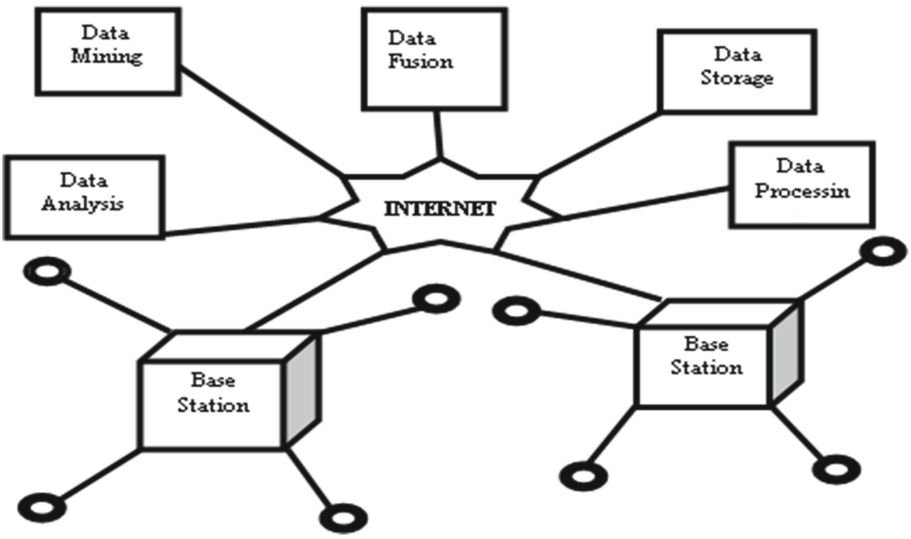


Fig. 2. Role of WSN in a different area

3.1 Military Applications

Wireless sensor systems are related to the military direction, control, interchanges, registering, knowledge, observation, and focusing on frameworks. Because of the adaptation to internal failure qualities of sensor systems, it utilizes as a promising

procedure for military arrangement. Sensor systems ideas are a superior methodology for war zones, in light of the fact that there are vast quantities of sensor hubs are utilized in the general military framework requiring little to no effort sensor hubs, on the off chance that there are a few hubs decimated by threatening activity, at that point there is no impact on military operation.

3.2 Health Applications

Biomedical gadgets and savvy coordinated sensors make the use of sensor systems for biomedical applications. A portion of the wellbeing applications for sensor systems is the arrangement of interfaces for the impaired; coordinated patient checking; diagnostics; sedate organization in medical clinics; observing the developments and inward procedures of creepy crawlies or other little creatures; tele check of human physiological information; and following and checking specialists and patients inside an emergency clinic.

3.3 Vehicle Parking

WSNs are utilized in applications, for example, a vehicle leaving with the end goal of successful utilization of existing leaving openings as opposed to making new costly establishments coupling with modest sensor hubs that can follow the vehicles adequately. Keen stopping the executive's framework (SPARK) given WSN has been introduced in [4]. Stopping reservation instrument, remote stopping observing, and robotized direction are the highlights given by the framework.

3.4 Environmental Applications

Some ecological uses of WSNs incorporate following the developments of winged creatures, little creatures, and bugs; observing natural conditions that influence yields and animals; water system; full scale instruments for enormous scale Earth checking and planetary investigation; concoction/organic discovery; organic, Earth, and ecological checking in marine, soil, and climatic settings; timberland fire location; meteorological or geophysical research; flood identification; bio intricacy mapping of the earth; and contamination considers.

3.4.1 Volcano Monitoring

WSNs are utilized in those situations, where human access is absurd. Well of lava checking is a model, where sensors systems can be sent close dynamic volcanoes to screen their exercises and give the information. During 2004–2005, two volcanoes in Ecuador utilized the idea of WSN uses of the well of lava observing [5]. In 2004, Volcano finding framework had three sensor hubs, which were outfitted with receivers, which was utilized in focal Ecuador. While In 2005, Volcano checking structure had 16 TMote Sky hubs, which were furnished with seismic and acoustic sensors. Those were being used for 19 days, to screen the exercises of a functioning well of lava, in northern Ecuador. To improve the correspondence, extend a whole deal correspondence hub was utilized to transmit the information to a focal controller that secured a 3-km exhibit.

A workstation was furnished with a directional radio wire and gathered the data to deal with the system remotely. The primary objective of the application was to collect seismic data dependent on quakes that happen close to the volcanoes.

3.4.2 Early Flood Detection

WSNs are utilized for early flood locations in creating nations [6]. The fundamental point of this framework is to constant checking of riverbeds. This kind of structure has been created at MIT and tried in Honduras, where floods are as often as possible influencing urban life. A vast region is to be secured with sensors for checking the wave. Two-level system engineering is utilized in Fig. 3. Three distinct sensors are being used in the lower level of the system for estimating precipitation, air temperature, and water stream information. These sorts of information are required for the expectation model. The subsequent level is calculation hubs, where Data gathering and data preparing are performed, which educate to the third level, for example, control focuses. There are four unique sorts of hubs or nodes that are utilized in the framework. Every hub incorporates a microcontroller and handsets that have to possess capacities.

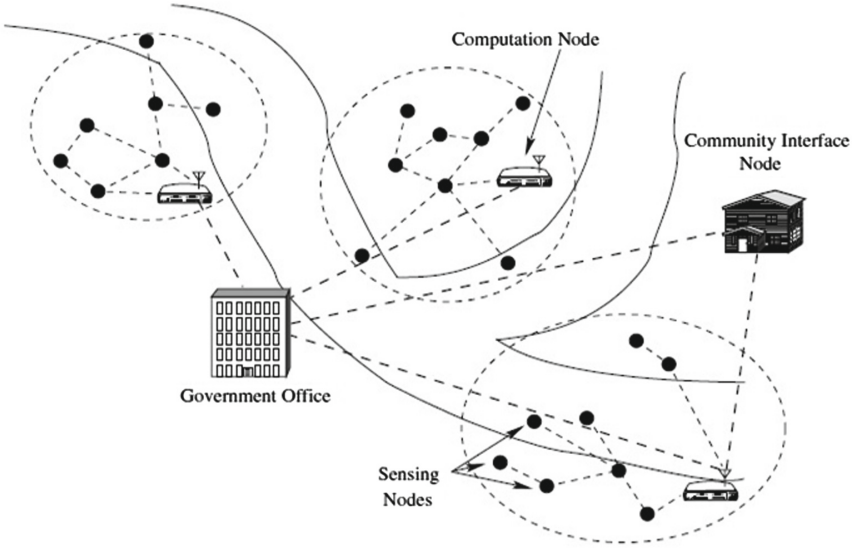


Fig. 3. Sensor network architecture for flood detection

3.4.3 Forest Fire Detection

Sensor nodes are inconstant, thick that are sent in a forest. Sensor nodes can communicate the precise cause of the flame to the clients before they spread wild. Generally, sensor hubs are furnished with optical frameworks. Additionally, they are equipped with the power to explore the strategies, for example, sun-based cells. The nodes will connect to perform circulate detecting and beat numerous obstructions [7] (Fig. 4).

Fig. 4. Forest fire detection

4 Data Mining in Wireless Sensor Networks

Data mining is cited as extracting learning from a considerable measure of information. It is a wide discipline and can be connected to any area of information. Information mining in remote sensor systems is the way toward extricating models and examples from a constant information stream. When the information is prepared, the information is feed to the information mining stage. Information mining assignment utilizes the savvy learning techniques which incorporate design revelation, grouping, characterization, expectation, and estimating. Information mining calculation rapidly processes the fast arriving information. The traditional information mining handles the static information and utilizes the multi-check mining calculation to dissect the static informational collections. That is the reason Conventional information mining strategies are not appropriate for gigantic information, disseminated information produced by the Wireless sensor systems. [8]. There is a contrast between customary information mining and Wireless sensor systems information mining process (Table 1).

Table 1. Difference between traditional and WSN's data mining processing.

	Traditional data mining	WSNs data mining
Processing architecture	Centralized	Distributed
Data type	Static	Dynamic
Memory usage	Unlimited	Limited
Processing time	Unlimited	Limited
Computational power	High	Low
Energy	No constraints	Limited
Data flow	Static	Continuous
Response time	Non-real time	Real-time
Speed	Low	High

4.1 Challenges

There are different difficulties to deal with the sensor information in conventional information mining methods:

a. **Resource Constraint:** The fundamental test is to limit the asset utilization of Wireless sensor systems.
b. **Rapid and Large Data Arrival:** In the WSN area, information arrives quickly in a huge sum, so there is a challenge in the information mining method as to how to deal with the constant fast, massive measure of information.
c. **Data Transformation:** The yield of extricated information of WSN is a model and example which are moved to the base stations. The test is to speak to information over the system for transmission productively.
d. **Online Mining:** WSNs information are in the conveyed way; the vast majority of the information mining strategies utilized the disconnected mining to break down the information that isn't adequate to deal with the appropriated information. Accordingly, there is a test on how to dissect appropriated information on the web.
e. **Dynamic Topology:** Wireless sensor systems are conveyed in the heterogenic, dynamic, unsure way, and the hubs move over the various areas whenever. Such a condition prompts the unpredictability of planning fitting digging methods for WSNs.

4.2 Classification Scheme of Data Mining Techniques for WSNs

The primary degree of characterization plan of information digging strategy for Wireless sensor systems are incessant example mining, successive example mining, bunching, and order. To discover the relationship between the WSN's information, utilize the Apriori and Frequent Pattern (FP) development-based calculations. The above calculations are helpful for the constant example mining and successive example mining system. Group based mining strategy utilizes the K-mean, various leveled, relationship-based bunching calculations, while order based mining procedure utilizes choice tree, rule-based, closest neighbor, and bolster vector machine strategies. These calculations are unique and use in various pieces of WSNs applications.

The Second degree of grouping plan of information digging strategy for Wireless sensor systems depend on the brought together or disseminated information preparing. Dispersed preparing utilizes the single-pass calculation to finish the information mining procedure. The principle point of the conveyed methodology is to constrain the back rubs and correspondence vitality of the sensor hub during the moving of information to the local server. It likewise improves the WSNs lifetime. Though brought together, preparing information is gathered from the whole arrange and put away on the focal server for examination. This methodology produces gigantic information that makes the bottleneck condition. These two methodologies are, for the most part, utilized in WSNs application.

The Third degree of characterization plan is relying upon the exhibition issue and application issues. The sensor nodes are generally asset compelled like vitality, memory, transfer speed, assets. There is a need for such kind of calculation that augments the presentation of the WSNs. Then again, WSNs application requires information exactness, precision, adaptation to internal failure, occasion expectation, versatility, heartiness. The grouping plan of information digging systems for WSNs is appeared as in Fig. 5.

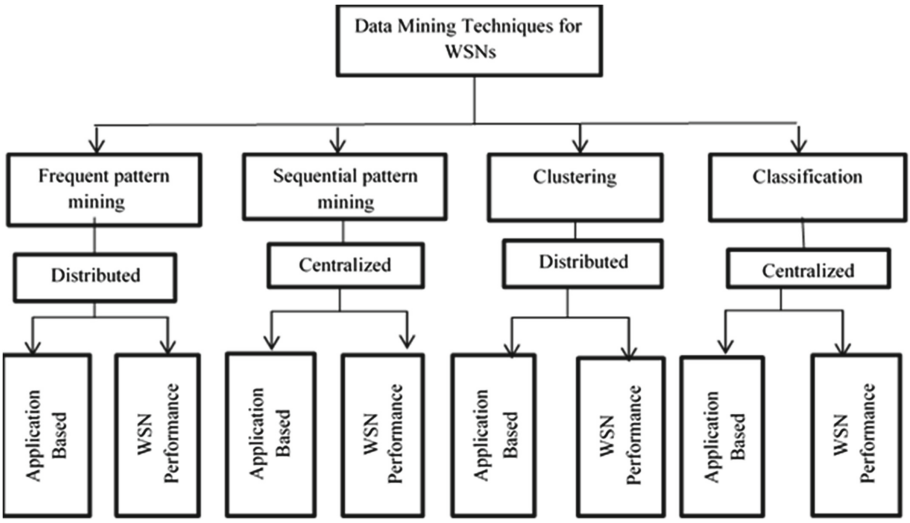


Fig. 5. Classification scheme of data mining techniques for WSNs.

5 Data Fusion

Data fusion is a significant idea in both enormous information and WSNs. In the huge information setting, the combination is accomplished at the computational stage while in the WSNs setting, the combination is performed inside the system (for example, in-organize process). As one of the sources of the enormous data, it is desirable to achieve this in-arrange mixture of data, thus unifying data depiction and avoiding data blasting.

This way, this will prompt sparing the restricted assets and abilities of the WSNs. Briefly, we can characterize information combination as a mix of numerous sources to acquire improved data; in this unique circumstance, improved data implies more affordable, higher quality, or progressively pertinent data.

Data fusion techniques systems have been widely utilized on multi-sensor situations with the point of intertwining and conglomerating information from various sensors; be that as it may, these procedures can likewise be connected to different spaces, for example, content preparing. The objective of utilizing information combination in multi-sensor situations is to acquire a lower location blunder likelihood and higher dependability by using information from different conveyed sources. The available information combination methods can be ordered into three nonexclusive classifications: (i) information affiliation, (ii) state estimation, and (iii) choice combination. In light of the huge number of distributed papers on information combination, this paper does not plan to give a comprehensive survey of the majority of the examinations; instead, the goal is to feature the fundamental advances that are engaged with the information combination system and to audit the most widely recognized methods for each step. WSN is regularly made out of an enormous number of sensor nodes representing another adaptability challenge brought about by potential crashes and transmissions of excess information. As to vitality limitations, correspondence ought to be diminished to build the lifetime of the sensor nodes. Subsequently, information combination is additionally essential to lessen the general correspondence load in the system by evading the transmission of repetitive messages. Likewise, any assignment in the system that handles flag or needs to cause surmising to can conceivably utilize information combination. Information combination ought to be viewed as an essential advance in structuring a remote sensor arrange. The reason is that information combination can be used to extend the system lifetime and is typically used to satisfy the application destinations, for example, occasion identification, target following, and essential leadership.

Consequently, a thoughtless information combination may bring about the misuse of assets and deluding appraisals. In this manner, we should know about potential confinements of information combination to abstain from ruining circumstances. On account of the asset justification needs of WSN, information handling is regularly executed as in system calculations.

Consequently, information combination ought to be appropriately performed to expand the system's lifetime. Information combination has built up itself as an autonomous research territory in the course of the most recent decades, however a general formal hypothetical structure to portray information combination frameworks. Information combination in WSNs can be grouped [9] as indicated by either the connection of the information's sources or the degree of reflection. That appears in Fig. 6.

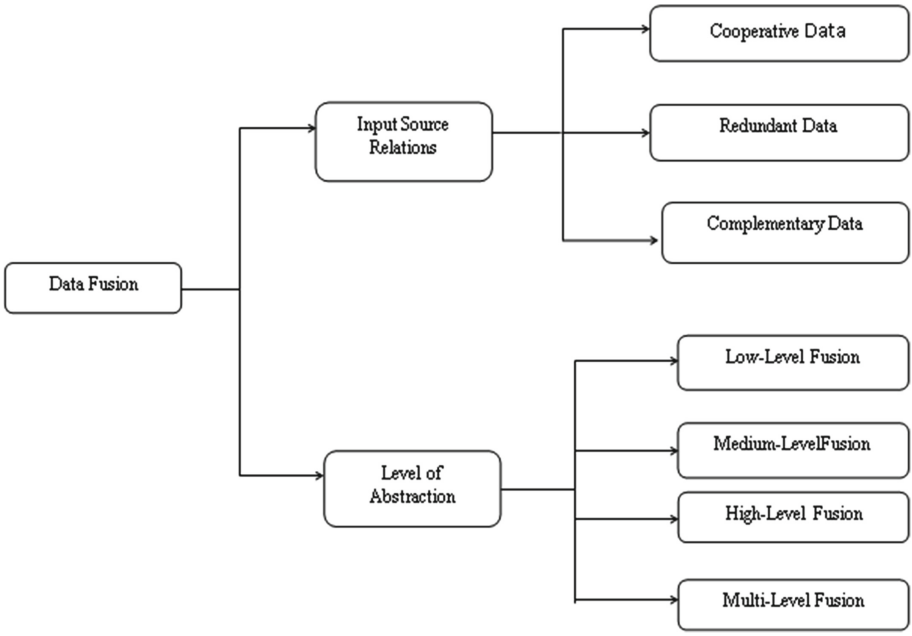


Fig. 6. Data fusion classification in WSNs

5.1 Fusion Based on Input Sources Relation

This can be defined into three groups depending on the association of the sources of information: Complementary, Redundant, and Cooperative data fusion. The correlative combination is performed when source hubs get various information that should be melded to finish the scene. For instance, a mechanical vessel is utilized to screen the dangerous cyanobacteria in a lake. For the last combination method, the vessel collects data from various focuses on a subpart of the lake to characterize the toxic performance rate. When two source nodes share a comparable piece of data in the repetitive combination strategy, the data is first placed and integrated into a superb single piece of data. Thus, this methodology gives trustiness and unwavering quality of detected information. The agreeable information mix is the third subclass of the information mix based on the association of the data sources. This class is used to generate another piece of data when free sources are incorporated with their data. This type of mixture of data is suitable for the use of Body Sensor Networks (BSN).

5.2 Fusion Based on the Abstraction Level

This mix of information can be characterized into four groups: low-level combination, medium-level combination, high-level combination, and a mixture of multilevel. The low-level mix is a mixture of some raw data into another, accurate information. For instance, the flame calamity occasion can be distinguished by processing the information combination gathered from humidity sensors and temperature sensors. Another

two types of data based on deliberation are a mixture of medium-level and high-level. A staggering combination framework that joins the medium-level and the abnormal state combinations in the mechanization of hindrance detection application.

5.3 Fusion of Information, a Fusion of Sensors, and Fusion of Data

The sensor-fusion is typically used to indicate the combination of information given by the sensors. Regardless of the hypothetical issues about the contrast among data and information, the terms data combination and information combination are generally acknowledged as by and large terms. The term information total term has turned out to be prevalent in the remote sensor arrange network as an equivalent word for data combination. Numerous meanings of information combinations have been given over the years; the more significant part of them was found in military and remote detecting fields. The multisensory combination is another articulation utilized in PC vision and modern robotization. Multi-sensor combination is a broader term than a multi-sensor combination. It clarifies how integrated information or data is being used by the entire framework to associate with nature. Be that as it may, this proposes just tactile information is utilized in the combination and coordination forms. Information accumulation contains the gathering of crude information from inescapable information sources, the programmable piece of the coarse information into less voluminous refined information, and the convenient conveyance of the processed data to information purchasers. The collection is the capacity to abridge information to diminish the measure of information (Fig. 7).

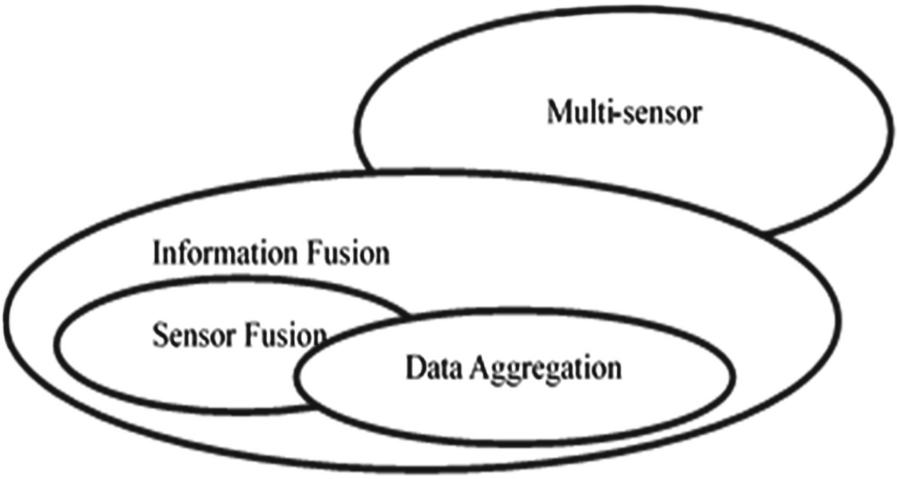


Fig. 7. Relationship between multi-sensor, information fusion, sensor fusion, data aggregation

6 Forest Fire Detection System Using Data Fusion and Data Mining Techniques

6.1 Background on Forest Fire

Forests are the defenders of earth's environmental equalization. Tragically, the most well-known speculation in forests is a forest woods fire. Forest flames are as old as the forest themselves. They represent a danger not exclusively to the woods riches yet additionally to the whole system to fauna and greenery, genuinely aggravating the biodiversity and the nature and condition of a locale. During summer, when there is no downpour for a considerable length of time, the timberlands become covered with dry senescent leaves and twinges, which could blast into blazes touched off by the smallest flash. The backwoods fire is usually possibly seen when it has spread over a considerable territory, making its control and stoppage challenging and even unthinkable now and again. The outcome is pulverizing misfortune and unsalvageable harm to the earth and climate (30% of carbon dioxide (CO_2) in the environment originates from backwoods fires), with hopeless damage to nature (enormous measures of smoke and carbon dioxide (CO_2) in the air). Among other awful results of a forest, flames are long haul sad impacts, for example, impacts on nearby climate designs, a dangerous atmospheric deviation, and elimination of uncommon types of the greenery.

6.1.1 Causes of Forest Fire

Forest flames are brought about by Natural causes just as Manmade causes.

a. Natural causes-Many forest flames begin from normal causes such as lightning, which set trees ablaze. In any case, rainstorm quenches such fires without causing much harm. High atmospheric temperatures and dryness (low dampness) offer an ideal situation for a flame to begin.
b. Manmade Causes-Fire is caused when a wellspring of fire like an exposed flame, cigarette or bidi, electric flash, or any wellspring of start comes into contact with flammable material.

6.1.2 Types of Forest Fire

There are two kinds of forest fire namely surface fire and crown fire.

a. **Surface Fire -** A forest fire may consume essentially as a surface flame, spreading along the ground as the surface litter (senescent leaves and twigs and dry grasses and so forth.) on the forest floor and is immersed by the spreading flares.
b. **Crown Fire -** The other kinds of forest fire is a crown fire in which the crown of trees and bushes consume, regularly continued by a surface flame. A crown fire is especially exceptionally hazardous in coniferous woodland because resinous material radiated consuming logs consume angrily. On slope inclines, if the flame begins downhill, it spreads up quick as warmed air neighboring a slant will, in general, stream up the slant spreading flares alongside it. If the fire starts tough, there is less probability of it spreading downwards (Fig. 8).

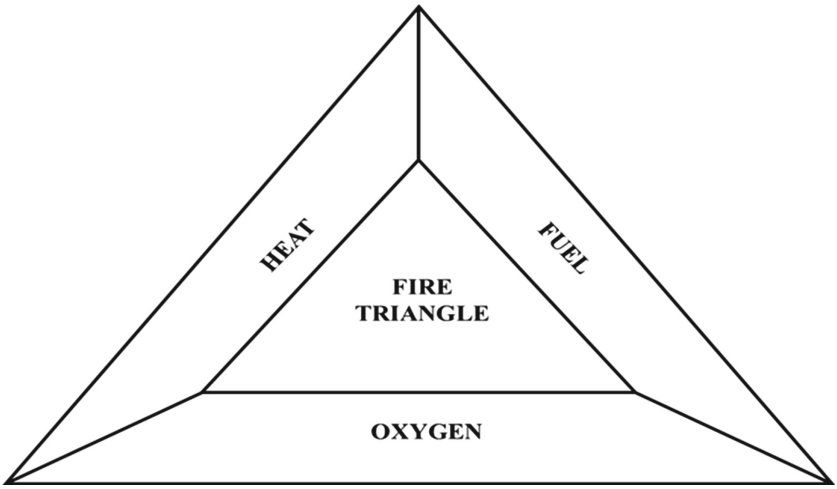


Fig. 8. Fire factors triangle

6.2 Forest Fire Monitoring System Based on Data Mining and Data Fusion Technique

Forest Fire Monitoring System dependent on information mining and data fusion procedure is represented by the Fig. 9 that consists of the five modules: Data Fusion, Database, Data Mining, Knowledge Base, Application Services.: Data Fusion, Database, Data Mining, Knowledge Base, and Application Services. The Wireless Sensor Network hubs can be characterized into two kinds of hubs source hubs and sink hubs in the observing region of the timberland fire checking framework [12].

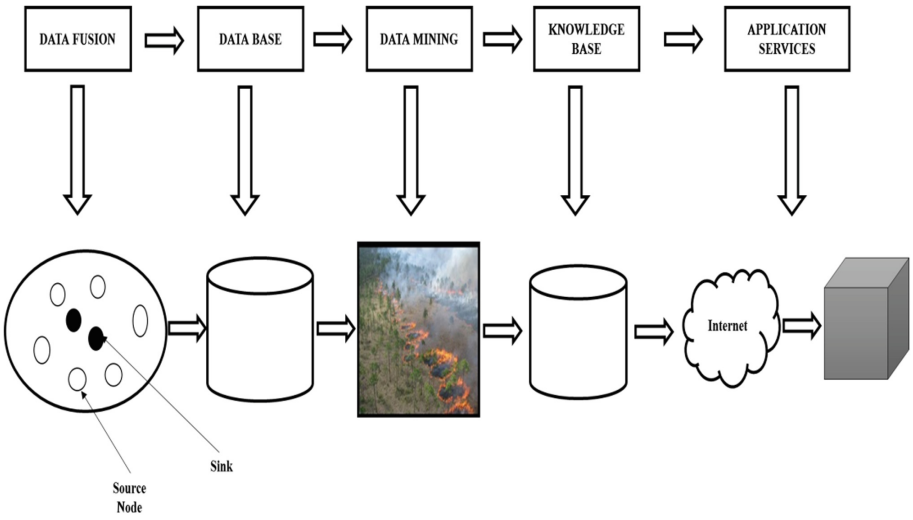


Fig. 9. Forest fire monitoring system architecture based on the technique of data mining and data fusion.

In this type of monitoring system generally uses the Heterogeneous wireless sensor networks (HWSN) equipped with several sensing nodes that provide different types of services. These nodes are of two types: high end and low end. The mixed deployments of these two nodes give a much better performance than the other types of nodes. Heterogeneous nodes in the sensor network decrease response time and improve battery lifetime. [10]. In data fusion, there are three kinds of Wireless Sensor Networks: complementary, collaborative, and competitive. Competitive sensor fusion relates to the sensors that can separately supply information and provide the system with fault tolerance and robustness. Data fusion for heterogeneous wireless sensor networks is explained as-

$$\text{Suppose } \{X_i\} \text{ is a random variable and } X_i \sim f(x_i, \mu_o, \sigma) \text{ where } i\varepsilon\{1, t-1]$$

$$\mu_o = \text{Initial value of mean,}$$

$$t = \text{ time(i.e., after t times signal raised)}$$

The fire scenario in the forest is regarded to test the efficiency of the suggested algorithm. The fire detection model data fusion method is shown in Fig. 10. The suggested model for fire detection has the level of data fusion and the level of fusion information. Resource information in the sensing sector is gathered from the sensors in the first stage. The fire is identified in the second stage by calculating the probabilities of data fusion acquired by the probabilities produced. Two sensors (temperature and moisture sensors) are incorporated together in the suggested fire detection method, given that all $X_i(i \geq 1)$ measurements are not dependent on normal random variables [13].

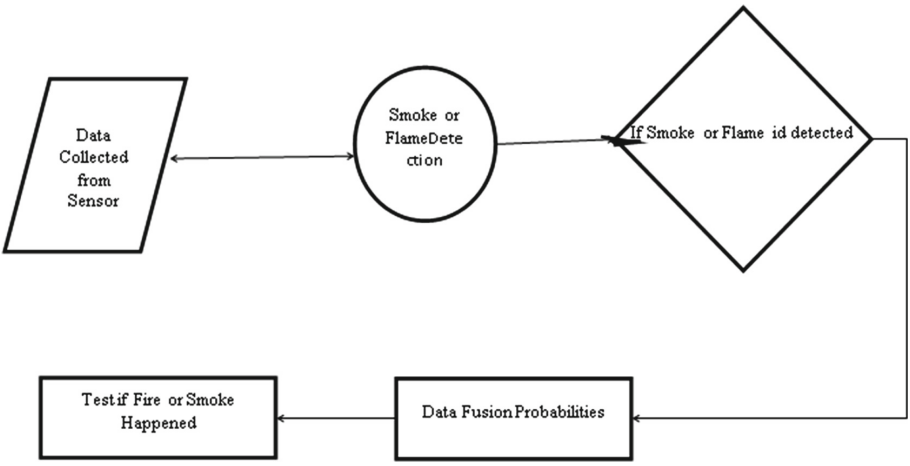


Fig. 10. Data fusion process for fire detection model

The condition satisfied with the temperature sensors

$$f(x_i, \mu_o, \sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\left[\frac{xi-\mu o}{\sigma}\right]^2} \quad (1)$$

The hypothesis should be satisfied for the fire detection

$$f(x_f, \mu_f, \sigma_f) = \frac{1}{\sigma f\sqrt{2\pi}} e^{-\left[\frac{xf-\mu_f}{\sigma_f}\right]^2} \quad (2)$$

if $\mu_f > \mu_0$ then condition is satisfied, μ_f = mean value of fire in trees.
Remaining trees after detection of fire is $Yi = X_i - \mu_0$
Difference mean $\mu_d = \mu_f - \mu_0$.
Hence, the absence of fire is shown as $Yi \sim N(0, \sigma^2)$.
that satisfies the condition $Yi \sim N(\mu_d, \sigma^2)$.

Test Statistics after time t defined as,

$$S_t = \sum_{i=1}^{k} \frac{y - \mu_d}{\sigma/\sqrt{k}}$$

In the data fusion strategy for heterogeneous wireless sensor networks, the genetic algorithm is suggested, which is used to classify the population to optimize the issue where each node is represented by their genotypes. After each generation, new artificial creatures are obtained. The suggested approach to a genetic algorithm based on data fusion is provided as follows.

Algorithm 1: Genetic algorithm for HWSNs
Input: E_i, L_f, L_c, C_{SP}
Output: N_{sp}

1. Choose the initial population of individuals E_i.
2. E_f is calculated through the method of effectiveness.
3. If $E_f > E_i$; then
4. $Best_{sp} = Last_{sp;}$
5. End If
6. Evaluate the fitness of each individual in that population $\Delta E_f = 1000^* (Last_{ef}/E_f\text{-}1)$;
7. Repeat on this generation until termination (time limit, sufficient fitness achieved, etc.)
8. Select the best-fit individuals for reproduction
9. Breed new individuals through crossover, Crossover ();
10. Mutation operations, Mutate ();
11. Evaluate the individual fitness of new individuals
12. Replace least-fit population with new individuals, i.e. $New_{sp} = Best_{sp}$;

Alert state is defined as follows

Case1: If the sensors of humidity are more than the sensors of temperature, we test the situation with statistics. S_t. Therefore, the equation satisfies

$$S_t < TA(f) \tag{3}$$

Where $T_a(f)$ indicates the alert state limit.

Case 2: If the sensors of humidity are less than the sensor of temperature, we will check the following condition.

$$(St < T_H(f)) \;\&\&\; (S_t < T_A(f)) \tag{4}$$

Where $T_H(f)$ indicates the alert status limit.

6.3 Multi-sensor Data Fusion

A multi-sensor data fusion strategy based on Bayesian approaches and methods for optimizing ant colony for distant sensor scheme. Each node is equipped with many sensors (i.e., temperature and humidity) in this approach. These sensors give extra data about ecological conditions. This methodology depends on the various leveled handling, and it is considered for experimentation. At first, the information is gathered by the sensors that are put in the detecting fields, and after that, the information combination probabilities are registered on the detected information. In this entire procedure,

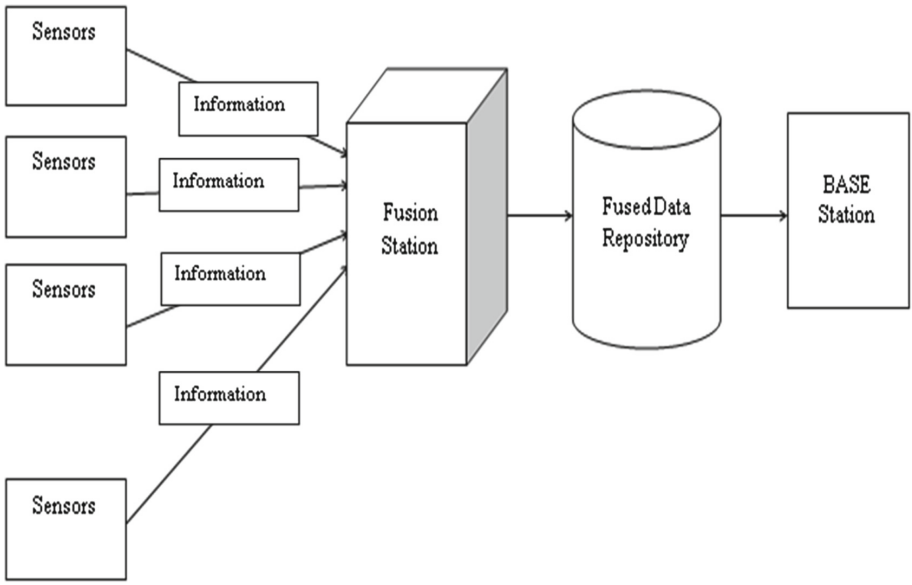


Fig. 11. The architecture of multi-sensor data fusion

the gathered temperature tends to moistness information is handled by multi-sensor information combination systems that aides in diminishing the vitality utilization just as correspondence costs by combining the repetitive information. The various information combination procedures improve the authenticity quality and exactness of the detected data and spare efficiency and power [15] (Fig. 11).

6.3.1 The Framework of Multi-sensor Wireless Network Using Data Fusion Technique

The framework is divided into three stages. The first stage is the choice of cluster heads, which is used for the formation of clusters. The second stage is the data fusion Bayesian method. The third stage is used for data routing from source to destination.

Phase I: Cluster head selection and cluster formation

Based on the specified circumstances, the sensors are grouped to create a cluster and one node functions as the head of the cluster. The clustering algorithm divides the network into smaller cluster fields. The following algorithm describes the selection of the cluster head and the formation of the cluster.

```
Cluster Formation (int x)
{
Int a; //Area of Sensor Network
Int cn; //No of Cluster
Int ac; //Area of Cluster
Int n; //No of Nodes in the total area of sensor Network
Int sd_m; //Minimum Separation Distance
Int d_c; //Number of desired cluster heads,
Int n_a; //Set of alive nodes,
Read (a);
Read (c_n);
a_c = a/c_n; //Area of each Clusters
for (i = 1 to n_t)
{
          Setup the energy of each node, E (n);
          Setup the location of each node, L (n);
}
          μ = Σ E (n)/n_a
for (j = 1 to x) //where x is number of repetitions to forming a cluster
{
          C_H = Highest Energy Node of the clusters
          Eligible = { n| E (n) ≥ μ }
          Assert (|Eligible| ≥ d_c)
          While (|C_H| < d_c)
          If ∃n: n∈ Eligible && (∀ m ∈C_H, dist (m, n)) ≥ sd_m
          add (m, C_H)
          remove (n, eligible)
          else n ∈ eligible
```

```
            add (n, C_H)
            remove (m, eligible)
            m sends a acknowledge message to C_H
            C_H and all m are synchronized for further communications
  }
}
```

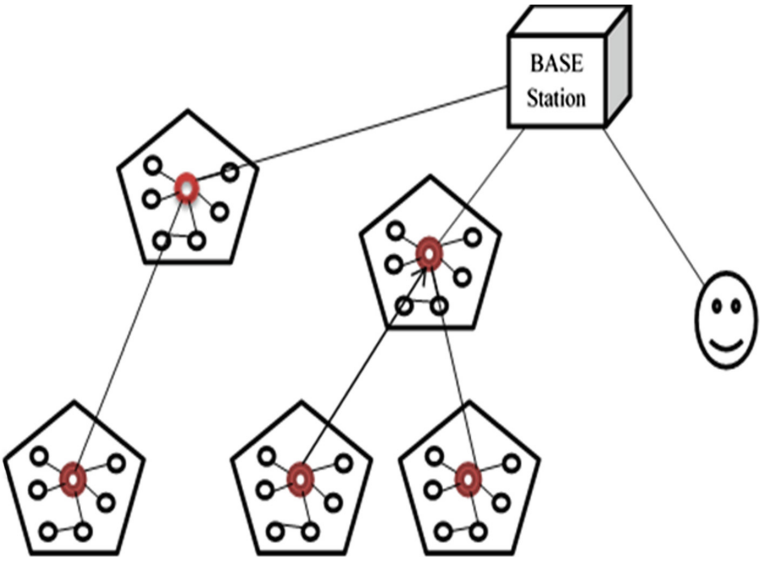


Fig. 12. Data fusion framework for event detection

For example, to calculate the area of the cluster by taking the following values:

Area of Network (a) = 1000*1000 m^2
Number of Cluster Head (C_H) c_n = 10
Area of each cluster $a_c = a/c_n$ = 1000*1000/10 = 1000*100 m^2

After Clustering has been done, then data is sent from node to cluster head, then cluster head again sends it to the base station. When the data transmission is complete, clustering formation is constantly implemented.

Analysis of the algorithm

Two nested loops have been evaluated about time and space complexity. Suppose the number of nodes is n and the number of rounds is x, then this algorithm's time complexity is O(xn). All other statements are executed linearly except the loop and will only contribute uninterrupted time, which can be ignored asymptotically.

$$\text{So that } T(n) = O(xn)$$

The complexity of space is the space needed to store the total number of nodes in the network, and it is n. Therefore, the space complexity will be O (n^2)

Phase II: Data fusion approach
Multi-Sensor data fusion aggregates the inputs from various sensors that make better use of energy. This sensor fusion can be implemented in different ways. We consider the sensor's mean and variance. We have the probability p of the node x then calculate the mean (μ) and variance V(x) by using the following equations:

$$\mu = \Sigma xp, \tag{5}$$

$$V(x) = \Sigma x^2 p - \mu^2 \tag{6}$$

There are a single base station and multiple sensors that receive the data from different sources; they are connected wirelessly. Thus, they interact to reach the base station through multi-hop communication. The architecture of the sensor fusion network was regarded to be of a competitive sort, which, as shown in Fig. 12, is called hierarchical processing. Each sensor node has the same characteristics in distinct sizes. In this form of architecture, the cluster head has a dual function that operates simultaneously as a fusion center and cluster head; it gathers sensed information from various sensor nodes and fuses all the collected data by choice criterion technique and then transfers it to the base station via the shortest routing system based on the ant colony algorithm. Therefore, this technique decreases the computational workload, traffic load, bandwidth and improves the network's lifetime by saving the energy of the sensor nodes.

The process of fusion by using Bayesian methods
The process of fusion uses the probability for each observation and uses the Bayesian method to integrate them. Each sensor senses the information and transmits it to the corresponding cluster head. The cluster head generally does not send information to another sensor instantly for more sensed information that provides better aggregation and increases performance and energy savings. In the process of fusion, the cluster head's primary responsibility is to compare the new data with the old data set, using some prior probabilities.

Suppose there are three sensors: temperature, humidity, precipitation, sensing, and sending information to the head of the cluster; then, the fusion method is based on the present measurement and the prior measurement.

Sensor 1:

Snd1 = new data set,
Sod1 = old data set,
Scd1 = current sensed data.

Sensor 2:

Snd2 = new data set,
Sod2 = old data set,
Scd2 = current sensed data.

Sensor 3:

Snd3 = new data set,
Sod3 = old data set,
Scd3 = current sensed data.

At the fusion mode, the probability of the latest data x (e.g., temperature/humidity) can be computed by using the Bayes rules are given as

$$P\left(\frac{x}{\text{Snd1, Snd2, Snd3}}\right) = P\left(\frac{x}{\text{Scd1, Scd2, Scd3, Sod1, Sod2, Sod3}}\right)$$

$$P\left(\frac{x}{\text{Snd1, Snd2, Snd3}}\right) = P\left(\frac{P(\text{Scd1, Scd2, Scd3/x, Sod1, Sod2, Sod3}) * P(x/\text{Sod1, Sod2, Sod3})}{\text{P(Scd1, Scd2, Scd3/Sod1, Sod2, Sod3)}}\right)$$

Because these sensors are independent so that

$$P\left(\frac{P(\text{Scd1/x, Sod1}) * P(\text{Scd2/x, Sod2}) * P(\text{Scd3/x, Sod3}) * P(\text{x/Sod1, Sod2, Sod3})}{\text{P(Scd1, Scd2, Scd3/Sod1, Sod2, Sod3)}}\right)$$
$$= P\left(\frac{P\left(\frac{\text{x}}{\text{Snd}_1}\right) * P\left(\frac{\text{Scd}_1}{\text{Sod}_1}\right) * P\left(\frac{\text{x}}{\text{Snd}_2}\right) * P\left(\frac{\text{Scd}_2}{\text{Sod}_2}\right) * P\left(\frac{\text{x}}{\text{Snd}_3}\right) * P\left(\frac{\text{Scd}_3}{\text{Sod}_3}\right) * P\left(\frac{\text{x}}{\text{Snd}_1\text{Snd}_2\text{Snd}_3}\right)}{P\left(\frac{\text{x}}{\text{Snd}_1}\right) * P\left(\frac{\text{x}}{\text{Snd}_2}\right) * P\left(\frac{\text{x}}{\text{Snd}_3}\right) * \text{P(Scd1, Scd2, Scd3/Snd1Snd2Snd3)}}\right)$$

On the fusion node

$\text{S} = \left(\frac{P\left(\frac{\text{x}}{\text{Snd}_1}\right) * P\left(\frac{\text{x}}{\text{Snd}_2}\right) * P\left(\frac{\text{x}}{\text{Snd}_3}\right) * P\left(\frac{\text{x}}{\text{Sod}_1,\text{Sod}_2,\text{Sod}_3}\right)}{P\left(\frac{\text{x}}{\text{Sod}_1}\right) * P\left(\frac{\text{x}}{\text{Sod}_2}\right) * P\left(\frac{\text{x}}{\text{Sod}_3}\right)}\right)$ is the required solution for fusion at the fusion station.

That solution is sent to the base station that is in a small size.

Phase III: Approach for data dissemination

Swarm intelligence is the investigation of aggregate conduct of social orders of organic species, for example, herds of feathered creatures, reefs of fish, and provinces of ants. One of the incredible concepts of an ant colony optimization (ACO) is a probabilistic method that is useful in problems to find better ways to nourish the charts. Recreated ants find ideal arrangements by traveling through a parameter space that speaks to every single imaginable arrangement. The reproduced ants record their positions and the nature of their answers like the characteristic insect's pheromones, which coordinated to one another to the assets.

We used forward ants and reverse ants to discover classes from source to BS to track the intertwined data from source to BS. In this technique, a node with the most noteworthy vitality and most astounding pheromone levels are utilized for choosing the likelihood of the following next nodes to be selected, which will have the insignificant separation and most significant node vitality to guarantee a higher network. The ant colony optimization technique had been used by the implementation of the intelligent sensor networks, which can easily identify the tree like burn condition.

7 Conclusion

We presented the design of an intelligent wireless sensor network to detect forest fires early. Our design is based on the techniques of data mining and data fusion, backed by decades of research in forestry. It is possible to detect the presence of smoke directly and indirectly by detecting flames. It outlines the methods used to detect smoke (or fire) and describes the basic steps in each technique. In most techniques mentioned above, ant colony optimization is use for creation of the multisensory base stations Our algorithm is straightforward to implement and requires no specific node deployment schemes. Thus, nodes can be deployed uniformly. It greatly improves the deployment of nodes in real life and can therefore, achieve higher accuracy detection in important areas such as neighborhoods near residential or commercial.

Backwoods flames are an extraordinary primary issue in numerous nations; this way, an unnatural weather change will make it increasingly genuine. It is acknowledged all around that counteractive action of timberland fires from occurring, which leads to prerequisites of new strategies and mechanical assembly that empowers a proficient system. Therefore, over the most recent two decades, significant exertion was made to create programmed detection tools that could help the Fire Management Systems (FMS). The three boss patterns utilized for the location of timberland flames are the use of satellite information, infrared/smoke scanners and nearby sensors (e.g. meteorological). In this section, we have displayed an intelligent framework for powerful woodland fire identification utilizing heterogeneous information. The proposed framework depends on information mining and information combination method through insightful remote sensor networks. In appear differently about the traditional strategies for flame counteractive action, remote sensor systems having more prominent advantages, and there are wide desires for woods fire observing application. Primarily, the scheme can be placed in the area of high-risk land. In WSN's physical scheme, the hubs are of two kinds: source hub, which collects data from nature and sinks hubs, assembles data from source hubs and also provides the base station with this data. The source hubs (sensor hubs) can conduct unique work that empowers it as a self-designing scheme, providing repetition and ensuring complete geographical integration within a fascinating area. There are various research issues arises during the creation and implementation of the of wireless intelligent sensor networks like sensor node design, system design, transducer design and protocol selection for multi sensor nodes. The future challenge for the detection of fire forest using wireless sensor network is design of the sensor nodes and their maintenance in the dense forests. It also a great challenge to the development of huge number of homogenous intelligent sensor node which is very powerful and cost-effective devices.

References

1. Zear, A., Singh, P.K., Singh, Y.: Intelligent transport system: a progressive review. Indian J. Sci. Technol. **9**(32), 1–8 (2016). https://doi.org/10.17485/ijst/2016/v9i32/100713. ISSN 0974-5645
2. Agarwal, D., Gupta, A., Singh, P.K.: A systematic review on artificial bee colony optimization technique. Int. J. Control Theory Appl. **9**(11), 5487–5500 (2016). ISSN 0974-5572
3. Kumar, H., Singh, P.K.: Analyzing data aggregation in wireless sensor network. In: Proceedings of the 11th INDIACoM-2017, 1–3 March 2017, pp. 4024–4029. Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi (2017). IEEE Conference ID: 40353
4. Swati, A.J., Priyanka, R.: Wireless sensor network (WSN): architectural design issues and challenges. Int. J. Comput. Sci. Eng. (IJCSE) **02**(09), 3089–3094 (2010)
5. Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., Welsh, M.: Deploying a wireless sensor network on an active volcano. IEEE Internet Comput. **10**(2), 18–25 (2006)
6. Basha, E.A., Ravela, S., Rus, D.: Model-based monitoring for early warning flood detection. In: Proceedings of ACM SenSys 2008, Raleigh, NC, USA, pp. 295–308, November 2008
7. Zhang, Y., Zhou, Z., Zhao, D., Barhamgi, M., Rahman, T.: Graph-based mechanism for scheduling mobile sensors in time-sensitive WSNs applications. IEEE Access **5**, 1559–1569 (2017)
8. Mahmood, A., Shi, K., Khatoon, S., Xiao, M.: Data mining techniques for wireless sensor networks: a survey. Int. J. Distrib. Sens. Netw. **9**(7), 1–24 (2013). Article ID 406316
9. Abdelgawad, A., Bayoumi, M.: Data fusion in WSN. In: Resource-Aware Data Fusion Algorithms for Wireless Sensor Networks, pp. 17–35. Springer (2012)
10. Brooks, R.R., Iyengar, S.S.: Multi-Sensor Fusion: Fundamentals and Applications with Software. Prentice-Hall Inc., Upper Saddle River (1998)
11. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies, FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
12. Tian, H., Li, W., Ogunbona, P.O., Wang, L.: Detection and separation of smoke from single image frame. 1057-7149 ©2017. IEEE (2017)
13. Surya, T.S., Suchithra, M.S.: Survey on different smoke detection techniques using image processing. IJRCCT **3**(11), 16–19 (2014)
14. Sadaphal, V.P., Jain, B.N.: The role of colinearity of sensors in target localization using distance measurements. In: The ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, ACM MsWim 2009 (2009)
15. Jagyasi, B.G., Dey, B.K., Merchant, S.N., Desai, U.B.: An efficient multibit aggregation scheme for multihop wireless sensor networks. EURASIP J. Wirel. Commun. Network. (EJWCN) **2008**, 11 (2008). https://doi.org/10.1155/2008/649581. Article ID 649581
16. Sadaphal, V.P., Jain, B.N.: Sensor selection heuristic for target tracking sensor network. In: Proceedings of International Conference on High Performance Computing, HiPC 2005. Lecture Notes in Computer Science, vol. 3769, pp. 190–200. Springer (2005)

Internet of Things for Enhanced Living Environments, Health and Well-Being: Technologies, Architectures and Systems

Gonçalo Marques[1,2(✉)], Jagriti Saini[3], Ivan Miguel Pires[2,4,5], Nuno Miranda[1], and Rui Pitarma[1]

[1] Polytechnic Institute of Guarda, Guarda, Portugal
goncalosantosmarques@gmail.com, nuno-miranda@sapo.pt, rpitarma@ipg.pt
[2] Instituto de Telecomunicações, Universidade da Beira Interior, Covilhã, Portugal
impires@it.ubi.pt
[3] National Institute of Technical Teacher's Training and Research, Chandigarh, Chandigarh, India
jagritisl327@gmail.com
[4] Altran Portugal, Lisbon, Portugal
[5] Polytechnic Institute of Viseu, Viseu, Portugal

Abstract. Internet of Things (IoT) stands as a concept where things are linked to the Internet, incorporate data collection capabilities and cooperation features between them. Ambient Assisted Living (AAL) is closely related to the necessity of pervasive healthcare supervision, and his main aim is to contribute to the independence and well-being of older adults using Information and Communication Technologies. At 2050 20% of the world population will be age 60 or older, which will lead to significant consequences for public health such as an increase of diseases, health care costs, shortage of caregivers, and dependency. IoT and AAL architectures enhancements will contribute to the development of personalized healthcare systems that incorporate real-time monitoring features for environmental quality and people's health status for enhanced living environments and well-being. Scientific developments turn possible to create novel and innovative instruments to empower real-time healthcare supervising solutions for decision making in the management of several syndromes. This paper provides a review summary of the main technologies, architectures, and systems based on IoT and AAL for enhanced living environments. The design, social, and ethical challenges for the implementation of efficient and effective systems for enhanced living environments and future directions are also discussed.

Keywords: Ambient Assisted Living · Enhanced living environments · Indoor environment quality · Internet of Things · Smart systems

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 616–631, 2020.
https://doi.org/10.1007/978-3-030-40305-8_29

1 Introduction

AAL is a multi-disciplinary approach to design advanced telehealth and personal healthcare monitoring systems by combining computers, sensors, wireless networks, mobile devices, and software applications on the same platform. AAL works in association with Information and Communication Technologies (ICTs) to provide prevalent healthcare supervision, ensuring complete well-being for the older adults [1]. The new age AAL systems make use of several sensors for measuring position, location, oxygen, blood pressure, temperature, glucose, and weight. These sensors are connected using wireless technologies such as Ethernet, Bluetooth, ZigBee, and Wi-Fi.

Lots of challenges are associated with designing and implementation of reliable AAL systems; the list includes accessibility, usability, ergonomics, human-computer interaction, interaction design, and information architecture related issues [2]. Other than this, few studies also report social and ethical problems for confidentiality, privacy, and full acceptance of AAL devices. At the same time, it is essential to mention that personal care cannot be replaced with technology; AAL systems can be considered as a relevant addition to an independent lifestyle [3].

IoT represents a wireless network of things with abilities to perform data collection over the internet. The objects connected to the IoT network have cooperation and interaction capabilities to achieve a common objective [4–6]. IoT is expected to have a material impact on the human lifestyle while offering several applications in assisted living, domotics, and e-health. These systems are incorporated with advanced software capabilities that offer a novel solution for data and computational abilities [7, 8]. There is a wide range of wireless communication technologies that can be used to establish interconnection among IoT objects; the list includes GSM-Based technologies, Wi-Fi-based technologies, Bluetooth based technologies, and NFC (Near Field Communication) based technologies. A basic example of mobile health solutions for AAL is shown in Fig. 1.

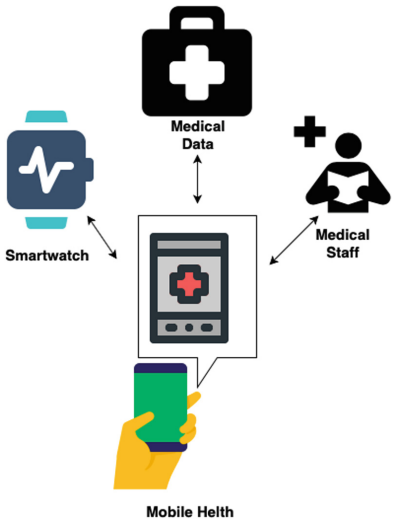


Fig. 1. Basic example of mobile health solutions for AAL.

IoT networks, with their remarkable environment intelligence skills, context-awareness, and pervasive performance, are considered as a suitable solution to develop well-being solutions and hence, show valuable scope for AAL [9]. The latest scientific development made it possible to develop innovative instruments for healthcare supervision and decision making, leading to the secure management of life-threatening syndromes.

At an average, human beings spend almost 90% of their routine time indoors; it is essential to monitor indoor living environments on a real-time basis. These applications are more useful for buildings that are occupied by a large population of new-borns and older people as they spent all their time indoors [10]. The decaying quality of indoor air brings a significant challenge for the health of vulnerable individuals.

Studies reveal that indoor air quality (IAQ) has become a global health problem, having considerable results as compared to other prevalent issues like sexually transmitted diseases and smoking [11]. The Environment Protection Agency (EPA) that is responsible for regulating air quality within the United States also predicted that the level of indoor air pollutants could go 100 times higher than the contaminants present in the outdoor air. With this, air quality has become one of the top five environmental severe health problems on a global scale [12]. It is crucial to work in the direction of IAQ management to provide a considerable solution for inspection, legislation, and development of automatic real-time monitoring systems for better occupational health and enhanced living environments. Such systems are useful not just for public places such as hospitals and institutions; instead, they must be incorporated into private buildings with better construction guidelines. Human beings need to opt for a few necessary behavioral changes, such as using natural ventilation systems and avoiding smoking indoors to enhance IAQ. Children must be guided to maintain a healthy living environment via some educational programs [13]. However, even after increasing cases of poor impact of IAQ on public health, the research community is still lacking behind in the development of new methods to improve IAQ [14].

Numerous researchers around the world are working to find a potential solution for the effective implementation of AAL systems [15]. New-age technologies are providing significant results; however, the most impactful solutions are led from IoT based methods [16, 17]. Few such IoT based projects are discussed in this book chapter, along with some current and future challenges in the field of AAL systems [18].

2 Smart Homes and Wearable Sensors

Advanced methods such as e-textile, assistive robots, smart homes, and wearable gadgets can be integrated using IoT technologies. Many algorithms, like context modeling, activity recognition, anomaly detection, planning, and location identification, are capable enough to turn the concept of AAL into reality [19]. The section below is focused on detailed discussion on smart homes, smart sensors, and wearable sensors.

Smart homes have been a matter of scientific discussion from the past few decades. MIT Media Labs implemented the first-ever project in this direction in the form of Smart Rooms [20]; however, experts these days have developed three different types of

smart homes. The very first type of smart homes is capable enough to detect and recognize the actions of residents living inside to estimate their health conditions. The second category is responsible for storing and retrieving information captured from smart homes in the form of various multi-media collections. The third category is related to surveillance; in this case, the data obtained from the building environment is processed to raise alarms to ensure complete protection to the residents. Few advanced smart home designs are also capable enough to reduce the overall consumption of energy by controlling and monitoring electric devices [21].

With the recent advancements in the field of information technology, it is now possible to design smart homes at low prices, but the biggest challenge in front of researchers is to create an intelligent environment for efficient decision making within the premises. It is expected that the number of smart homes will increase in the future with the use of sensor networks that have enhanced real-time monitoring abilities.

Three potential views are presented by Wilson et al. [22]: a functional view, a socio-technical view, and an instrumental view. Functional views are designed with an idea to manage routine needs via technology. The socio-technical view presents smart homes as a new advancement for the development of digitalization and electrification in everyday life. Furthermore, the instrumental view of smart homes emphasizes on management and reduction of energy demands in the households. It is expected to reduce the carbon footprints for the coming future.

A smart home application was proposed by Adib [23] named as Vital Radio. It is a wireless sensing technology that can collect data about heart rate and breathe in the human body without even making direct contact with the subject; it provided the median accuracy of 99%. Other smart home projects developed in Europe are iDorm [24], Gloucester Smart Home [25], and CareLab [26].

The new age smartphones are designed with high-end processing capabilities, and the advanced sensor systems such as BLE, NFC, microphone, camera, proximity sensor, gyroscope, accelerometer, and GPS further provide enhanced scope for assisted living applications. The latest smartphones are loaded with advanced sensors that are capable enough to recognize physical activities cycling, driving, descending stairs, climbing stairs, running, walking, and inactivity as well, without any additional sensing hardware [27, 28].

Some projects are also capable enough to detect the driver's behavior to ensure safe or unsafe movements. These systems work with Bayesian classification and optimal path detection algorithms; the event data for such systems is collected through smartphone sensors such as magnetometer, gyroscope, and accelerometer [29].

Researchers have also developed a Distributed Particle Filter Simultaneous Localisation and Mapping (DPSLAM) method for providing drift constraints on a simple mounted inertial measurement unit. These systems work in association with smartphones to provide core information on user movements [30]. In short, smartphones play a significant role in building smart communication architectures for AAL; users can avail instant updates about what is happening in the network while detecting any assistance required by the older adults [31].

Light sensors, gyroscopes, and accelerometers are widely used for recognizing daily activities; cameras and microphones can be applied for multimedia applications such as e-health and AAL [32].

Using long-range (3G/4G, GPRS), short-range (Wi-Fi and Bluetooth) communication abilities of smartphones, and advanced information processing capabilities of modern platforms loaded with powerful CPUs, it is possible to monitor co-morbid patients remotely [33, 34].

The NFC sensors are also utilized for the development of an open platform for regular monitoring of clinical signs; such tasks are executed with the help of smart and non-invasive wearable devices. The communication channels are further established using Near Field Communication while developing an efficient link between host and accessories, without requiring any additional effort for pairing [35].

The above discussions show that smartphones are an integral element of AAL systems due to their vast processing power, communication technologies, and efficient sensor units.

Wearable sensors find a variety of applications in the AAL systems. While working in combination with visualization tools and data treatment algorithms, they ensure efficient measurements for real-life environments, physical activities, mobility, and other physiological responses. Yan et al. [36] proposed an interesting project where wearable sensors were used to collect real-time data from patients suffering from cardiometabolic and pediatric risks.

Few other notable projects in the AAL domain also used wearable headbands to detect emotions in the form of electroencephalogram (EEG); this data was further utilized for evaluating the quality of life of assisted people [37].

Wearable motion sensors can also collect motion data in smart AAL to analyze behavioral anomaly situation concerning the location of the person [38]. Wearable technologies make it easier to reduce the overall cost of healthcare by allowing natural monitoring abilities to the patients at home, instead of spending a higher amount at hospitals [39]. Wrist bands work as non-invasive sensors to monitor and measure various physiological activities in the form of respiration, electrodermal activity, electroencephalogram, electrocardiogram, and few other biochemical processes such as healing of a wound [40]. The non-invasive wearable sensors are expected to work as low-cost solutions for monitoring the health of older adults remotely at nursing homes or within their personal living spaces. These inventions provided significant improvements for ensuring patient well-being and continuous monitoring of healthcare services [41].

The latest wearable computing devices loaded with the embedded camera can be used to determine the orientation and position of the user. Such AAL systems can be designed using SLAM and Visual Odometry techniques in combination with Augmented Reality; there is no need to use any off-the-shelf equipment or introduce any change in the environment for making measurements [42].

It is also possible to promote a healthy lifestyle by processing potential bio-signals generated from wearable sensors with the help of machine learning algorithms. Such systems can make instant guidelines and recommendations for fostering active routines as per specific health conditions of the individual [43].

HealthMon is a recently developed framework for mobile health solutions; it proposes an affordable wristband for all clinical monitoring needs such as Parkinson's disease, dementia, and aging. This system generates contextualized alerts as per the real-time updates from the automated health monitoring unit [44].

The new age wearable sensors can be used to monitor and predict patient conditions while combining some relevant clinical observations. It can help in the identification of "abnormal" physiological data due to any deterioration in patient health [45].

Another relevant project based on wearable sensors was proposed by Sano et al. [46] that works for recognizing academic performance, stress levels, sleep quality, and mental health of individuals using different personality traits. When combined with mobile phones for real-time data analysis, such systems provided accuracies within 67 to 92%.

The detailed study above shows the impact of advanced, interesting, and intelligent wearable sensor networks on assisted living environments. IoT systems are designed by connecting various objects having unique sensing abilities to the single network over the internet. These devices are expected to have context-aware and ubiquitous performance; the intelligent features further contribute to the improvement of assisted living environments.

IoT hardware has a direct relation to Sensor Networks, NFC and RFID; these systems work with the help of specific protocols and standards to assist machine to machine (M2M) communication capabilities; one of the best examples of such networks is semantic web. IoT promises considerable improvement in the human lifestyle with its low-cost automation and augmentation abilities [47].

Potential challenges associated with AAL and IoT systems are legalization, privacy, and security issues. Note that the IoT devices work wirelessly, and they are placed in the public range; it is essential to establish reliable protocols for ownership of data collected through these units. All new age IoT devices must be equipped with robust privacy policies and should support encryption methods for safe data transfers [48].

The Industry 4.0 Standard (I4S) provides efficient solutions for automation and data exchange by utilizing few latest technologies such as IoT Big Data, augmented reality, cloud computing, content-based image retrieval, 5G technology, wireless internet, and cryptography. The most important extension of I4S in the healthcare sector is named Healthcare 4.0 that is closely related to finitude medicine, home care, and remotely trigger pharmaceutical treatments. Several researchers have provided an in-depth analysis of utilizing Healthcare 4.0 for improving patient health and the quality of medical care facilities. Vohra at el. [49] proposed a Tactile internet-based AAL solution for fog environment, whereas Budhiraja et al. [50] gave insights to NOMA-based solutions using 5G technologies. The biometric healthcare approach was discussed in [51]; however, [52] shared verification and validation techniques for streaming big data analytics in the IoT environment. The future scope of healthcare 4.0, along with potential opportunities and challenges, was presented in [53].

AmbLEDs project made some efforts to resolve privacy issues by using LEDs instead of invasive sensors such as microphones and cameras for ensuring positive interactions in the AAL environment [54]. Humans are an integral part of IoT systems; hence, these advancements are going to leave a significant impact on the human lifestyle [55].

A valuable system for monitoring and controlling the household environment using ZigBee Wireless Network was proposed by Suryadevara et al. [56]; it works by combining the technologies of AAL and IoT to lead reliable performance. Furthermore,

SPHERE Project [57] proposes a generic platform for using complementary sensor data to generate valuable datasets for supporting the management and detection of different healthcare issues. It is based on three sensing technologies: wearable, video, and environment sensing. SPHERE project is expected to cover the gap between AAL and IoT systems.

Other areas of interest include cloud-based IoT platforms for AAL where the main goal is to manage device integration while ensuring easy access to services via cloud-based AAL applications [58]. The earlier technologies such as RFID are still useful in the world of IoT and AAL for designing intelligent systems so that supervised machine learning algorithms can analyze user-object interactions. One such system proposed by Parada et al. [59] provided 86% accuracy.

Home Health Hub Internet of Things (H3IoT) is a new architectural framework with an application to monitor elderly health at home. It is another efficient combination of IoT and AAL systems [60].

The projects discussed above show the potential of combined IoT and AAL systems to solve several routine issues and that too at low-cost implementation abilities.

3 Internet of Things and Wireless Sensor Networks Architectures for Enhanced Indoor Air Quality

IoT based projects for IAQ monitoring make use of open source technologies for data acquisition, transmission, and processing microsensors. They allow easy and simultaneous access to a database collected from different sites using mobile computing devices [5, 61–71].

Furthermore, a context-aware system with mobile sensing capabilities is proposed by [72]. This project makes use of the Arduino platform while sensing data about a few significant parameters such as CO_2, CO, humidity, and temperature. The collected data is further uploaded to servers online with the help of Wi-Fi communication; however, it can be accessed on a mobile phone via Bluetooth Low Energy (BLE).

A system for supervising energy parameters and the comfort of occupants within buildings is designed using autonomous mobile indoor robots [73]. This system works with the help of TurtleBot that allows easy navigation while incorporating various sensors for monitoring indoor parameters such as electricity consumption, airspeed, occupancy levels, light, CO_2, humidity, and temperature.

Another hybrid WSN (Wireless Sensor Network)/IoT based IAQ monitoring system was proposed by [74]. This system is made up of multiple sensor nodes with CO_2 sensing capabilities, and it permits instant data visualizations of IAQ information on remote servers.

A group of researchers proposed an indoor autonomous mobile robot system for the supervision of environmental quality [75]. This system was enabled by a sensor-rich navigation-capable robot to ensure the active monitoring of indoor premises. The promised automated sensor network incorporates Wi-Fi communication technology to handle data collected from temperature, VOC, light, and CO_2 sensors.

The "open-source smart lamp" system was developed for smart indoor air quality management by using the Arduino platform [76]. This system is designed to ensure a

cost-effective solution to maintain enhanced control on indoor lighting quality, IAQ, and thermal comfort. The sensor network consists of light, CO_2, humidity, and temperature sensor.

An advanced environmental supervision system was developed by combining wireless communication technologies to mobile robots, and it allowed secure storage of collected data on cloud servers [77]. The master robot in this system designated as a base station, whereas other robots are configured to work as sensor nodes; they collect data from end nodes and send them to master robots. After receiving data from end nodes, the base station transfers it further to the cloud system for easy visualization and analysis.

A WSN based, high-performance combination of Waspmotes and ZigBee communication technology was designed for IAQ monitoring [78]. The sensor nodes in these projects collect data related to CO_2, CO, humidity, and temperature. Furthermore, DUSTTRAK DRX 8533 Aerosol was used to ensure continuous monitoring of particulate matter. The collected environment data can be accessed with the help of a JAVA powered desktop application. The base station is responsible for collecting data from sensor nodes placed in the indoor environment.

IoT is an interesting concept for building advanced healthcare systems while allowing efficient treatment of several diseases. An IoT based solution for therapy of diabetic patients was proposed by [79]. This project supports easy data management for patient profiles using personal RFID cards. The collected data can be accessed anywhere in the world using personal gadgets based on 6LoWPAN, patient's web portal, glycaemic index information system, and physicians/nurses desktop application.

The IoT approach is also useful for real-time transmission of physical information. One such project was proposed in 2009 for leading remote healthcare program with the intelligent information collection system. It promotes the sound application of IoT in the medical health industry [80].

Although IoT systems and few new technologies ensure significant advancements in the healthcare sector, few challenges are yet to be addressed. Despite being a feasible solution with secure implementation options, there are few considerable barriers in the immediate adoption of IoT products and services at ground level [81].

IoT technologies ensure a wide range of benefits in the healthcare domain; it can be used for tracking staff, patients, objects, provide secure authentication and identification of people along with automatic data sensing and collection abilities [82]. Wearable sensors are a great addition to the IoT platform with their capabilities to upload data directly to the servers. At the same time, these new-age sensors ensure reliable communication with smartphones via Bluetooth networks. It provides easy interfacing of sensors for measuring a wide range of physiological parameters [83].

Healthcare applications are adopting IoT technologies to ensure secure and easy access to sensitive patient information via convenient mechanisms. The integration of various IoT systems and sensors provide a fast solution from the medical staff whenever a severe health deterioration is recorded. Hence, it leads to preventive care services [84].

An IoT based in-home healthcare service, Health-IoT, promises efficient results for maintaining the health of the people living within the premises. This business-technology

co-design methodology is designed to ensure reliable cross-boundary integration for various in-home healthcare devices [85].

Security vulnerabilities are a significant issue in the M2M/IoT communication network. One of the significant challenges is to create a secure architecture and ensure adequate access to the entities at the desired time. Another main issue with M2M/IoT devices is missing encryption abilities at the device level [86]. It is crucial to address these problems to ensure reliable solutions for healthcare systems using IoT.

The IoT based architecture with enhanced sensing abilities was designed to lead energy-efficient performance [87]. It achieved higher performance by using IPv6 protocol over Low Power Wireless Personal Area Networks (6LoWPAN). The idea helped to connect energy-constrained WPAN devices to the internet while ensuring the dynamic utilization of sensors to execute the desired process.

The IoT paradigm is a trusted solution for real-time monitoring, storing, and utilizing data related to health and well-being [88]. Such systems can work 24 $\times$ 7 while ensuring personalized data collection online [84, 89].

A Smart e-Health Gateway named UT-GATE was proposed to monitor the health of the residents from remote locations [83]. This Gateway makes use of IoT technologies to provide local services for health management. Some of the most common applications for such systems include WebSocket server, signal processing, compression, local repository, protocol translation and tunneling, data mining and notification, firewall.

Health, IoT, and AAL systems are closely related to each other and have a few common challenges in real-time implementation. However, few projects bring all these domains to a single platform for ensuring secure and efficient architectures.

4 Design, Social and Ethical Challenges

The systems designed for older adults demand special attention because of their physical and cognitive limitations. It is a big challenge for the health system design and implementation.

The health systems at the design level must follow a simple process; the wearable sensors are further required to be more compatible with the human body. Another big challenge in front of upcoming researchers is to maintain the energy consumption of the healthcare systems. The battery lifespan must be enhanced to ensure convenient and reliable performance. It is good to lead device level interactions using smart objects such as smartphones and TV; they can help to manage the efficiency to a considerable level.

It is essential to develop smart housing solutions as per the unique health status of individuals. The systems must ensure adequate support for health care services while ensuring more privacy to the users. Maintaining the comfort of individuals is another big challenge in society [90]. Once older adults realize the importance of these smart health care systems installed within living space, they will naturally consider them an integral part of their routines. The enhanced user-interfaces and efficient alert systems can motivate older adults to use these systems in their everyday life [91].

The adequate integration of health services such as context awareness, communication, dynamic configuration, and interoperability can provide better solutions to human beings. Furthermore, these systems must be loaded with security abilities based on physiological features and biometrics to safeguard user privacy [92]. An interesting idea for designing enhanced living environments for AAL platforms was proposed by [93]. However, improving reliability and dependability with enhanced interoperability and standardization is still a relevant challenge [94].

The socially interactive and assistive robots raise the safety and privacy of the end-users. But few ethical issues in replacing personal care with robots are still required to be addressed [95]. The challenges associated with the real-time implementation of AAL systems are highlighted in Fig. 2.

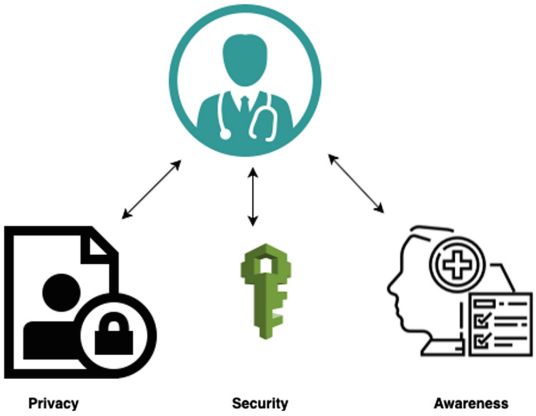


Fig. 2. Challenges associated with the real-time implementation of AAL systems.

5 Conclusions

AAL platform plays a crucial role in solving the independence problems of older adults. These systems can provide better performance to deal with emergencies associated with disease and disabilities when integrated into IoT technologies, wearable devices, smartphones, and smart homes. But, even after the unlimited benefits of AAL systems and considerable advancements in technologies, there is no point in replacing personal care because such interactions and social care have their importance in human life. While offering some efficient solutions to the healthcare sectors, technological advancements will continue to face some challenges in terms of invasive devices, energetic autonomy, and uncomfortable devices. It is essential to do in-depth research to find some reliable solutions to these problems.

The AAL and IoT systems are expected to grow side by side while contributing to scientific advancements in assisted living environments. They are also likely to provide low-cost solutions to improve the lifestyle of older adults. Although technologies are improving with each passing day, some difficulties related to confidentiality, privacy,

and security are still causing troubles in the successful implementation of AAL systems. Moreover, most of AAL and IoT solutions are based on WSN architectures. Therefore the research on WSN issues and challenges plays a significant role in the proliferation of these systems. The enhancements on the IoT and AAL systems for enhanced living environments and healthcare will depend on the research and innovation of WSN architectures, particularly on the specific themes related to security, privacy, bandwidth demand, energy consumption, and quality of service.

Some legal and social issues also demand the attention of upcoming researchers and policymakers for enhanced consumer protection. At the same time, it is crucial to ensure efficient reporting of possible consequences while using these systems on a routine basis. The real-time monitoring is a reliable solution to support clinical analysis as medical specialists, and therapeutic teams can provide in-depth analysis of the history of collected data. With this, it is possible to link the collected data to the ongoing health changes in the patients. Furthermore, the supervision of IAQ can help to identify poor air quality conditions so that some considerable solutions can be planned for enhanced living environments.

References

1. Marques, G., Pitarma, R., Garcia, N.M., Pombo, N.: Internet of Things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review. Electronics **8**(10), 1081 (2019)
2. Koleva, P., Tonchev, K., Balabanov, G., Manolova, A., Poulkov, V.: Challenges in designing and implementation of an effective Ambient Assisted Living system. In: 2015 12th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), pp. 305–308 (2015)
3. Marques, G., Pitarma, R.: IAQ evaluation using an IoT CO_2 monitoring system for enhanced living environments. In: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S. (eds.) Trends and Advances in Information Systems and Technologies, vol. 746, pp. 1169–1177. Springer International Publishing, Cham (2018)
4. Giusto, D. (ed.): The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications. Springer, New York (2010)
5. Marques, G., Pitarma, R.: Monitoring and control of the indoor environment. In: 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6 (2017)
6. Marques, G., Pitarma, R.: Monitoring energy consumption system to improve energy efficiency. In: Rocha, Á., Correia, A.M., Adeli, H., Reis, L.P., Costanzo, S. (eds.) Recent Advances in Information Systems and Technologies, vol. 570, pp. 3–11. Springer International Publishing, Cham (2017)
7. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
8. Khanna, A., Goyal, R., Verma, M., Joshi, D.: Intelligent traffic management system for smart cities. In: Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies, vol. 958, pp. 152–164. Springer Singapore, Singapore (2019)

9. Marques, G.: Ambient assisted living and Internet of Things. In: Cardoso, P.J.S., Monteiro, J., Semião, J., Rodrigues, J.M.F. (eds.) Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities, pp. 100–115. IGI Global, Hershey (2019)
10. Walsh, P.J., Dudney, C.S., Copenhaver, E.D.: Indoor Air Quality. CRC Press, Boca Raton (1983)
11. Bruce, N., Perez-Padilla, R., Albalak, R.: Indoor air pollution in developing countries: a major environmental and public health challenge. Bull. World Health Organ. **78**(9), 1078–1092 (2000)
12. Seguel, J.M., Merrill, R., Seguel, D., Campagna, A.C.: Indoor air quality. Am. J. Lifestyle Med. **11**(4), 284–295 (2017)
13. Butz, A.M.: A randomized trial of air cleaners and a health coach to improve indoor air quality for inner-city children with asthma and secondhand smoke exposure. Arch. Pediatr. Adolesc. Med. **165**(8), 741 (2011)
14. De Vito, S., et al.: Cooperative 3D air quality assessment with wireless chemical sensing networks. Procedia Eng. **25**, 84–87 (2011)
15. Dimitrievski, A., Zdravevski, E., Lameski, P., Trajkovik, V.: A survey of Ambient Assisted Living systems: challenges and opportunities. In: 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, pp. 49–53 (2016)
16. El murabet, A., Anouar, A., Touhafi, A., Tahiri, A.: Towards an SOA architectural model for AAL-Paas design and implementation challenges. Int. J. Adv. Comput. Sci. Appl. **8**(7), 52–56 (2017)
17. El murabet, A., Abtoy, A., Touhafi, A., Tahiri, A.: Ambient Assisted Living system's models and architectures: a survey of the state of the art. J. King Saud Univ. - Comput. Inf. Sci. **32**(1), 1–10 (2020)
18. Choi, D., Choi, H., Shon, D.: Future changes to smart home based on AAL healthcare service. J. Asian Archit. Build. Eng. **18**(3), 190–199 (2019)
19. Rashidi, P., Mihailidis, A.: A survey on ambient-assisted living tools for older adults. IEEE J. Biomed. Health Inform. **17**(3), 579–590 (2013)
20. Moukas, A., Zacharia, G., Guttman, R., Maes, P.: Agent-mediated electronic commerce: an MIT media laboratory perspective. Int. J. Electron. Commer. **4**(3), 5–21 (2000)
21. De Silva, L.C., Morikawa, C., Petra, I.M.: State of the art of smart homes. Adv. Issues Artif. Intell. Pattern Recogn. Intell. Surveill. Syst. Smart Home Environ. **25**(7), 1313–1321 (2012)
22. Wilson, C., Hargreaves, T., Hauxwell-Baldwin, R.: Smart homes and their users: a systematic analysis and key challenges. Pers. Ubiquit. Comput. **19**(2), 463–476 (2015)
23. Adib, F., Mao, H., Kabelac, Z., Katabi, D., Miller, R.C.: Smart homes that monitor breathing and heart rate. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, pp. 837–846 (2015)
24. Pounds-Cornish, A., Holmes, A.: The iDorm - a practical deployment of grid technology. In: 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2002, pp. 470–470 (2002)
25. Orpwood, R., Gibbs, C., Adlam, T., Faulkner, R., Meegahawatte, D.: The Gloucester smart house for people with dementia—user-interface aspects. In: Keates, S., Clarkson, J., Langdon, P., Robinson, P. (eds.) Designing a More Inclusive World, pp. 237–245. Springer, London (2004)
26. Henkemans, O.B., Caine, K.E., Rogers, W.A., Fisk, A.D.: Medical monitoring for independent living: user-centered design of smart home technologies for older adults. In: Proceedings of Med-e-Tel Conference eHealth, Telemedicine and Health Information and Communication Technologies, pp. 18–20 (2007)

27. Anjum, A., Ilyas, M.U.: Activity recognition using smartphone sensors. In: Consumer Communications and Networking Conference (CCNC), 2013, pp. 914–919. IEEE (2013)
28. Shoaib, M., Scholten, H., Havinga, P.J.M.: Towards physical activity recognition using smartphone sensors. In: 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp. 80–87 (2013)
29. Eren, H., Makinist, S., Akin, E., Yilmaz, A.: Estimating driving behavior by a smartphone. In: 2012 IEEE Intelligent Vehicles Symposium (IV), pp. 234–239 (2012)
30. Faragher, R.M., Sarno, C., Newman, M.: Opportunistic radio SLAM for indoor navigation using smartphone sensors. In: 2012 IEEE/ION Position Location and Navigation Symposium (PLANS), pp. 120–128 (2012)
31. Lloret, J., Canovas, A., Sendra, S., Parra, L.: A smart communication architecture for ambient assisted living. IEEE Commun. Mag. **53**(1), 26–33 (2015)
32. Parra, L., Sendra, S., Jiménez, J., Lloret, J.: Multimedia sensors embedded in smartphones for ambient assisted living and e-health. Multimedia Tools Appl. **75**(21), 1–27 (2015)
33. Bisio, I., Lavagetto, F., Marchese, M., Sciarrone, A.: Smartphone-centric ambient assisted living platform for patients suffering from co-morbidities monitoring. IEEE Commun. Mag. **53**(1), 34–41 (2015)
34. Mishra, D., Mishra, A.: Self-optimization in LTE: an approach to reduce call drops in mobile network. In: Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies, vol. 958, pp. 382–395. Springer Singapore, Singapore (2019)
35. Leone, A., Rescio, G., Siciliano, P.: A near field communication-based platform for mobile ambient assisted living applications. In: Andò, B., Siciliano, P., Marletta, V., Monteriù, A. (eds.) ambient assisted living, vol. 11, pp. 125–132. Springer, Cham (2015)
36. Yan, K., et al.: Innovation through wearable sensors to collect real-life data among pediatric patients with cardiometabolic risk factors. Int. J. Pediatr. **2014**, 9 (2014)
37. Matiko, J.W., Wei, Y., Torah, R., Grabham, N., Paul, G., Beeby, S., Tudor, J.: Wearable EEG headband using printed electrodes and powered by energy harvesting for emotion monitoring in ambient assisted living. Smart Mater. Struct. **24**(12), 125028 (2015)
38. Zhu, C., Sheng, W., Liu, M.: Wearable sensor-based behavioral anomaly detection in smart assisted living systems. IEEE Trans. Autom. Sci. Eng. **12**(4), 1225–1234 (2015)
39. López, S.A., Corno, F., De Russis, L.: Supporting caregivers in assisted living facilities for persons with disabilities: a user study. Univers. Access Inf. Soc. **14**(1), 133–144 (2015)
40. Acampora, G., Cook, D.J., Rashidi, P., Vasilakos, A.V.: A Survey on Ambient Intelligence in Health Care. Proc. IEEE Inst. Electr. Electron. Eng. **101**(12), 2470–2494 (2013)
41. Bandodkar, A.J., Wang, J.: Non-invasive wearable electrochemical sensors: a review. Trends Biotechnol. **32**(7), 363–371 (2014)
42. Saracchini, R.F.V., Catalina, C.A.: An augmented reality platform for wearable assisted living systems. J. Theor. Appl. Comput. Sci. **9**(1), 56–79 (2015)
43. Páez, D., de Buenaga Rodríguez, M., Sánz, E., Villalba, M., Gil, R.: Big data processing using wearable devices for wellbeing and healthy activities promotion. In: Cleland, I., Guerrero, L., Bravo, J. (eds.) Ambient Assisted Living. ICT-based Solutions in Real Life Situations, vol. 9455, pp. 196–205. Springer, Cham (2015)
44. Stavropoulos, T.G., Meditskos, G., Andreadis, S., Kompatsiaris, I.: Real-time health monitoring and contextualised alerts using wearables. In: 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), pp. 358–363 (2015)
45. Clifton, L., Clifton, D.A., Pimentel, M.A.F., Watkinson, P.J., Tarassenko, L.: Predictive monitoring of mobile patients by combining clinical observations with data from wearable sensors. IEEE J. Biomed. Health Inform. **18**(3), 722–730 (2014)

46. Sano, A., et al.: Recognizing academic performance, sleep quality, stress level, and mental health using personality traits, wearable sensors and mobile phones. In: 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN), pp. 1–6 (2015)
47. Whitmore, A., Agarwal, A., Da Xu, L.: The Internet of Things—a survey of topics and trends. Inf. Syst. Front. **17**(2), 261–274 (2015)
48. Sachdeva, S., Kakkar, A.: Implementation of AES-128 using multiple cipher keys. In: Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies, vol. 958, pp. 3–16. Springer Singapore, Singapore (2019)
49. Vora, J., Kaneriya, S., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S.: TILAA: tactile internet-based Ambient Assistant Living in fog environment. Future Gener. Comput. Syst. **98**, 635–649 (2019)
50. Budhiraja, I., Tyagi, S., Tanwar, S., Kumar, N., Rodrigues, J.J.P.C.: Tactile Internet for smart communities in 5G: an insight for NOMA-based solutions. IEEE Trans. Ind. Inform. **15**(5), 3104–3112 (2019)
51. Hathaliya, J.J., Tanwar, S., Tyagi, S., Kumar, N.: Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach. Comput. Electr. Eng. **76**, 398–410 (2019)
52. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N.: Fog computing for Healthcare 4.0 environment: Opportunities and challenges. Comput. Electr. Eng. **72**, 1–13 (2018)
53. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N.: Verification and validation techniques for streaming big data analytics in Internet of Things environment. IET Netw. **8**(3), 155–163 (2019)
54. Cunha, M., Fuks, H.: AmbLEDs para ambientes de moradia assistidos em cidades inteligentes. In: Proceedings of the 13th Brazilian Symposium on Human Factors in Computing Systems, Foz do Igua & ccedil; u, Brazil, pp. 409–412 (2014)
55. Stankovic, J.A.: Research Directions for the Internet of Things. IEEE Internet Things J. **1**(1), 3–9 (2014)
56. Suryadevara, N.K., Kelly, S., Mukhopadhyay, S.C.: Ambient Assisted Living environment towards Internet of Things using multifarious sensors integrated with XBee platform. In: Mukhopadhyay, S.C. (ed.) Internet of Things, vol. 9, pp. 217–231. Springer (2014)
57. Zhu, N., et al.: Bridging e-health and the Internet of Things: the SPHERE project. IEEE Intell. Syst. **30**(4), 39–46 (2015)
58. Cubo, J., Nieto, A., Pimentel, E.: A cloud-based Internet of Things platform for Ambient Assisted Living. Sensors **14**(8), 14070–14105 (2014)
59. Parada, R., Melia-Segui, J., Morenza-Cinos, M., Carreras, A., Pous, R.: Using RFID to detect interactions in Ambient Assisted Living environments. IEEE Intell. Syst. **30**(4), 16–22 (2015)
60. Ray, P.P.: Home Health Hub Internet of Things (H3IoT): an architectural framework for monitoring health of elderly people. In: 2014 International Conference on Science Engineering and Management Research (ICSEMR), pp. 1–3 (2014)
61. Pitarma, R., Marques, G., Ferreira, B.R.: Monitoring indoor air quality for enhanced occupational health. J. Med. Syst. **41**(2), 23 (2017)
62. Marques, G., Pitarma, R.: Health informatics for indoor air quality monitoring. In: 2016 11th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6 (2016)
63. Marques, G., Roque Ferreira, C., Pitarma, R.: A system based on the Internet of Things for real-time particle monitoring in buildings. Int. J. Environ. Res. Public. Health **15**(4), 821 (2018)

64. Feria, F., Salcedo Parra, O.J., Reyes Daza, B.S.: Design of an architecture for medical applications in IoT. In: Luo, Y. (ed.) Cooperative Design, Visualization, and Engineering, vol. 9929, pp. 263–270. Springer, Cham (2016)
65. Ray, P.P.: Internet of Things for smart agriculture: Technologies, practices and future direction. J. Ambient Intell. Smart Environ. **9**(4), 395–420 (2017)
66. Matz, J.R., Wylie, S., Kriesky, J.: Participatory air monitoring in the midst of uncertainty: residents' experiences with the speck sensor. Engag. Sci. Technol. Soc. **3**, 464 (2017)
67. Demuth, D., Nuest, D., Bröring, A., Pebesma, E.: The airquality sensebox. In: EGU General Assembly Conference Abstracts, vol. 15 (2013)
68. Marques, G., Pitarma, R.: A cost-effective air quality supervision solution for enhanced living environments through the Internet of Things. Electronics **8**(2), 170 (2019)
69. G. Marques, C. R. Ferreira, and R. Pitarma, "Indoor Air Quality Assessment Using a CO2 Monitoring System Based on Internet of Things," J. Med. Syst., vol. 43, no. 3, Mar. 2019
70. Marques, G., Pitarma, R.: Monitoring and control of the indoor environment. In: 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, pp. 1–6 (2017)
71. Marques, G., Pitarma, R.: mHealth: indoor environmental quality measuring system for enhanced health and well-being based on Internet of Things. J. Sens. Actuator Netw. **8**(3), 43 (2019)
72. Lohani, D., Acharya, D.: Smartvent: a context aware IoT system to measure indoor air quality and ventilation rate. In: 2016 17th IEEE International Conference on Mobile Data Management (MDM), vol. 2, pp. 64–69 (2016)
73. Mantha, B.R., Feng, C., Menassa, C.C., Kamat, V.R.: Real-time building energy and comfort parameter data collection using mobile indoor robots. In: Proceedings of the International Symposium on Automation and Robotics in Construction Presented at the ISARC, vol. 32, p. 1 (2015)
74. Srivatsa, P., Pandhare, A.: Indoor air quality: IoT solution. In: National Conference, NCPCI, vol. 2016, p. 19 (2016)
75. Jin, M., Liu, S., Schiavon, S., Spanos, C.: Automated mobile sensing: towards high-granularity agile indoor environmental quality monitoring. Build. Environ. **127**, 268–276 (2018)
76. Salamone, F., Belussi, L., Danza, L., Galanos, T., Ghellere, M., Meroni, I.: Design and development of a nearable wireless system to control indoor air quality and indoor lighting quality. Sensors **17**(5), 1021 (2017)
77. Meena, M.J., Prabha, S.S., Pandian, S.: A cloud-based mobile robotic system for environmental monitoring. In: 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE), South Kuta, Indonesia, pp. 122–126 (2014)
78. Bhattacharya, S., Sridevi, S., Pitchiah, R.: Indoor air quality monitoring using wireless sensor network, pp. 422–427 (2012)
79. Jara, A.J., Zamora, M.A., Skarmeta, A.F.: An Internet of Things—based personal device for diabetes therapy management in ambient assisted living (AAL). Pers. Ubiquit. Comput. **15**(4), 431–440 (2011)
80. Luo, J., Chen, Y., Tang, K., Luo, J.: Remote monitoring information system and its applications based on the Internet of Things. In: 2009 International Conference on Future BioMedical Information Engineering, FBIE 2009, pp. 482–485 (2009)
81. Swan, M.: Sensor mania! The Internet of Things, wearable computing, objective metrics, and the quantified self 2.0. J. Sens. Actuator Netw. **1**(3), 217–253 (2012)
82. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)

83. Rahmani, A.-M., et al.: Smart e-health gateway: bringing intelligence to Internet-of-Things based ubiquitous healthcare systems, pp. 826–834 (2015)
84. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of Things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
85. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., Chen, Q.: Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. Enterp. Inf. Syst. **9**(1), 86–116 (2015)
86. Lake, D., Milito, R., Morrow, M., Vangheese, R.: Internet of Things: architectural framework for eHealth security. J. ICT **3**, 301–330 (2014)
87. Hassanalieragh, M., et al.: Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: opportunities and challenges, pp. 285–292 (2015)
88. Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., Schreier, G.: The Internet of Things for Ambient Assisted Living, pp. 804–809 (2010)
89. Domingo, M.C.: Review: an overview of the Internet of Things for people with disabilities. J. Netw. Comput. Appl. **35**(2), 584–596 (2012)
90. Geman, O., et al.: Challenges and trends in Ambient Assisted Living and intelligent tools for disabled and elderly people. In: 2015 International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM), pp. 1–5 (2015)
91. Muñoz, D., Gutierrez, F.J., Ochoa, S.F.: Introducing Ambient Assisted Living technology at the home of the elderly: challenges and lessons learned. In: Cleland, I., Guerrero, L., Bravo, J. (eds.) Ambient Assisted Living. ICT-based Solutions in Real Life Situations, vol. 9455, pp. 125–136. Springer, Cham (2015)
92. Li, R., Lu, B., McDonald-Maier, K.D.: Cognitive Assisted Living Ambient system: a survey. Digit. Commun. Netw. **1**(4), 229–252 (2015)
93. Grguric, A., Gil, A.M.M., Huljenic, D., Car, Z., Podobnik, V.: A survey on user interaction mechanisms for enhanced living environments. In: Loshkovska, S., Koceski, S. (eds.) ICT Innovations 2015, vol. 399, pp. 131–141. Springer, Cham (2016)
94. Monekosso, D.N., Florez-Revuelta, F., Remagnino, P.: Guest editorial special issue on ambient-assisted living: sensors, methods, and applications. IEEE Trans. Hum.-Mach. Syst. **45**(5), 545–549 (2015)
95. Felzmann, H., Murphy, K., Casey, D., Beyan, O.: Robot-assisted care for elderly with dementia: is there a potential for genuine end-user empowerment?. In: The Emerging Policy and Ethics of Human Robot Interaction (2015)

Energy Efficient Data Collection in Smart Cities Using IoT

Tanuj Wala[1(✉)], Narottam Chand[1], and Ajay K. Sharma[2]

[1] Department of Computer Science and Engineering,
NIT Hamirpur, Hamirpur, India
tanu.thakur52@gmail.com, nar.chand@gmail.com
[2] Department of Computer Science and Engineering,
NIT Jalandhar, Jalandhar, India
vcptul3@gmail.com

Abstract. Wireless sensor network (WSN) has emerged as a major part of the Internet of Things (IoT) and their collaboration helps in the formation of a smart environment. The usability of WSN has gained impetus with the advancement in the field of wireless technology. The impact of this growth can be seen in expanded smart city applications that have enhanced the living standards of citizens. In a smart city, millions of sensors are deployed in various intelligent applications like smart homes, smart transportation, smart industries, smart parking, and so forth to make the city smarter and efficient. These applications continuously generate a huge amount of data to provide innovative services to citizens. Therefore, an efficient collection of this data is utmost important to make an effective decision for the betterment of society. The sensor nodes work in collaboration to send the collected data to the base station. In WSN, the sensor nodes have resource constraints like low power and limited communication range. So, as a result, in reference to sensor processing, the continuous stream of data generated by sensor nodes need to be processed and delivered to the end-user in the optimal lapse of time. One promising approach to accomplish these needs is to collaborate among the sensors and sink in an efficient way to reduce the transmission cost. Recent research showed the emergence of several data collection approaches as data aggregation, data compression, optimal deployment of sinks and sink mobility. These approaches mainly aim specifically to reduce consumption of energy, time delay management and maximize the network lifetime. Referring to this context, this chapter discusses challenges in the field of data collection approaches and proposes possible future directions.

Keywords: Wireless sensor network (WSN) · Internet of Things (IoT) · Smart city · Sink mobility · Data collection

1 Introduction

The current era unveils billions of sensor enabled intelligent devices that work on the Internet and are referred to as IoT (Internet of Things) altogether. IoT is an upcoming platform of network paradigm that aims to provide interaction among various pervasive things through heterogeneous connections. RFID tags, mobile phones and sensors are

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 632–654, 2020.
https://doi.org/10.1007/978-3-030-40305-8_30

referred to as pervasive things [1]. They can interact and communicate with each other at any point in time at anyplace. The IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people with unique identifiers (UIDs) capable of transferring data over a network without the need for human-to-human or human-to-computer interaction [2]. Millions of objects can be embedded with sensors for data collection and can be analyzed on data services using IoT. Several smart systems can be constructed using this data such as smart grid, smart city, smart parking, smart environment, etc. [3]. WSNs (Wireless sensor networks) which are generally ad hoc networks and an integral part of IoT are used for collecting data from these sources. The tiny sensor nodes of WSN are capable of sensing, communication and computation [4]. WSN should be integrated with IoT to manage and use the collected data to provide smart services. The plethora of devices that are connected to the Internet has resulted in an unprecedented growth of IoT in the current world and is expected to grow manifold.

1.1 IoT Architecture

A well-defined IoT architecture has not yet been created. However, a high-level architecture of three-layers is widely recognized. This architecture comprises of three layers: Perception Layer, Network Layer, and Application Layer. Figure 1, describes these layers thoroughly with the functionalities of each component [5].

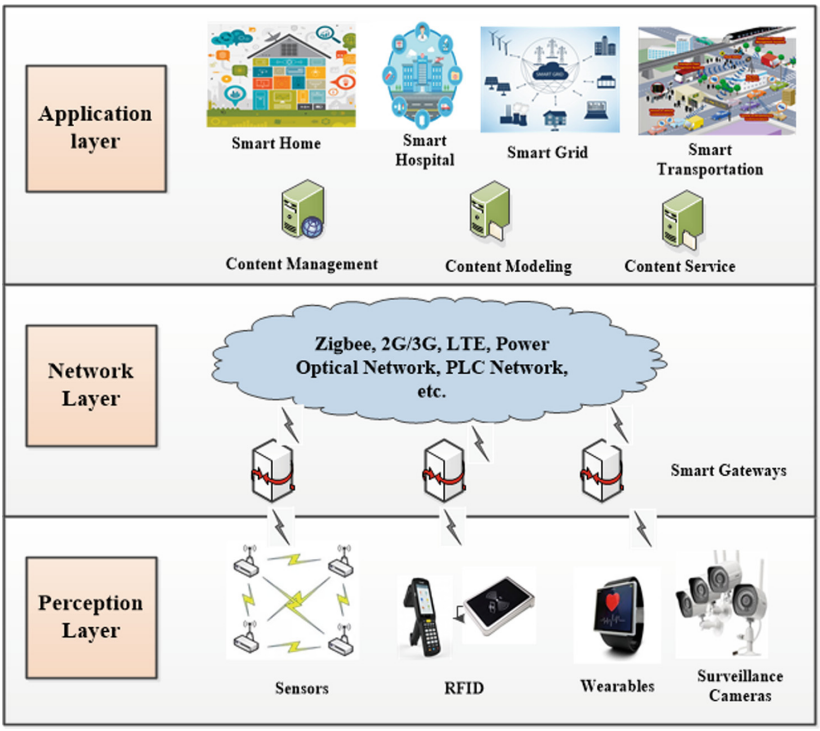


Fig. 1. Three layer architecture of IoT [5].

A short description of each layer is provided as follows:

(1) Perception layer: The task of the perception layer is to recognize, identify, collect and exchange data using a group of devices enabled by the Internet. RFID, cameras and sensors are some examples of perception layer devices [5]. Furthermore, this layer is responsible for changing data to digital signals, which are increasingly helpful for network transmission.
(2) Network layer: The network layer forwards the data from the perception layer to the application layer under some constraints such as capability and limitations of the network. Short range network communication technologies such as Bluetooth and Zigbee are combined with IoT to transfer information from perception devices to nearby gateways [6]. The capability of communicating parties still remains under lived constraints. The information is carried over long distances with the help of Internet technologies like 2G, 3G, 4G, etc.
(3) Application layer: The application layer utilizes the prior layers of processed information. In reality, this layer gives the front end of the entire IoT architecture through which services are utilized. In addition, this layer offers developers with the necessary instruments like actuating devices to understand the IoT vision.

Usually, the three-phase procedure is used to deal with the sensor data that is generated through IoT architecture. Figure 2, shows the three-phase procedure: (1) data acquisition (2) data collection and (3) data computation in detail. The first phase i.e. data acquisition using the sensing equipment to sampling the sensory data that measure the physical conditions and convert into electrical signals. In the second phase, the raw sampled data is transmitted through the intermediate nodes towards data collector or collectors, where they connect an IoT environment to the cyber world such as cloud, servers. In the last phase, the delivered data is further computed by using various techniques such as numerical analysis, knowledge discovery, and so forth as per the requirements of applications and users [7].

All the above discussed phases are necessary for any IoT application, but this chapter is mainly based on the second phase i.e. data collection. The main aim of this phase is to successfully deliver data from all sensor nodes towards data collectors.

According to world population prospects report, about 70% of the population would be residing in urban areas by 2050. Also as per the 2011 census, currently 31.1% of India's population resides in urban areas [8]. With the urban population expected to expand manifold, requirements to manage urban living also needs an evolving. In this context, the Government of India has also launched Smart India Mission to scale up the urban infrastructure and revolutionize the urban living standards [9]. Though, physical infrastructure stands at the pinnacle, quality of knowledge communication and social infrastructure do provide a significant add on. The concept of the smart city encompasses applying next generation advancements in technology in various domains of life, encapsulating sensors in physical corners and utilizing the concept of the IoT. Internet of Things refers to the extension of Internet connectivity into physical devices and everyday objects. It offers a plethora of possibilities to researchers relating to smart cities and helps them to figure out ways to evolve ideas relating to the sustainable development of smart cities.

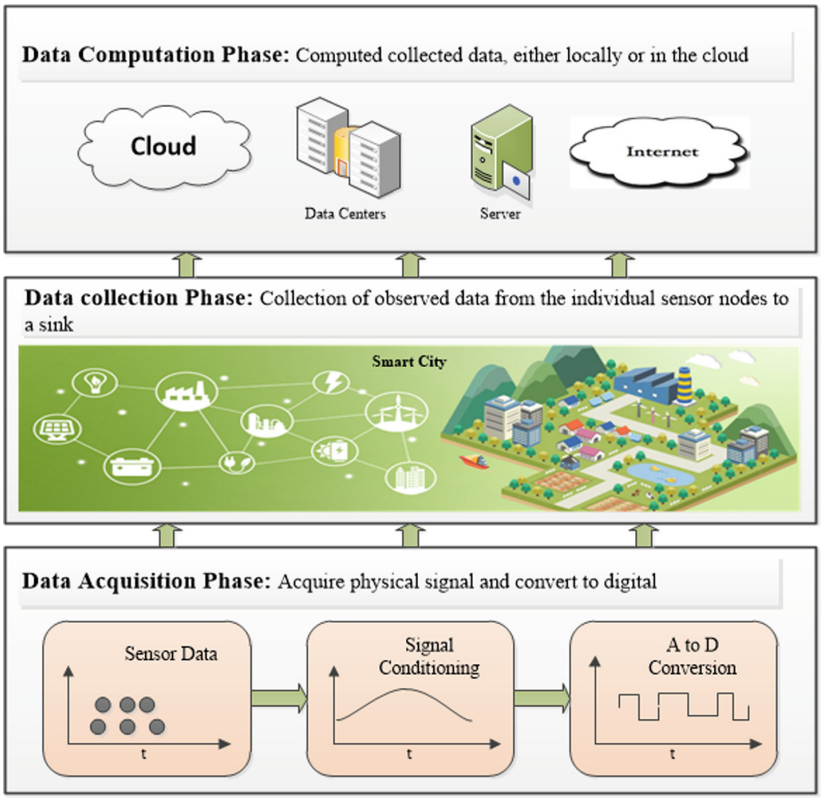


Fig. 2. Three phase procedure to deal with sensor data [7].

1.2 Smart Cities Using IoT

IoT in integration with WSN successfully paves a roadmap for establishing smart cities that comprises of smart devices [10]. The concept of a smart city is to enhance the living standard of people by utilizing information technology and creating a modern urban area. The effective communication and proper data management using a physical infrastructure enhancement are the integrated foundation of the smart city development concept. Sophisticated computing and technology, lots of devices and connected servers form the working components of a smart city [8]. Sensor technology and IoT have given the solution for living in a smart environment with efficient management of natural resources, mobility, healthcare, governance and energy. Several services of the smart city concept include smart transportation, smart parking, smart home, smart grid, and so forth. Figure 3 describes the smart city applications in detail [11].

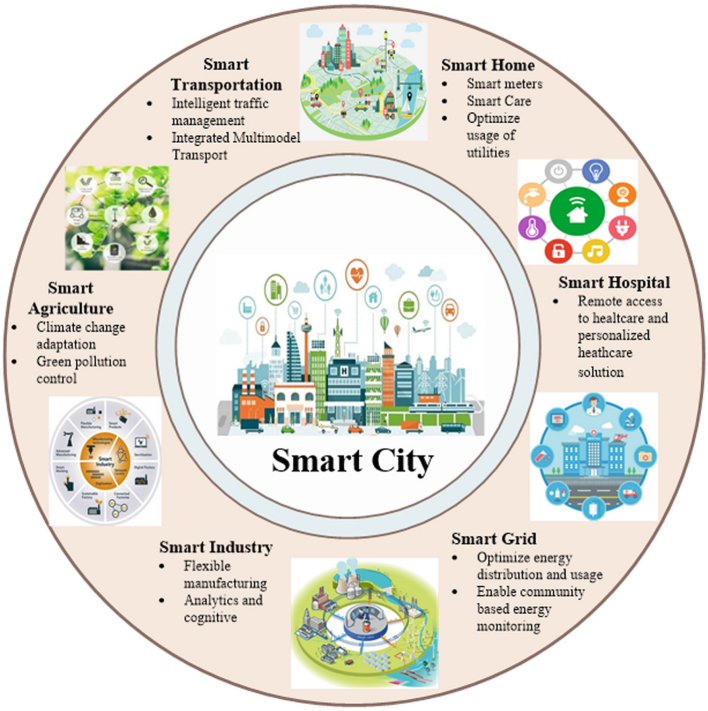


Fig. 3. Smart city applications [11].

The continuous city information is collected from smart homes, smart transportation, agriculture framework, smart grid, security and observation framework, and others. Later, the majority of this information is utilized by the experts to take the city-related decision, utilizing insightful structure furnished with information examination, devices and algorithms. In the smart home, the home is ordinarily digitized by constantly checking the temperature and smoke to detect the flame, day by day energy consumption and water utilization, individual's exercises by cameras, and significantly more. This information is utilized by the smart city framework to produce cautions and take activities if there should be an occurrence of a crisis in a house. Similarly, in the smart transportation system, efficient transport is a key part of a smart city commuting system. Using IoT with the help of physical interfaces such as road sensors, citizens can find the fastest route to their destination [12]. The authorities can be notified once any highway has been closed or incident has occurred. Sustaining our energy demands and needs is one of the core priorities of our country. India's energy demands are expected to double by 2030, keeping in view the demographic changes that it is witnessing. Hence, optimizing energy consumption is a key issue in the IoT environment. For this purpose, energy and power-related information are collected and shared with Power Supply Company for improving efficiency, reliability and economics. Also, with the help of IoT, advancements such as remote heart transplant, smart beds are coming into picture which earlier was thought of as mere imagination [13].

All these applications come together to enhance the living standards of modern society. Currently, advancements in physical infrastructure and effective real-time communication are the biggest constraints for smart city management. IoT technology forms the bridge for communication among various applications of the smart city. The rapid increase in IoT technology is resulting in the generation of high volume data which is having various structural formats and is being generated at a very high speed. This data defines the real significance and characteristics of smart city applications and is called big data [14]. The collected big data is unstructured and needs to be stored at various data centers using a distributed database. Since most of the data collected is unstructured and most of the IoT applications are work on battery operated smart devices which are constraint by energy, therefore energy efficient data collection issue is one of the most challenging tasks in IoT based environment.

Several approaches are used to collect data with the aim of reducing energy consumption and improving network life. Data aggregation is one of the most prominent examples of reducing total communication costs [15]. However, a number of aggregated data is still significant in large scale IoT environments. The reason is a huge volume of data is transferred from the collection point to the base station. Hence, the need for precision of aggregation has to be taken care of. This is usually done by the trading off precision with energy-saving. The data prediction is yet another energy-efficient approach for collecting data from sensors enabled environment [16]. It considered the spatial and temporal correlation between sensor data. Further, there is data compression technology that reduces the volume of transmitted data by compressing the huge volume of data [17]. The task required nodes to be equipped with sufficiently large storage and powerful computation. Recently, a boom in intention has been noticed for a mobile sink scheme [18]. The scheme includes the dense deployment of sensing areas for data collection. The data collectors are generally called sinks and are movable such that the traveling sinks sense the data and also transfers it where so ever required. A significant amount of energy can be saved by following the approach of reduction in wireless transmission. Since every technique has pros and cons, increase latency and huge energy consumption is emerging out to be a challenging task. So, in this chapter, we discuss various data collection approaches associated with smart cities using IoT.

The rest of the chapter is organized under the following sections. Section 2 covers the literature survey in brief about the data collection approaches in the IoT environment. Section 3 provides a future direction and Sect. 4 gives the conclusion.

2 Data Collection in IoT Environment

One of the main issues with the IoT system is the magnitude of data collected by different sensors or actuators. Transmission and storage of such large data have become a challenging task because of significant-high bandwidth and space requirements.

So, this section discusses several approaches to cope with unbalanced issues in data collection. The drawing mechanism of data collection is a very challenging task

because of the constraint resources and hot spot problem. From the last decade, various data collection approaches are proposed to reduce energy consumption and for efficient collection of data in the context of IoT and smart cities [19]. Figure 4, depicts the different data collection approaches presented in this section.

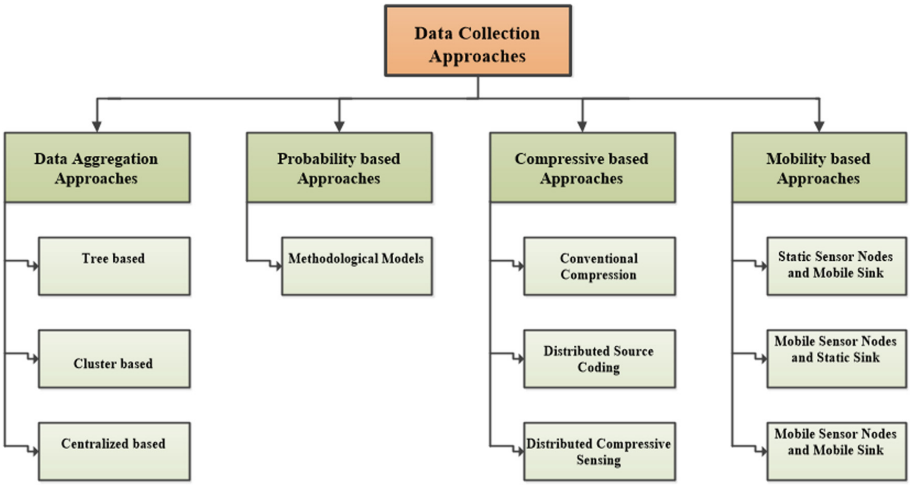


Fig. 4. Different data collection approaches.

2.1 Data Aggregation Approaches

Data aggregation is a process that diminishes the number of transmissions in the network by utilizing different aggregation methods such as MAX, MIN, SUM, AVG, COUNT, and so forth at the relay nodes [20]. The primary objective of this process is to remove duplicated transmission of data that leads to maximize network lifetime and balance energy consumption. In this chapter, data aggregation techniques are divided into three categories; (1) Tree-based, (2) cluster-based, and (3) Centralized based.

Tree Based Mechanism

In tree-based mechanism, all the nodes are arranged in hierarchical manners and the data aggregation task is carried out at intermediate nodes. Thereafter, all the aggregated data is forward to the root node. In this methodology, initial an aggregation tree is constructed which is commonly known as the minimum spanning tree. In this tree, the root node goes about as base station or sink, leaf nodes go about as source nodes and intermediate nodes go about as parent nodes. The data aggregation process using a tree-based mechanism is appeared in Fig. 5 [15]. The aggregated data is moved to the sink by choosing the best route.

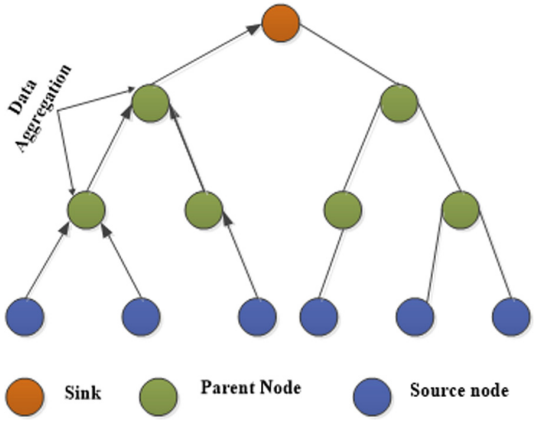


Fig. 5. Data aggregation using a tree-based mechanism [15].

Many research studies are based on this type of mechanism to accomplish the aggregation task. Virmani et al. [21] have proposed an Adaptive Energy-Aware Data Aggregation Tree (AEDT). In this tree, a node whose energy is maximum selected as an aggregator node. To save energy consumption, the proposed tree joins rest hold up a method where just the parent node and the communicating node in the wakeful state, rest every one of the nodes in a rest state, wherein the intermediate nodes intermittently go to alert state in the event that they have any message to be sent. In every event the traffic burden is evaluated, if the evaluated traffic burden is more than the communication limit of parent node then an overload message is transmitted in the network. A memory table is likewise kept up in which all the found ways are put away.

Lachowski et al. [22] have discussed the various distributed tree-building algorithms like distributed bellman ford (DBF), shortest hop multipath (SHM) and depth-first search (DFS) in a wireless sensor network. In this paper, the authors have additionally proposed an energy-efficient distributed tree building algorithm that relies upon the bellman ford distributed algorithm to keep up the required features. For example, scalability, resilience is appropriate for wireless sensor network, implies that the algorithm must develop a tree even in the loss of messages and node failure. The main objective of this algorithm is to diminish the communication overheads of the DBF and making it a versatile solution to maintain the quality of the tree.

Tree structures are commonly associated with sensor frameworks of IoT. Qie et al. [23] also have proposed another efficient tree-based self-organizing protocol (ETSP) for IoT based sensor networks. The primary aim of this protocol is to maintain energy consumption and network lifetime by building up a tree-based framework quickly. ETSP categorized nodes into two forms: (1) network nodes and (2) non-network nodes.

At the start of the protocol, there is just a root node with hop count zero. At that point, the root node looks through a child node by communication through the message. After getting the message, the neighboring non-network nodes record the data and utilize various metrics, for instance, child node quantity, residual energy, hop count and communication distance between the nodes to determine the sink node. During data transmission sink node is dynamically reselected because the sink node consumes more energy as compared to other nodes.

Concerning emergency services of IoT innovation, a basic issue is to provide an effective and robust information collection system. The solution proposed in the present techniques is to build a spanning tree over the IoT system and retrieve information using the tree [24]. The inadequacy of these techniques is that they do not consider the likelihood of device mobility or failure. In these instances, the tree is divided and it is difficult to transmit basic information on schedule to the base station. To mitigate this issue, Samad et al. [25] have proposed another reliable spanning-tree building algorithm based on an artificial bee colony method to produce appropriate trees. The algorithm uses various metrics, for example, a number of hop count, remaining energy of the devices and their mobility probabilities to assess the propriety of the trees. In addition, the algorithm produces a number of trees rather than a solitary one. These trees are organized by their preferences and used in sequence to collect information.

Cluster Based Mechanism

In this mechanism, the concerned network is divided into numerous clusters or groups. Each cluster comprises a number of sensor nodes. One specific node is chosen for each cluster, which is recognized as the head of the cluster. The primary objective of the cluster head node is to aggregate the information [26, 27]. This will reduce the overhead bandwidth as a number of transferred packets are less. Figure 6, clarifies the design of data aggregation in cluster based mechanism [28]. The concept of minimizing energy consumption through the use of aggregation function in the cluster head and sink is studied by Mantri et al. [29]. In their work, they have proposed bandwidth efficient cluster-based data aggregation technique using heterogeneous nodes with different energy levels. This technique utilizes the notion of data correlation within the packet to apply the aggregation function to the information produced by the sensor nodes. Using the random function, random information is generated by each node between 0 and 1. A cluster head is considered to be a node with maximum energy and a node occupied with a maximum number of neighbor nodes in one hop. Effectively, these techniques improve the usage of bandwidth and energy consumption but result in reduced throughput.

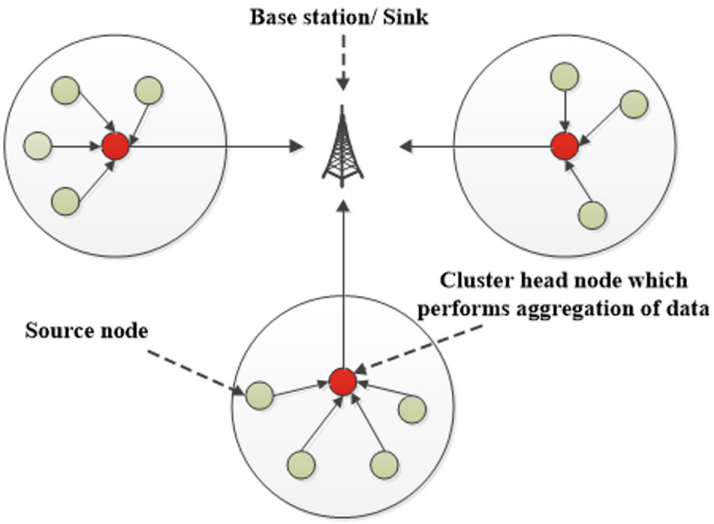


Fig. 6. Data aggregation using cluster-based mechanism [28].

To prevent the selection of inaccurate cluster heads leading to the overlap of communication coverage between clusters and an unequal distribution in energy consumption, the Jia et al. [30] have suggested an adaptive energy-optimized clustering algorithm that maintained the network energy consumption by dynamically selecting the cluster head node. The technique suggested in this paper overcome the energy consumption discrepancy, reduces the data redundancy in transmission, decreases energy consumption and expands the network lifetime.

Mohapatra et al. [31] studied that data reliability is accomplished by applying fault-tolerant protocols. Most of the studies are based on the stable cluster head scheme. This is impractical and could have unpredictable effects on the failure of the cluster head. In their work, they have proposed a dynamic cluster head scheme, where cluster head is likely to create errors in the network like other nodes. Using the remaining energy and sensor measurements, the LEACH protocol is further altered to integrate intelligent dynamic cluster head selection at the end of each round. This guarantees minimum power consumption and provides an environment-friendly model for smart cities. An effective dissemination scheme is also discussed in the paper to promote the achievement of the network worldwide perspective among all cluster heads at the end of each round.

Under the current network structure, large scale connectivity to IoT devices leads to system overload and low energy efficiency usage. Zhao et al. [32] have discussed these issues by considering the scenario of large scale IoT devices access and proposed an improved K-means algorithm based on distributed dynamic cluster head choice and clustering scheme.

Centralized Based Mechanism

In this process, each node sends data towards the main node through the shortest route. All the sensor nodes send information to a powerful node among all other nodes. This powerful node is referred to as a header node. The primary objective of this node is to aggregate the whole data and convert it into a single packet for transmission. Due to the massive amount of data being transferred, this strategy suffers from the issue of heavy data traffic. The centralized data aggregation mechanism structure is depicted in Fig. 7 [33].

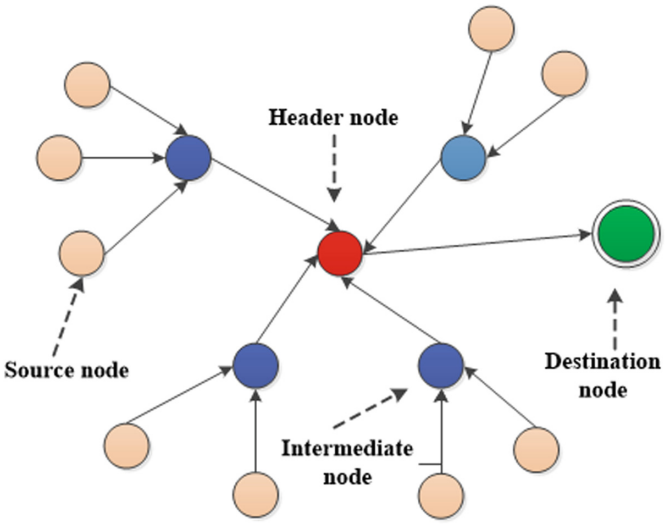


Fig. 7. Data aggregation using centralized-based mechanism [33].

Zhu et al. [34] have proposed a distributed service-oriented architecture to gather information from multiple data nodes which are common to many IoT applications. Each producer provides a service for their products and in this architecture, the gathered data is stored in a data node by itself. This method is scalable in view of the reality that each query node has a duty with respect to its own products and that each data node has a duty with regard to the data collected individually of anyone else.

Discussion

The paper listed in this section are categorized into three classifications; tree-based, cluster-based and centralized based. Constructing an energy-efficient tree is a significant problem in a tree-based mechanism. Most of the papers considered the energy consumption and network lifetime issues but other important features such as data accuracy, heterogeneity, and security and so on, still need to be addressed in order to extend the lifetime of the network.

In a cluster-based mechanism, most articles are about how to reduce the traffic load by dynamically selecting the cluster head node, how to reduce energy consumption and

improving the lifetime of the network. These papers, however, do not consider the problem of latency.

Furthermore, two articles are assessed which are based on a centralized data aggregation mechanism. These methods centrally aggregate data from several data nodes, offering better security and flexibility but suffering from a single point of failure. Table 1 summarizes the main pros and cons of the discussed data aggregation approaches.

Table 1. A summary of the pros and cons of the approaches under discussion.

Data aggregation approach	Pros	Cons
Tree based structure	• Reduces energy usage • Enhance data reliability and precision throughout the network • High network lifetime • Low traffic load	• Less Secure • Without taking node heterogeneity into consideration • Less attention to latency
Cluster based structure	• Efficient load balancing and effective use of resources • CH can set the nodes to sleep mode for saving energy	• Less attention to latency • Less secure, an attacker can obtain information directly through CH
Centralized based structure	• High security and flexibility	• Low fault tolerance

2.2 Probability Based Approaches

Probability models provide approximate answers to the queries. This type of model helps to identify the hidden variables. Hidden variables are the variables that are not observed directly. These models can be learned from historical data using a standard algorithm [35].

Mathematical Model based Data Collection

Several prior studies are based on mathematical models for approximate data collection in the IoT environment [36–39]. The algorithms that belong to this category covers these three basic steps: (1) Mathematical model is chosen to describe the correlation among the data and parameters of the selected model are predicted from the historical data, (2) In accordance with all parameters, local prediction model is constructed. Furthermore, for the construction of the global model, every one of the parameters of the local model are transferred to the sink, (3) after the construction of local and global model, there is no need to transfer the recently acquired sensor data that is anticipated by the local model just the non-anticipated data need to be transferred to the sink, after that with the help of global model, sink evaluate the sensor data [37]. The primary difficulties of such data collection methods are the way in which the local and global models are developed and maintained, so that they are constantly significant.

Deshpande et al. [38] have suggested a model of statistics prediction based on Gaussian Multivariate distribution to historical sensory information. It is not necessary

to transmit sensory information with greater confidence in estimation to the sink. In their research work, they also examined how to develop a resource consumption optimization query plan. However, in order to ensure efficiency, it does not consider network dynamics and still needs a big quantity of historical information. In the meantime, since it relies on historical data, the model cannot detect unusual occurrences.

Wang et al. [39] have discussed that the approximate data gathering is a smart decision in numerous applications of WSN because of the limitations in transmission capacity and energy budget. In their work, they have focused on an efficient approximate data collection method with predefined error constraints in the network. The main concept of this method is to partition the network in the form of clusters, detect local approximation model on each cluster head and conduct an approximate global information collection on sink node based on model parameters transferred by the cluster head. In this paper, a linear regression model is preferred rather than Gaussian distribution to depict a node temporal correlations of sensory information and a correlation graph is used to represent the spatial correlation of various cluster nodes. Just the supervisory nodes of each cluster chosen from the base predominant set are in charge of revealing information to the sink.

Li et al. [40] proposed an energy-efficient K-coverage algorithm based on a probability driven mechanism for building a coverage model using node positions. In their work, they also considered the issues of planning low energy nodes, balancing energy consumption and optimizing the energy resources.

In applications for medical services, an adaptable scheme for mobile data collection is proposed by Schobel [41]. Such a scheme supports techniques of accumulation of data based on the model. In addition, the detail description of algorithms has not been given.

Hao et al. [42] have outlined a probabilistic algorithm based on model activity to estimate trajectories of vehicles using information from mobile sensors and understanding of vehicle kinematics. The suggested model examined all necessary model activity sequences between successive mobile sensor information points. The activity sequence was evaluated, subject to maximizing the probability function and a detailed direction of vehicle velocity would be rebuilt as needed. Since numerous directional data are evaluated as opposed to being recovered from the sensor nodes, it saves a lot of energy and transmission expenses.

Discussion

Most of the algorithms listed in this section attempt to capture the correlation between the data through the use of probabilistic data approximation models like Gaussian distribution, linear regression and so forth. The primary goal of these algorithms is to save energy by predicting the sensed value without transmitting it. Though, all these methods have some drawbacks. First of all, the models really are not that optimal to define clearly the complex correlation between the sensory data. With the wide utilization of WSN and IoT technologies, the devices controlled by them are becoming increasingly complex and the data correlation extracted from the devices is also quite complex. So, we cannot consider a particular model for data collection. Second, they bring additional communication expenses to ensure the accuracy of the prediction model and to maintain the stability of local and global prediction models.

2.3 Compressive Sensing Based Approaches

Minimizing energy consumption in the IoT environment is a major challenge. A compressive sensing approach has been successfully applied in developing an efficient collection of data. Data compression is an important method for reducing the quantity of data to be sent across the network. It also maintains the precise reorganization of sensory information at the aggregation point. Compressive Sensing based approaches are categorized into three forms; (1) Conventional compression, (2) Distributed source coding and (3) Distributed compressive sensing [43].

Conventional Compression

Conventional compression methods involve explicit information communication between the sensors in order to minimize the correlation during information collection. This is necessary for each sensor to conduct complicated computations and the compression of information depends upon the routing approaches. Distinct routing approaches can receive distinct compressed information [44]. A conventional method of compression takes on a particular data structure and therefore involves communication between sensor nodes. In the coding strategy of joint entropy, nodes use transmitted data to encode their measurements. If the information can be transmitted through the encoding process, sensor nodes can cooperate in the transformation to make better use of correlation, for example, by using the gossip based method used by Zheng et al. [45] in their work. This strategy has two primary difficulties. First, compression efficiency is strongly affected by the route. In order to attain a high compression ratio, it is essential to optimize both data compression and routing together, as demonstrated by NP-hard. Second, compression of structure sensitive data leads to communication overheads, making such schemes inadequate.

Distributed Source Coding

Distributed source coding is one of the capable techniques for sensor networks that refers to the compression of the several correlated sensor outputs that do not interact with one another and jointly decoded these compressed data at the sink. The notion of entropy is necessary to clarify the concept behind the distributed source coding [46].

The primary objective of distributed source coding is to decrease complexity at nodes level and use correlation at the sink node. After separately encoding the sensor measurements, each node normally sends the coded signal through the shortest route towards the sink. It works well for static patterns of correlation. Though, if patterns changes, the estimate precision will be significantly impacted.

Aktas et al. [47] have proposed a decoding delay distributed source coding compression (D-DST) scheme. Basically, D-DST is a novel methodology that fundamentally improves the old DST by using the decoding delay concept in efficient data compression. This allows the optimum correlated part of the sensor datasets to be used during the evaluation of the event, which helps to minimize energy usage. In this scheme, the entire network is divided in the form of clusters where the cluster head transmits their uncompressed data conveying edge information and cluster nodes send the compressed data. After that sink performs the decoding of compressed and uncompressed datasets together and then on the basis of decoded signals, the event signal is reconstructed. In addition to effective data compression methods, D-DSC also

has secure and energy-efficient protocol specifications for event evaluation and communication applications in WSN.

Distributed Compressive Sensing

The compressive sensing concept is derived from the area of signal processing. It can rebuild small or compressible signals from a minimal amount of samples without needing any prior understanding of the signal composition [48].

Li et al. [49], suggested a matrix in their work that is constructed in a distributed way to compress the sensory information during data collection. The work considers the three main steps. First, on the basis of identification number each node produces a random vector and the random seed is transmitted through the sink. Second, by multiplying their sensed values and random vector, a fresh data vector is acquired for each sensor. At last, the sink calculates the random vectors to produce a random matrix depending on the random seed and node identification number.

Compression sensing and clustering algorithms depending on diagonal matrices were suggested by Zhang et al. [50]. First of all, the network is portioned in the form of clusters. After that cluster nodes send the sensed values towards the cluster head and then cluster head generated estimations of compressive sensing. At last, for regeneration, these estimations are sent to the base station.

The JSM-2 model has been implemented by Wang et al. [51] for information compression in sensor networks, in which, JSM is short of the Joint Sparsity Model. There is three distinct joint sparsity model, such as: JSM-1, JSM-2 and JSM-3, according to the distribution theory of compression sensing.

Approximate information collection algorithm depending on compression sensing is also suggested by Nguyen et al. [52]. First of all, the algorithm chooses the number of the necessary readings, marked by M, as per the remoteness of sensor information using compressive sensing methods. After that, for further regeneration, M number of paths are selected to route and aggregate the necessary readings towards the sink. The work was based on the premise that sensory data is known to be sparse. Furthermore, the repetitive information is likewise incorporated into the compressed data, as the random walking method often involves the same sensor.

Discussion

From the last decade, various methods have been adopted to resolve the energy constraints and for increasing the lifespan of the IoT applications including the newly implemented IoT energy harvesting system, ultra-low power sensor systems and so forth. So, in this section, we focus on data compression algorithms with the aim of reducing information redundancy. The main objective of compressive sensing information collection algorithms is to reduce the size of the sensory information matrix in accordance with user demands as far as feasible. When sensory information matrices are restricted in certain subspaces, then these methods are very efficient and reliable but such truth in all cases is not real and seems impractical in WSN and IoT framework. Although, if the above reality is true, the sparsity of sensory data is also very difficult to achieve, so that it is not possible to theoretically derive the compression rate of these algorithms.

2.4 Mobility Based Approaches

Mobility in IoT network is helpful in data collection, as it has a number of benefits including excellent connectivity, reliability and power effectiveness, which allow the maximization of network lifetime, as well as the reduction of latency in the network. Even though mobility offers significant advantages, it also suffers from various challenges such as secure transfer of information, power management in mobility, location identification, contact detection, and so forth [53]. To overcome these challenges, several methods have been suggested over the past few years based on distinct kinds of mobility architecture such as static sensor nodes with mobile sink architecture, mobile nodes with static sink and hybrid of both.

Static Sensor Nodes and Mobile Sink

In static sink architecture, nodes near to the sink suffered from energy depletion problems resulting in the disconnectivity of the network. In order to resolve this issue, a mobile sink scheme is the best solution. It solves the problem by implicitly maintaining the burden and moving towards every node for data collection [54]. Authors have suggested various methods to plan the use of mobile sink for effective and fruitful information collection in sensor networks [55–58]. However, sink mobility planning is a significant problem and can be widely categorized into two classifications: (1) random and (2) controlled sink scheduling [55]. Even though it is easy to implement a random movement scheme but it constitutes an excessive delay in data collection. However, in the case of controlled mobility, the trajectory of the sink depends on the predefined location or special points like rendezvous points in the network.

Sharma et al. [56] have proposed a rendezvous based routing protocol (RRP) that cover the necessity of energy efficiency and minimum latency in the network. In RPP, a meeting region is constructed in the center of the network and a tree is formed within that region. The protocol contains two different methods of transmitting data. In the first method, the tree is coordinated in the direction of the sink and source nodes transmit information through this tree to the sink. Whereas, in the second method, the sink communicates its position to the tree and source nodes get sink position from the tree and directly communicate to the sink.

In order to improve the network lifetime with mobile sink, Zhao et al. [57] have proposed a tree-based heuristic control algorithm recognized as MLS i.e. minimum load set algorithm. MLS formed the tree starting from the root node and at each iteration, it adds an additional node that is slightly similar to Dijkstra shortest path tree algorithm. The primary distinction is that, at each phase of MLS the added node does not need to maintain the shortest path among feasible nodes but should prevent those nodes that already suffered from the heavy load.

Most of the studies based on single sink data collection issues [56, 57], there is very less consideration to multiple sinks. Fitzgerald et al. [58] discussed that the existing data collection approaches have very little impact on newly developed applications due to the emergence of IoT. In specific, the present move towards fog computing, where command, calculations and processing are shifted to nodes near the network border, leads to the requirement to collect data at multiple locations instead of a single one, generally considered in WSN data collection algorithms. In their work, they proposed a

mixed integer programming methodology and algorithm relating to the issue of optimized energy scheduling and multi sink integration as well as joint integration and distribution of sensor information in the IoT environment.

In recent times a lot of attention has been given to unmanned aerial vehicles (UAV) or drones in the IoT environment. Due to their high speed, they are applicable to use in various non-delay tolerant IoT applications [59].

Mobile Sensor Nodes and Static Sink

The special feature of this architecture is the movable sensor nodes. In the latest years, this strategy has been the topic of much research [60]. Because the nodes are movable, this architecture significantly decreases the number of sensor nodes to be deployed. It supports good coverage of the network. This design also enables a healthy power usage at nodes level and a substantial amount of information gathered by the sink.

A mobile wireless sensor network is an auto-configuring and auto curing network consisting of movable sensor nodes linked wirelessly to create an autonomous topology. An excellent network coverage guarantees safe interaction, increases network accessibility, reduced power usage and, as a result, greater life of sensor nodes. In mobile WSN, various models for mobility have been taken into account for determining the various activities of the nodes [61].

Wang et al. [62] have discussed the data collection and dissemination issues in Internet of Vehicles (IoV) network. Basically, the reliable vehicular infrastructure depends on precise and timely procurement and dissemination of traffic information. To accomplish this, the study is mainly concentrated on enhancing mobility designs and connectivity outcomes.

Mobile Sensor Nodes and Mobile Sink

In this framework, mobility is taken into account at both the node and sink level. This structure has been applied in various research projects in science and industry. For example, this structure was introduced in Kenya as a part of Zebra monitoring operations, where sensors were mounted on Zebras and sink was placed on the vehicle [63]. This initiative was one of the first research to concurrently consider the mobility of nodes and sinks in the sector of environmental surveillance. Unique GPS collars attached to the wild Zebras and all their information sent to their neighbors until the base station ultimately receive their own information. This is an efficient approach but has two significant disadvantages for business farms. Firstly, the price is high, since every animal requires a GPS collar and secondly, updating data requires moving the vehicle around. To solve the second issue, Ayele et al. [64] have suggested the integration of low power wide area (LPWA) and opportunistic networks. In their work, they have introduced a dual service IoT network architecture.

In the past sixty years, technologies for the animal location have evolved substantially. Animal tracking strategies depending on GPS are now widely accessible. However, current systems have a number of limitations, mainly linked to the communication of cellular information and economic costs, making monitoring of all animals in a group impossible [65].

Xu et al. [66] also suggested using WSNs with UAV aid in wildlife regions to monitor animals. They have developed a model in which UAV moves towards the cluster head node for the purpose of data collection. They proposed a route scheduling

strategy relying on a Markov decision-making system model that maximizes the value of information and reduces communication distances.

Discussion
The distinct architecture studied in this section has its own pros and cons, mainly because the layout of these architecture depends on the objectives that we have set. Otherwise, the number of devices deployed in the wide area of concern is high in the case of large scale wireless sensor networks. In IoT applications, where the devices are movable, mobility in the network plays an important role to efficiently collect data from the overall network. Mobile WSNs are more flexible than existing WSN, since devices can be implemented in any situation and are capable to deal with fast topology changes.

2.5 Overall Comparison

The major pros and cons of the data collection approaches for the above mentioned four categories are discussed in Table 2.

Table 2. Comparison among discussed data collection approaches.

Approaches	Pros	Cons
Data aggregation approaches	• It helps to improve the quality and reliability of data obtained through the entire network • It helps to reduce redundancy that occurs in data collected from nodes. • It provides efficient load balancing and effective use of resources	• Less secure because the attacker can attack directly to the aggregator node • Less attention toward latency and heterogeneity
Probability based approaches	• It helps to save energy by transmitting only partial sensor values • The temporal and spatial correlation between sensor data is taken into consideration	• There is a bunch of in-network interactions involved in determining parameters of predictive models and ensuring consistency between local and global models • In general, the mathematical model is too ideal
Compressive based approaches	• The compression ratio can be adjusted as per the requirements of users • Efficient when the matrix of sensor data is sparse	• Very difficult to obtain the sparsity of sensor data • All algorithms have a fixed rate of global data loss
Mobility based approaches	• Efficient network coverage to collect data • Highly capable to deal with fast topology changes • It helps to reduce the routing distance by minimizing the hops between origin and its target in order to complete the collection of the packets	• Difficult to identify the efficient trajectory for the sink movement • The mobile nodes have the power to reconfigure themselves at broken points to restore the network. Nevertheless, this method raises the expenditure of energy

3 Future Direction: Open Research Issues and Challenges

Efficient data gathering is one of the major challenges in a smart city environment. In order to address this challenge, numerous efficient data collection methods have been suggested over the last few years. However, with the advent of IoT technologies, some unresolved issues still occur and must be examined for future research.

Firstly, the emergence of the IoT system is a manifestation of explosive progress in the amount of sensory information. As discussed in the above sections, a number of IoT devices connected to the Internet are increasing day by day. Such devices would generate a great amount of sensory data. Therefore, a number of new algorithms are needed to efficiently collect data. In view of the current methods, mobility in a network is one of the appropriate ways to construct efficient algorithms for managing huge data. Although, most of the current mobility based techniques are constructed for particular types of applications and do not support timely data collection. Therefore, a number of mobility based data collection methods are still needed to be explored in the future.

Secondly, since energy and resources are restricted to WSN and IoT devices, we simply need to transmit and gather the relevant set of data rather than the raw ones. The various probabilistic data approximation models like Gaussian distribution and linear regression are discussed in this chapter. These models only transmit the partial information to the sink, since the number of values can be predicted by the models. The key challenge of such predictive models of collecting data is how to build and maintain the local and global models so that they can be accurate all the time.

Thirdly, in data aggregation, time-bound is a major challenge that should be taken into consideration along with energy efficiency. During data aggregation, a considerable amount of time is taken by the aggregator node to collect, aggregate and transfer all the data to the base station. Although, the delay is a key limitation in some IoT applications. Therefore, an aggregation method should be implemented in such a way that together with energy usage it decreases delay.

Fourth, an IoT network has a variety of sensor nodes. For instance, some sensing sensors could be included in a smart traffic monitoring network such as digital eyes, GPS systems, smart traffic lights, and so forth. These sensors can collect various types of data such as multimedia data, scalar data and vector data. These varieties of data bring many challenges for data collections. But, the present work on sensor data collection focuses mainly on a single type of data and rarely addresses the issue of how to successfully capture multi types of sensors data. In order to overcome the above issue and to ensure that multi types of sensors data are gathered in a cooperative manner, the correlation among multiple types of sensory data should be deeply identified.

At last, data collections in respect of advanced applications deserve to be researched rigorously in the future also. For instance, visualization is a popular network application that offers the user a friendly interface for viewing and understanding the physical world. However, hardly anyone considers how to support these types of applications in current methods of data collection.

4 Conclusion

As energy efficient data collection is a key issue in smart cities using IoT, numerous effective and efficient algorithms for data collection have been reviewed. This chapter discusses the current data collection approaches, presents their main concept and analyzes their benefits and drawbacks. Finally, considering the future directions in existing data collection problems, some unsolved issues that are worth studying are also discussed.

References

1. Ray, P.P.: A survey on Internet of Things architectures. J. King Saud Univ.-Comput. Inf. Sci. **30**(3), 291–319 (2018)
2. Sheng, Z., et al.: Recent advances in industrial wireless sensor networks toward efficient management in IoT. IEEE Access **3**(1), 622–637 (2015)
3. Ahmed, E., et al.: Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel. Commun. **23**(5), 10–16 (2016)
4. Singh, S., Singh, P.K.: Performance investigation of energy efficient HetSEP for prolonging lifetime in WSNs. In: International Conference on Futuristic Trends in Network and Communication Technologies, pp. 496–509. Springer, Singapore (2018)
5. Talari, S., et al.: A review of smart cities based on the Internet of Things concept. Energies **10**(4), 1–23 (2017)
6. Burhan, M., et al.: IoT elements, layered architectures and security issues: a comprehensive survey. Sensors **18**(9), 1–37 (2018)
7. Cheng, S., Cai, Z., Li, J.: Approximate sensory data collection: a survey. Sensors **17**(3), 1–16 (2017)
8. Rathore, M.M., et al.: Exploiting IoT and big data analytics: defining smart digital city using real-time urban data. Sustain. Cities Soc. **40**(1), 600–610 (2018)
9. Randhawa, A., Kumar, A.: Exploring sustainability of smart development initiatives in India. Int. J. Sustain. Built Environ. **6**(2), 701–710 (2017)
10. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.): FTNCT 2018. Communications in Computer and Information Science, vol. 958. Springer, Singapore (2018)
11. Su, K., Li, J., Fu, H.: Smart city and the applications. In: International Conference on Electronics, Communications and Control (ICECC), pp. 1028–1031. IEEE, China (2015)
12. Jawhar, I., Mohamed, N., Al-Jaroodi, J.: Networking architectures and protocols for smart city systems. J. Internet Serv. Appl. **9**(1), 1–26 (2018)
13. Mohbey, K.K.: An efficient framework for smart city using big data technologies and Internet of Things. In: Progress in Advanced Computing and Intelligent Engineering, pp. 319–328. Springer, Singapore (2019)
14. Marjani, M., et al.: Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access **5**(1), 5247–5261 (2017)
15. Randhawa, S., Jain, S.: Data aggregation in wireless sensor networks: previous research, current status and future directions. Wirel. Pers. Commun. **97**(3), 3355–3425 (2017)
16. Avinash, R.A., et al.: Data prediction in Wireless sensor networks using Kalman Filter. In: International Conference on Smart Sensors and Systems (IC-SSS), pp. 1–4. IEEE, Bangalore (2015)

17. Wang, Q., Lin, D., Yang, P., Zhang, Z.: An energy-efficient compressive sensing-based clustering routing protocol for WSNs. IEEE Sens. J. **19**(10), 3950–3960 (2019)
18. Yu, S., Kim, J., Lee, J.: Lifetime improvement method using mobile sink for IoT service. In: Proceedings of the 10th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, pp. 145–150. ACM, New York (2013)
19. Akkaya, K., Guvenc, I., Aygun, R., Pala, N., Kadri, A.: IoT-based occupancy monitoring techniques for energy-efficient smart buildings. In: Wireless Communications and Networking Conference Workshops (WCNCW), pp. 58–63. IEEE, USA (2015)
20. Pandey, V., Kaur, A., Chand, N.: A review on data aggregation techniques in wireless sensor network. J. Electron. Electr. Eng. **1**(2), 1–8 (2010)
21. Virmani, D., Sharma, T., Sharma, R.: Adaptive energy aware data aggregation tree for wireless sensor networks. Int. J. Hybrid Inf. Technol. **6**(1), 26–36 (2013)
22. Lachowski, R., et al.: An efficient distributed algorithm for constructing spanning trees in wireless sensor networks. Sensors **15**(1), 1518–1536 (2015)
23. Qiu, T., et al.: An efficient tree-based self-organizing protocol for Internet of Things. IEEE Access **4**(1), 3535–3546 (2016)
24. Yin, B., Wei, X.: Communication-efficient data aggregation tree construction for complex queries in IoT applications. IEEE IoT J. **6**(2), 3352–3363 (2018)
25. Najjar-Ghabel, S., Yousefi, S., Farzinvash, L.: Reliable data gathering in the Internet of Things using artificial bee colony. Turk. J. Electr. Eng. Comput. Sci. **26**(4), 1710–1723 (2018)
26. Kumar, H., Singh, P.K.: Node energy based approach to improve network lifetime and throughput in wireless sensor networks. J. Telecommun. Electron. Comput. Eng. (JTEC) **9**(3), 79–88 (2017)
27. Lin, D., Wang, Q.: An energy-efficient clustering algorithm combined game theory and dual-cluster-head mechanism for WSNs. IEEE Access **7**(1), 49894–49905 (2019)
28. Kalantari, M., Ekbatanifard, G.: An energy aware dynamic cluster head selection mechanism for wireless sensor networks. In: Annual IEEE International Systems Conference, pp. 1–8. IEEE, Canada (2017)
29. Mantri, D.S., Prasad, N.R., Prasad, R.: Bandwidth efficient cluster-based data aggregation for wireless sensor network. Comput. Electr. Eng. **41**(1), 256–264 (2015)
30. Jia, D., et al.: Dynamic cluster head selection method for wireless sensor network. IEEE Sens. J. **16**(8), 2746–2754 (2015)
31. Mohapatra, A.D., et al.: Distributed fault diagnosis with dynamic cluster-head and energy efficient dissemination model for smart city. Sustain. cities Soc. **43**(1), 624–634 (2018)
32. Zhao, Y., et al.: Distributed dynamic cluster-head selection and clustering for massive IoT access in 5G networks. Appl. Sci. **9**(1), 1–15 (2019)
33. Kaur, S., Gangwar, R.: A study of tree based data aggregation techniques for WSNs. Int. J. Database Theory Appl. **9**(1), 109–118 (2016)
34. Zhu, T., et al.: An architecture for aggregating information from distributed data nodes for industrial Internet of Things. Comput. Electr. Eng. **58**(1), 337–349 (2017)
35. Ferrari, S., Zhang, G., Wettergren, T.A.: Probabilistic track coverage in cooperative sensor networks. IEEE Trans. Syst. Man Cybern. **40**(6), 1492–1504 (2010)
36. Chu, D., et al.: Approximate data collection in sensor networks using probabilistic models. In: 22nd International Conference on Data Engineering (ICDE 2006), pp. 48. IEEE, USA (2006)
37. Wang, L., Deshpande, A.: Predictive modeling-based data collection in wireless sensor networks. In: European Conference on Wireless Sensor Networks, pp. 34–51. Springer, Berlin (2008)

38. Deshpande, A., et al.: Model-driven data acquisition in sensor networks. In: Proceedings of the Thirtieth International Conference on Very Large Databases, vol. 30, pp. 588–599. VLDB Endowment, Canada (2004)
39. Wang, C., et al.: Adaptive approximate data collection for wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **23**(6), 1004–1016 (2012)
40. Li, C., et al.: A novel energy-efficient k-Coverage algorithm based on probability driven mechanism of wireless sensor networks. Int. J. Distrib. Sens. Netw. **12**(4), 1–9 (2016)
41. Schobel, J., et al.: Towards flexible mobile data collection in healthcare. In: IEEE 29th International Symposium on Computer-Based Medical Systems (CBMS), pp. 181–182. IEEE, Ireland (2016)
42. Hao, P., et al.: Modal activity-based stochastic model for estimating vehicle trajectories from sparse mobile sensor data. IEEE Trans. Intell. Transp. Syst. **18**(3), 701–711 (2016)
43. Liu, X.Y., et al.: CDC: compressive data collection for wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **26**(8), 2188–2197 (2015)
44. Wu, X., et al.: An efficient compressive data gathering routing scheme for large-scale wireless sensor networks. Comput. Electr. Eng. **39**(6), 1935–1946 (2013)
45. Zheng, H., et al.: Data gathering with compressive sensing in wireless sensor networks: a random walk based approach. IEEE Trans. Parallel Distrib. Syst. **26**(1), 35–44 (2014)
46. Barcelo-Llado, J.E., Perez, A.M., Seco-Granados, G.: Enhanced correlation estimators for distributed source coding in large wireless sensor networks. IEEE Sens. J. **12**(9), 2799–2806 (2012)
47. Aktas, M., et al.: D-DSC: decoding delay-based distributed source coding for internet of sensing things. PLoS ONE **13**(3), 1–25 (2018)
48. Masoum, A., Meratnia, N., Havinga, P.J.: A distributed compressive sensing technique for data gathering in wireless sensor networks. Procedia Comput. Sci. **21**, 207–216 (2013)
49. Li, S., Da Xu, L., Wang, X.: Compressed sensing signal and data acquisition in wireless sensor networks and Internet of Things. IEEE Trans. Ind. Inf. **9**(4), 2177–2186 (2012)
50. Zhang, C., et al.: Dynamic clustering and compressive data gathering algorithm for energy-efficient wireless sensor networks. Int. J. Distrib. Sens. Netw. **13**(10), 1–12 (2017)
51. Wang, W., Wang, D., Jiang, Y.: Energy efficient distributed compressed data gathering for sensor networks. Ad Hoc Netw. **58**(1), 112–117 (2017)
52. Nguyen, M.T., Teague, K.A., Rahnavard, N.: CCS: energy-efficient data collection in clustered wireless sensor networks utilizing block-wise compressive sensing. Comput. Netw. **106**(1), 171–185 (2016)
53. Yarinezhad, R., Sarabi, A.: Reducing delay and energy consumption in wireless sensor networks by making virtual grid infrastructure and using mobile sink. AEU-Int. J. Electron. Commun. **84**(1), 144–152 (2018)
54. Gupta, N., Gupta, V.: A review on sink mobility aware fast and efficient data gathering in wireless sensor networks. In: International Conference on Advances in Computing, Communication, & Automation (ICACCA), pp. 1–4. IEEE, Dehradun (2016)
55. Zareei, M., et al.: Mobility-aware medium access control protocols for wireless sensor networks: a survey. J. Netw. Comput. Appl. **104**(1), 21–37 (2018)
56. Sharma, S., et al.: Rendezvous based routing protocol for wireless sensor networks with mobile sink. J. Supercomput. **73**(3), 1168–1188 (2017)
57. Zhao, H., et al.: Energy-efficient topology control algorithm for maximizing network lifetime in wireless sensor networks with mobile sink. Appl. Soft Comput. **34**(1), 539–550 (2015)
58. Fitzgerald, E., Pióro, M., Tomaszewski, A.: Energy-optimal data aggregation and dissemination for the Internet of Things. IEEE IoT J. **5**(2), 955–969 (2018)
59. Liu, X., et al.: Optimizing trajectory of unmanned aerial vehicles for efficient data acquisition: a matrix completion approach. IEEE IoT J. **6**(2), 1829–1840 (2019)

60. Mohamed, S.M., et al.: Coverage in mobile wireless sensor networks (M-WSN): a survey. Comput. Commun. **110**(1), 133–150 (2017)
61. Jain, M., Patle, V.K., Kumar, S.: Performance of mobility models with different routing protocols by using simulation tools for WSN: a review. Int. J. Adv. Res. Comput. Commun. Eng. **4**(1), 57–61 (2015)
62. Wang, J., et al.: Internet of vehicles: Sensing-aided transportation information collection and diffusion. IEEE Trans. Veh. Technol. **67**(5), 3813–3825 (2018)
63. Juang, P., et al.: Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with ZebraNet. ACM SIGARCH Comput. Architect. News **30**(5), 96–107 (2002)
64. Ayele, E.D., Meratnia, N., Havinga, P.J.: Towards a new opportunistic IoT network architecture for wildlife monitoring system. In: 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5. IEEE, France (2018)
65. Maroto-Molina, F., et al.: A low-cost IoT-based system to monitor the location of a whole herd. Sensors **19**(10), 1–15 (2019)
66. Xu, J., et al.: Animal monitoring with unmanned aerial vehicle-aided wireless sensor networks. In: IEEE 40th Conference on Local Computer Networks (LCN), pp. 125–132. IEEE, USA (2015)

A Review on Hybrid WSN-NGPON2 Network for Smart World

Meet Kumari[1(✉)], Reecha Sharma[1], and Anu Sheetal[2]

[1] Punjabi University, Patiala, Punjab, India
meetkumari08@yahoo.in
[2] Guru Nanak Dev University Regional Campus, Gurdaspur, Punjab, India

Abstract. The emerging wireless sensor network (WSN) is a wireless network of low-power, high-resolution nodes for sensing the environment. WSN, a future technology, has been deployed for numerous smart world applications such as smart agriculture, homes, cities, transportation, hospitals etc. But, the presence of limited bandwidth, small coverage and the limited energy sensor nodes retards the lifetime of the WSNs. Thus to remove all these shortcomings of sensor network at a high data rate over long reach distance, the passive optical network (PON) plays an important role for WSNs. Further, an attractive and energy-efficient next generation passive optical network stage 2 (NG-PON2) provides a higher data rate and better quality of services at a low cost. Furthermore, the hybrid wireless sensor network- next generation passive optical network stage 2 (WSN-NGPON2) is a future proof energy efficient optical network for a smart world. In this chapter, the hybrid WSN-NGPON2 network is studied and compared with other PON architectures like gigabit passive optical network (GPON), ethernet passive optical network (EPON), next generation passive optical network stage 1 (NG-PON1) etc. In addition of describing the key challenges of hybrid WSN-NGPON2 network, this chapter also presents the various applications in different smart fields. It is concluded that although hybrid WSN-NGPON2 network has challenges, but also it provides the lots of numerous advance applications for smart world.

Keywords: Ethernet passive optical network (EPON) · Gigabit passive optical network (GPON) · Next generation passive optical network stage 2 (NGPON2) · Passive optical network (PON) · Wireless sensor network (WSN)

1 Introduction

1.1 Introduction to WSN

In today smart world, a wireless sensor network (WSN) has become the spotlight and the integral part of our daily life due to its most attractive core infrastructure to implement the smart services in military surveillances, healthcare, environment science, grid, agriculture, transportation, city, home etc. [1].

A WSN includes numerous advantages such as evasion of installation, regular maintenance of wired communication cables, minimum power consumption, low cost, low complexity, high flexibility, high scalability, high risk tolerance, high environment adaptability etc. [2].

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 655–671, 2020.
https://doi.org/10.1007/978-3-030-40305-8_31

Figure 1 shows the basic WSN architecture. Here, a WSN consists of a huge number of energy-limited sensor nodes with base stations for real-time sensing and collecting data of different environment parameters as well as and monitoring the system [2]. Sensor nodes measures the analog signals and it typically consists of analog to digital converter (ADC) to transmit the signals by using radio frequency protocols. The base station utilizes a computer associated with a radio frequency transceiver to receive and decode the incoming signals. A WSN can use different types of topology such as star, mesh and hybrid star-mesh [3].

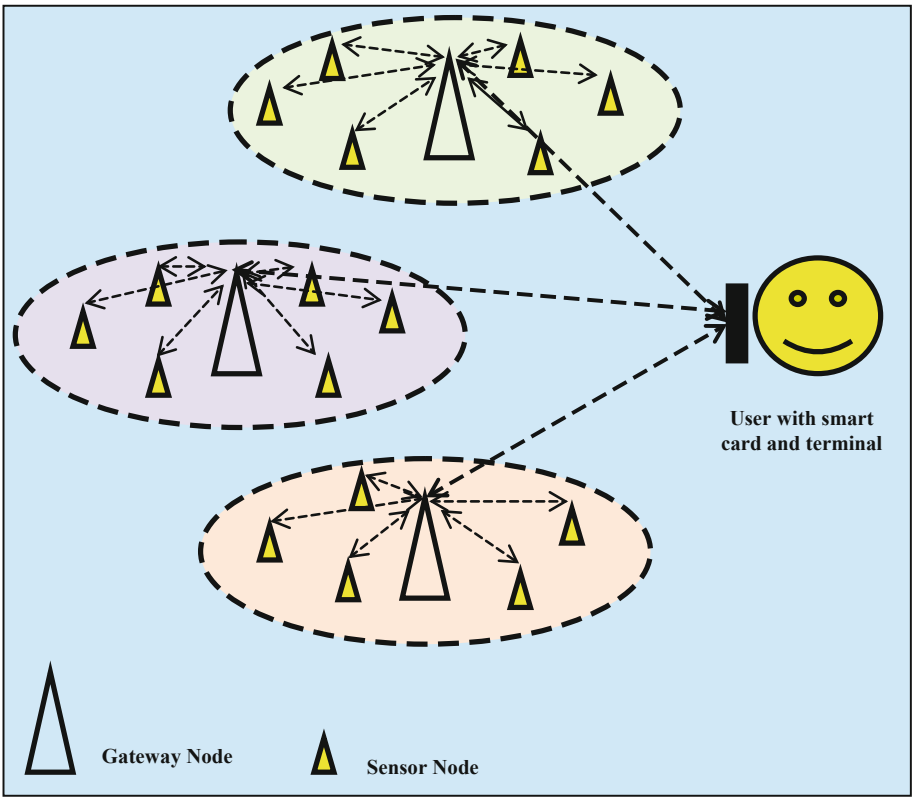


Fig. 1. WSN system architecture [3]

The ever increasing demands of high data rate applications such as ultra-high definition television, browsing, multimedia applications and various internet services require the gigabit per second (Gbps) data rate in near smart future. Furthermore, there should be high flexibility of data with high mobility. Thus, the wireless access network should target at wireless optical access network having low energy consumption. Passive optical network (PON) is an energy saving network which uses the passive components to saves energy for different applications. Out of various PON architectures the NG-PON2 is a future proof optical access network. The hybrid wireless sensor

network- next generation passive optical network stage 2 (WSN-NGPON2) is an innovative network that uses the advantages of both PON and wireless sensor nodes at high bit rate over long reach distance from rural to urban areas [4].

1.2 Introduction to PON

PON is a promising broadband access network which is used in different fiber to the x (FTTx) applications [5].

The PON architecture is shown in Fig. 2. It consists of an optical line terminal (OLT), optical distribution network (ODN) and many optical network units (ONUs). The OLT is located at central office (CO). The CO is connected to the splitter 1:N by fiber to split the incoming signals into N numbers of ONUs [5].

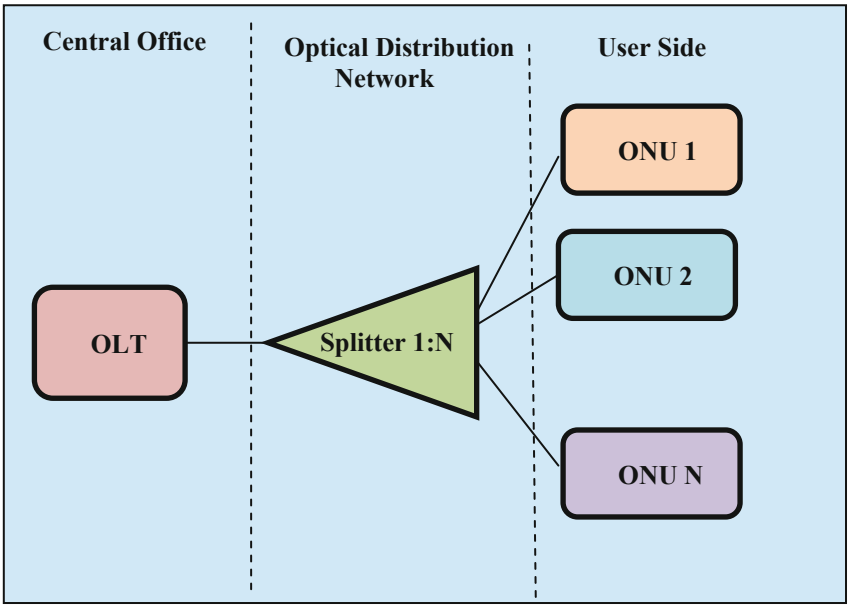


Fig. 2. PON architecture [5]

There are various PON architectures which have been developed by the International Telecommunications Union (ITU) and the Institute of Electrical and Electronic Engineers (IEEE). Figure 3 shows the PON generations. The various PON architectures are as follows: [5]

- Asynchronous Transfer Mode (ATM) PON or APON
- Broadband PON (BPON)
- Gigabit PON (GPON)
- Ethernet PON (EPON)
- Next Generation PON stage 1 (NG-PON1)
- Next Generation PON stage 2 (NG-PON2)

First generation PON: It is based on time division multiple access (TDMA) having bit rate of 1/1 Gbps (downstream/upstream) and 2.4/1 Gbps for EPON and GPON respectively.

Next Generation PON Stage 1 (NG-PON1): It is the upgradation of EPON to next generation (XG)-EPON and GPON to XG-GPON. It provides the high bandwidth and quality of services for future upgradation. It has maximum bit rate of 10/10 Gbps.

Next Generation PON Stage 2 (NG-PON2): It is the upgradation of NG-PON1. It consists of various multiplexing techniques such as time division multiplexing PON (TDM-PON), optical code division multiplexing PON (OCDMA-PON, wavelength division multiplexing PON (WDM-PON) and orthogonal frequency division multiplexing PON (OFDM-PON). It also consists of other hybrid multiplexing techniques such as WDM/TDM-PON, WDM/OCDMA-PON, OFDM/OCDM-PON, OFDM/WDM-POM etc. Out of all these multiplexing techniques, TDM/WDM-PON (TWDM-PON) has been selected as the base for NGPON2 by full service access network (FSAN) community [5].

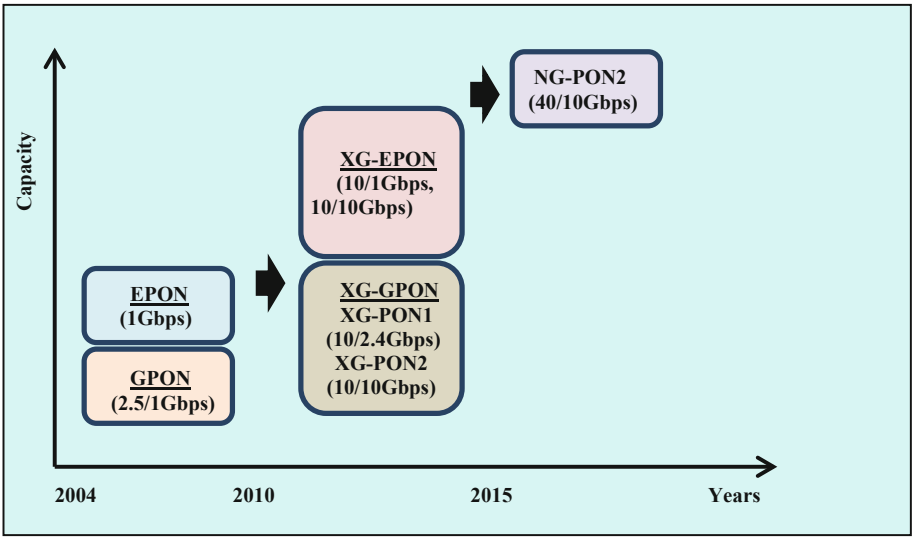


Fig. 3. PON generations [5]

1.3 Hybrid WSN-PON Networks

The various hybrid WSN-PON networks are shown in Fig. 4 [5].

WSN-EPON: It offers the bit rate of 1Gbps both for downlink and uplink transmission. It uses the 8B/10B line coding. The downstream wavelength is 1480–1550 nm while the upstream wavelength is 1260–1360 nm. It has 16 split ratio.

WSN-GPON: It offers the bit rate of 1 Gps for uplink and 2.4 Gbps for downlink. For GPON, the downstream wavelength is 1480–1550 nm while the upstream wavelength is 1260–1330 nm. It has 64 split ratio.

WSN-XG-EPON: It offers the bit rate of 10 Gbps for downstream while 10 or 1 Gbps for upstream. For this, the downstream wavelength is 1260–1280 nm while the upstream wavelength is 1575–1580 nm. It has 32 split ratio.

WSN-XG-GPON: It offers the bit rate of 10 Gbps for downstream while 10 or 2.5 Gbps for upstream. For this, the downstream wavelength is 1260–1280 nm while the upstream wavelength is 1575–1580 nm. It has 32 split ratio. The various hybrid WSN-PON architectures are shown in Fig. 4.

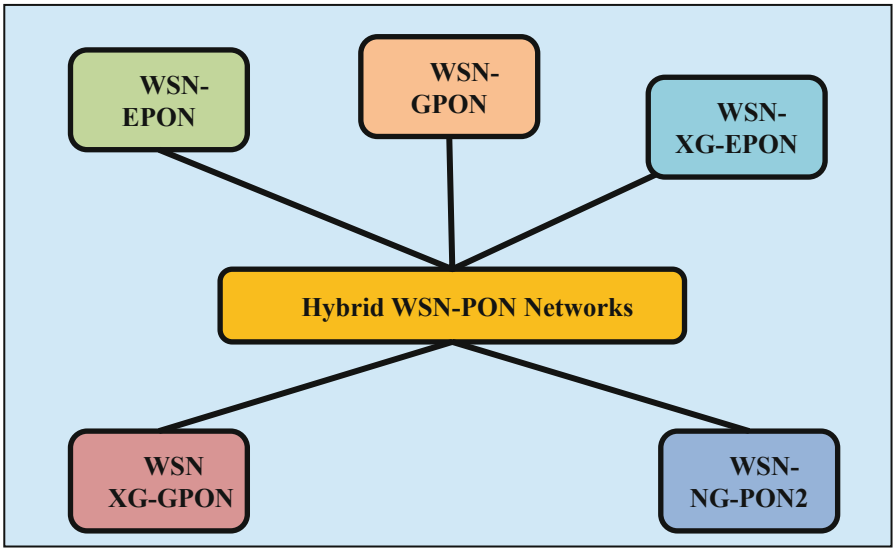


Fig. 4. Hybrid WSN-PON architectures

1.4 Hybrid WSN-NGPON2 Network

It offers the bit rate of 40 Gbps for downstream while 10 or 40 Gbps for upstream. For this, the downstream wavelength is 1596–1603 nm while the upstream wavelength is 1524–1544 nm. It has 256 split ratio [5]. This network has numerous advantages as compared to previous PON architectures such as easy upgradeability, scalability, flexibility, reliability and cost effectiveness for large number of users [6].

The hybrid WSN-NGPON2 tree-topology based network is shown in Fig. 5. It consist of single OLT providing FTTx and wireless sensor nodes providing WSN services which are connected to various ONUs. Here, the ONUs provides the two types of services viz. fiber to the home (FTTH) and different types of mobile sensor nodes at cluster heads (CHs) [7].

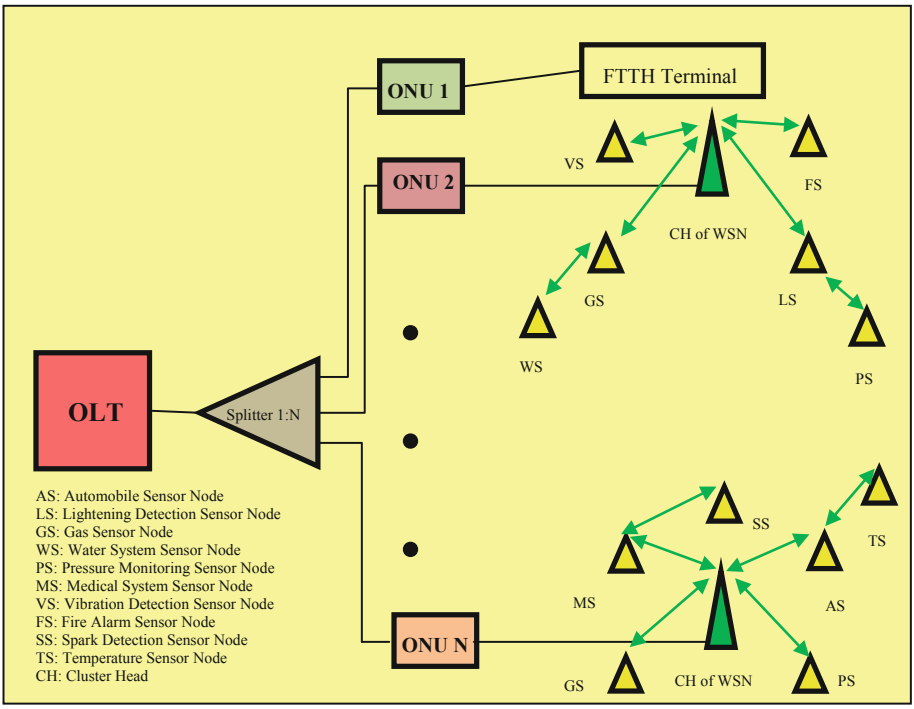


Fig. 5. Hybrid WSN-NGPON2 architecture

The protocol stack for WSN-PON has been shown in Fig. 6. The WSN consists of five layers same as open system interconnection (OSI) viz. physical, medium access control (MAC), network, transport and application. The network collects the energy of wireless sensors nodes and routes awareness, integrates the packets with network protocols and communicate efficiently. The protocol stack exchanges the information from one layer to another layer. Here, the physical layer works for frequency selection, frequency generation, data encryption, modulation and signal detection. The MAC layer is used for data multiplexing, detection of data frame and error control for ensuring point to point/multipoint connection. The transport layer is responsible for data flow maintenance. The application layer helps in sensing tasks with application software. The PON works on bottom two layers viz. physical and MAC layers of WSN protocol stack [8]. The various characteristics of hybrid WSN-NGPON2 architecture is shown in Fig. 7.

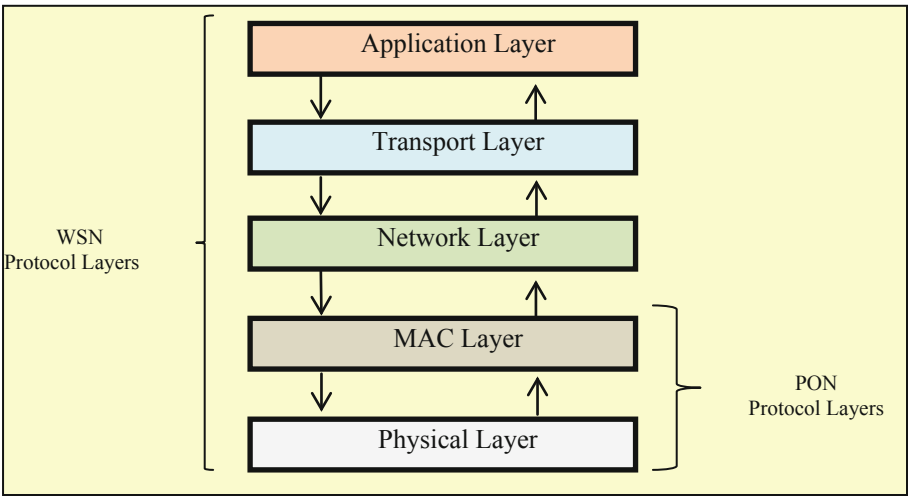


Fig. 6. Hybrid WSN-PON protocol stack

In this chapter, the contribution of hybrid WSN-NGPON2 network in smart world's applications to accomplish the requirements of next generation wireless networks has been studied. The Sect. 2 presents the literature review of various energy efficient passive WSNs Sect. 3 provide the major key challenges in hybrid WSN-NGPON2 network. Section 4 describes the applications of hybrid WSN-NGPON2 network in various smart fields. A general conclusion is drawn in Sect. 5.

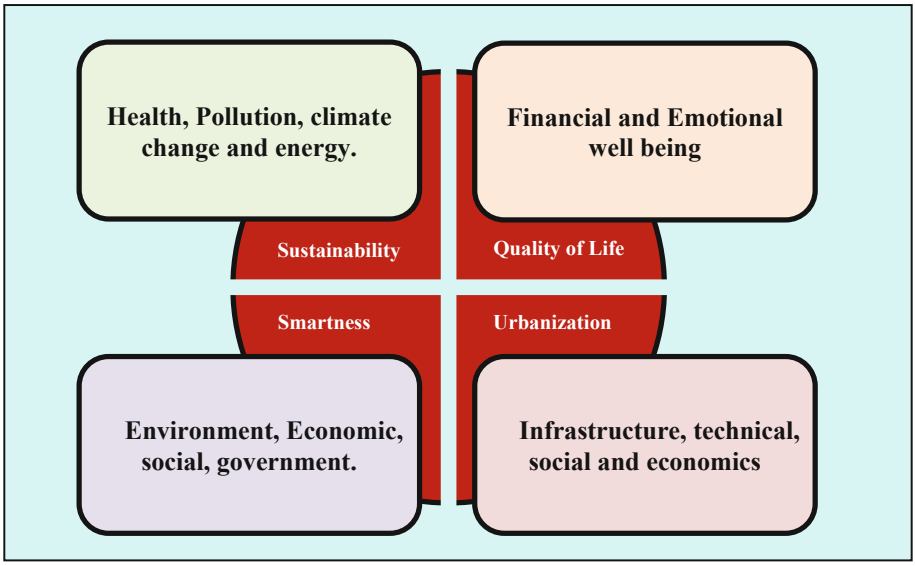


Fig. 7. Characteristics of hybrid WSN-PON architectures [9]

2 Literature Review

A comprehensive literature review has been presented on the energy efficient methods for passive WSNs at minimum cost is as follows:

S. No.	Author	Year	Literature review	Research gaps
1.	Y.-W. Peter Hong et al.	2016	In this paper, charging power allocation and beam pattern selection problems in the wireless passive sensor networks (WPSNs) are discussed. These problems are determined by mean square error (MSE) under prefect and imperfect channel state information (CSI). The result shows that using the block successive upper bound minimization (BSUM) technique, the MSE is reduced in imperfect CSI [10]	The proposed distributed WPSN network consists of directional antenna to obtain the desired information at sensor nodes. Also, the charging and channel gain should be high This may vary due to environment conditions like floods, earthquakes etc. of sensor nodes
2.	C.-H. Chang et al.	2016	In this paper, a bidirectional passive optical sensor network using add drop multiplexer has been presented with self-healing property. The result shows that the proposed network reduces the power usage, system complexity and recovers the optical connection. Also, this network is a reliable, flexible and easily maintained network [11]	Although the proposed network reduces the cost of system, but there is still the problem of input power supply
3.	Q. Yu et al.	2017	In this paper, WPSNs with improved sensor medium access control (IS-MAC) protocols has been analyzed. The proposed network minimizes the network load, energy consumption and enhances the performance throughput [12]	The IS-MAC protocols in WPSN are considered to minimize the energy consumption but not for delay and other parameters of network
4.	L. Kumar et al.	2017	In this paper, a WSN-PON network based on cluster to improve the transmission distance (10–20 km) under the diverse phase delay with 1:2 or 1:4 power splitter has been proposed. The result shows that bit error rate (BER) is improved at 0^0 and 90^0 phase delay as compared to other phase delay [13]	In future, the proposed network can be utilized for evaluating various data collection techniques for increasing the number of ONUs along with error correction techniques

(*continued*)

(*continued*)

S. No.	Author	Year	Literature review	Research gaps
5.	L. Kumar et al.	2017	In this paper, the bidirectional WSN-PON network has been demonstrated to handle the heavy traffic load using the M/M/1 queue theory as bandwidth algorithm to avoid the packets clash. The results shows that proposed scheme reduces the time delay increase the bandwidth utilization and handle the massive traffic load [14]	As the proposed network is suitable for EPON/GPON but can be further used for hybrid wired and wireless based on NG-PON2
6.	C.-H. Chang et. al.	2018	In this paper, passive sensor network using optical add drop multiplexer has been proposed. The result shows that maximum power penalty is around 6dB. The proposed network can easily reduce the fiber link failure with simple control management [15]	The cost of the proposed system is high at remote network.
7.	C. An et al.	2018	In this paper, two way cluster association (TWCA) algorithm in WPSNs has been proposed. The results show that the proposed scheme solves the association faults with simple operations by detecting sensor clusters. It also provides low consumption power and high accuracy [16]	The presence of noises in environment such as animal noises etc. creates multipath fading which can misguide the tracking and detection targets
8.	M. Akerele et al.	2019	In this paper, fiber wireless sensor network (Fi-WSN) has been proposed for cross layer service mechanism. The results shows that by reducing the delay at ONUs, the proposed network can be used for long reach PON under massive traffic conditions [17]	The network has various challenges such as channel and routing assignment and bandwidth variation between sensor nodes

From the literature review it is clear that various energy efficient techniques are used for WSNs but they have some limitations such as low battery life, data loss, delay, packet misunderstood and communication constraints. This reduces the network performance. Also, recently the WSNs showed the great importance in variety of smart applications such as healthcare, e-governance, agriculture, security and environment monitoring as they uses the simple design and low cost wireless technology. Thus, to overcome these shortcomings, NGPON2 can be used with WSNs. The hybrid WSN-NGPON2 will greatly improve the performance of network. This hybrid network can improve the sensor network performance by saving energy with passive components at 40 Gbps over more than 40 km transmission distance [18].

3 Key Challenges in Hybrid WSN-NGPON2

A number of challenges have been recognized when designing a hybrid WSN-NGPON2 network. These are as follows: [3]

3.1 High Data Quantity

The hybrid WSN-NGPON2 developed network needs to be efficient to handle the great amount of bidirectional data in network transmission. Also, there should be a synchronization of incoming and outgoing packets at transreceivers.

3.2 Network Robustness and Realistic Implementation

To maintain the network's robustness with large number of communication devices, the network must be redundant to avoid the high cost requirements. Also, the realistic implementation of Hybrid WSN-NGPON2 network is a major challenge for designer [9].

3.3 Power Deficiency

The commonly used battery based sensor nodes require regular recharge and maintenance. This is a very critical challenge for a wide network which have numerous sensors.

3.4 Design Maintenance Cost

The hybrid WSN-NGPON2 network has higher cost as compared to others analog based sensor networks. For this, the network design should be cost effective. This motivates for high probability of implementing WSN-NGPON2 in real world implementation. It also adds daily operational cost which should be minimum for sustainability of network in real world. This cost optimization of the network lifetime key in the smart world [9].

3.5 Data Security

Data security is another challenge in hybrid WSN-NGPON2 network in today life. It comes with price. As users communicates with each other through smart appliances. Thus, it is mandatory to manage the price of data from threads and eavesdrops. To transmit the sensitive information, the network must be highly secure by using advanced encryption standard (128-bit advance encryption standard) [9].

3.6 Failure Management

This is the another key challenge for the smart world network. The network failure includes the subsequent to natural such as earthquakes, tsunami, and cyclones etc. which causes the network and infrastructure breakdown. Thus it is necessary to overcome these failures to manage the smart world network back into normal

condition. Various failure management techniques can be used with minimal cost [9] (Fig. 8).

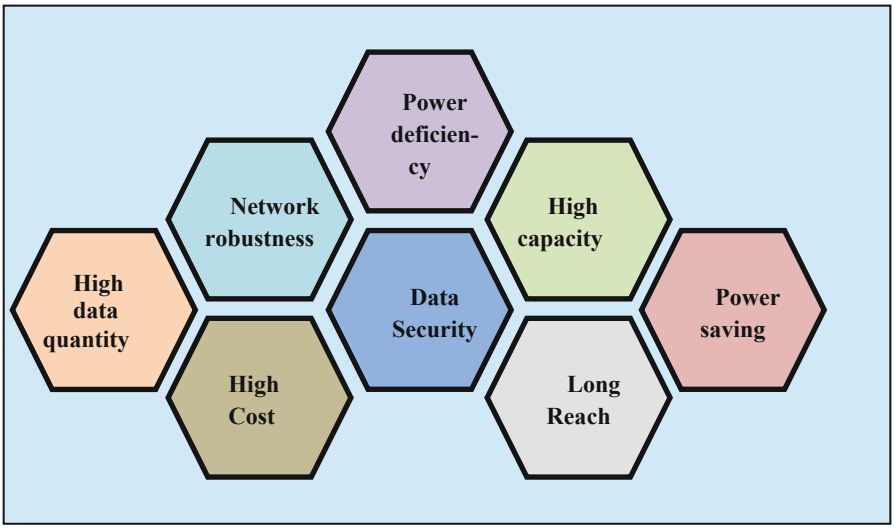


Fig. 8. Challenges in hybrid WSN-NGPON2 Network

- **High capacity:** The bit rate means high capacity of network is restricted by fiber nonlinearities such as self-phase modulation (SPM), four wave mixing (FWM) and cross phase modulation (XPM). It should be minimum as possible [5, 19].
- **Long Reach:** The long reach application of network is degraded by chromatic dispersion and low spectral efficiency in optical fiber cable [5].
- **Power saving:** For WSN-NGPON2, the power saving is a major challenge. This can be solved by point to point and virtual point to point techniques [5].

4 Applications of Hybrid WSN-NGPON2

The various quality of service (QoS) parameters for hybrid WSN-NGPON2 are delay, jitter, packet loss, bandwidth, throughput and routing protocol's performance. Based on these parameters the various applications of hybrid WSN-NGPON2 network are as follows: [20, 21].

4.1 Smart Healthcare

The hybrid WSN-NGPON2 network can be used for smart healthcare systems by using energy efficient wearable biosensors (medical sensor network). This network can

monitor the health of patients in real time. Further, to secure the patients' personal information a password can be implemented in real world [22].

Using hybrid wireless medical sensor network (WMSN) and NGPON2 i.e. hybrid WMSN-NGPON2 architecture support heath monitoring system with highly secure protocols. In the future, the protocols can be implemented in Internet-of Things and cloud computing [23] (Fig. 9).

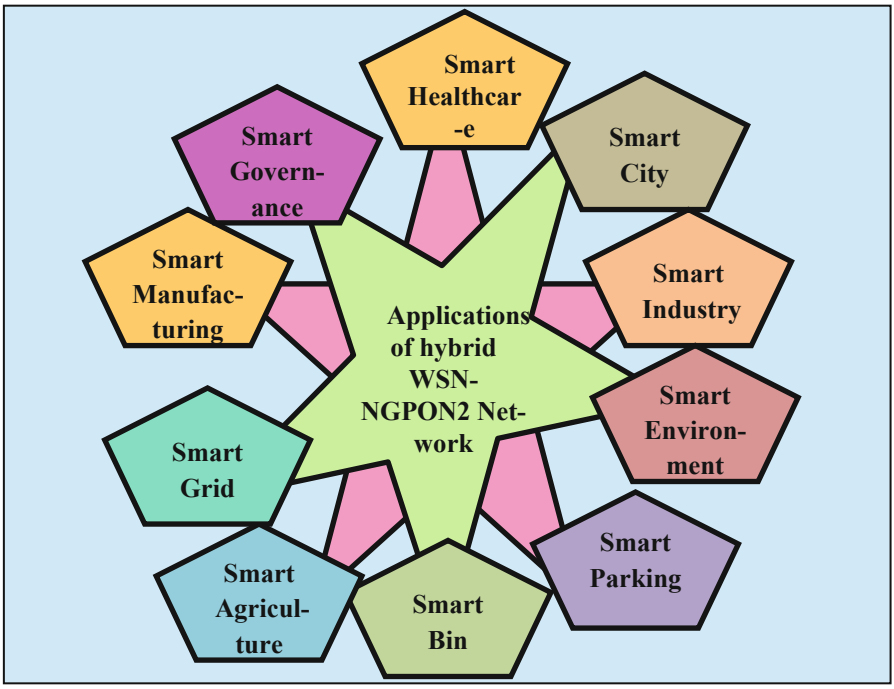


Fig. 9. Hybrid WSN-NG-PON2 applications

4.2 Smart City

A smart city is a place where services and networks are made flexible, sustainable, convenient and efficient with the use of digital technologies. In formal, a smart city is an innovative city that uses information and information technologies (ICTs) to improve the quality and efficiency of life from urban to rural areas by considering the economic, environmental and social needs.

As it has been predicted that in 2050, around 70% of world population will live urban areas and at present the cities are consuming 75% of world's energy and resources which causes to the production of 80% of greenhouse gases. This leads to make the concept of smart cities due to presence of negative impact on the environment. The smart cities will not only reduce the cost associated but also, minimize the

consumption of various environment resources like water, carbon emission, waste products and energy [24].

The number of the city facilities required with respect to city population calculated as follows: [24]

$$N_f = N_p(R_p/1Y)(1Y/D)(1H/N_c)(1D/H) \quad (1)$$

where N_f = number of facilities

N_p = population of city in millions
R_p = rate per person use in year/weak
Y = year
D = days per year
H = hours per day
N_c = customers per hours.

Smart Infrastructure and Building: Smart infrastructure and building includes smart systems such as transit, waste management, road, railway, communication, traffic light, street light, office space, water supply, gas supply, power supply firefighting, hospital, bridges, living apartments, hotels, digital library, economy etc. The smart infrastructure will be more efficient, secure and safe as compared to classic infrastructure. This will includes wireless sensors, firmware, software, smart grid etc. [24].

Smart Transpiration: Smart transportation includes global airway hubs, intelligent road networks, intercity railways, integrated and protected pedestrian paths for safe and reliable transportation. It also includes sensors in vehicles for antiskidding and collision avoidance to improve the safety of the network e.g. radio frequency identification (RFID) system, use to smart apps to hire and tracking taxies with exact location in mobile phones [24].

Smart Energy: Smart energy means 'Internet of Energy'. It includes smart power grids, power generation, optimum power consumption, efficient distribution and storage. The presence of information and communication technologies (ICT), green energy, clean energy, sustainable energy and renewable energy makes smart energy system. The backbone of smart energy is the use of smart grid in consumers and generators [24].

Smart Technology: Smart technology involves the renewable or green energy resources such as solar energy, wind energy etc. It also includes green buildings and neighborhood development societies like leadership in energy and environment design (LEED) and building research establishment environment assessment methodology (BREEAM) in US and UK respectively. Furthermore, smart sustainable resource management, communication infrastructure, state of art technology and social network & cyber physical system makes possibilities for smart technology [24].

4.3 Smart Industry

The industrial wireless sensor networks (IWSNs) can be used for smart industry through semiconductor fabrication applications and oil tankers in plants. Here, vibration sensors can be used to find the impending equipment failures. It will support high quality data with repairing and replacing the fault equipment in advance which will save the money and guarantee smooth operation in industries. The IWSN can be used for IoT manufacturing to lead the INDUSTRIE 4.0 upto 20 years [25].

4.4 Smart Environment Monitoring System

The smart environment monitoring system consists of various environment resources with smart monitoring system.

The smart water quality monitoring (WQM) is implemented for the detection of real time polluted water globally with hybrid WSN-NGPON2 technology by data acquisition, transmission and processing. It consists of field programmable gate array (FPGA) design with very high speed integrated circuit hardware description language (VHDL)/C language, WSNs, wireless communication (based on Zigbee) and Quartus II software or Qsys tool in computer. This system can detect the water pH, turbidity, water level, carbon dioxide on water surface and temperature of water [26].

The hybrid WSN-NGPON2 network can be utilized for temperature sensing in hostile environment (such as high temperature, pressure and humidity) to control the steam sterilizers and logging the data in real time. This system confirms the accuracy, feasibility, reduce the cost as compared to wired solutions [27].

4.5 Smart Parking System

Smart parking system or intelligent transportation system includes the counting of number of times the vehicles have entered or leave the vehicle parking spaces to know the available space remaining. It can also detect the wrongly parked cars or parking in booked spaces specially in malls or shopping centers. It also simplifies the parking system by users with proper guidance and intelligent decision in real time. The hybrid WSN-NGPON2 parking system utilizes the wireless energy saved sensors to monitor the parking area conditions at reasonable cost by using an ultrasonic detector or RFID technology [28].

4.6 Smart Waste Management

The hybrid WSN-NGPON2 network can be used for smart waste management system by using smart bins to handle the solid waste to keep the environment clean and green. It reduces the manpower, cost, time fuel deceases and pollution. It includes the wireless monitoring units installed in each smart bins and sensor measures the unfilled levels. Wireless access point unit collects data from every wireless monitoring units and transmits the data to central station. Finally the, central station implement evaluate the solid waste on the basis on received data [29].

4.7 Smart Agriculture

One of biggest problem in agriculture filed is the real time monitoring and analysis of crops data. As the experimental crops are planted typical 400 km in rural areas which is far away from major cities. This leads to expensive and time consuming site visit. This problem can be solved by introducing hybrid WSN-NGPON2 network that enabled the monitoring and analyzing the performance of crop data anywhere with the help to thousands of wireless sensors at high data rate. Some sensors can be used to detect the weather conditions, soil moisture (humidity) and water levels. This will helps to grow the varieties of plants and real time analysis at less cost [30].

4.8 Smart Grid

Smart grid includes the smart meters at appliance and circuit at user end to rapidly control and measure the energy consumption through ZigBee, wireless fidelity (WiFi), Ethernet etc. The received energy then distributed to energy distributed to send to its targets. When the extra benefits are added for customers, then it will increase the cost to distributor, for gaining more energy. Thus energy efficient hybrid WSN-NGPON2 architecture using sensor database sensor (DB) utilized for at lost cost and high gain [30].

4.9 Smart Manufacturing

Smart manufacturing includes the mining and food processing sectors to improve and monitor the safety and productivity. This is done by using key performance indicator (KPI) to design and implement suitable production process for plant operation and resources related to food safety and productivity. Thus hybrid WSN-NGPON2 network can be used for real time KPI assignment and monitoring services to assesses the plant's quality, product safety etc. Further, this will improve the quality of plant's product, plant efficiency, properly utilize the human resources, product's process efficiency and regular optimization [30].

5 Conclusion

This chapter provided an extensive review on the latest research trends in hybrid WSN-NGPON2 network along with the key challenges and applications in smart world. As the energy efficient and cost effective smart world applications have always been in significant demand. The enormous increase of these applications motivated towards the high energy efficient, flexible, scalable, fast and, secure network. The hybrid WSN-NGPON2 network has multiple applications and provides a large scope for innovative products as compared to existing PON architectures. It combines the both the characteristics of WSN and NGPON2 networks.

Furthermore, as the step toward smart world with hybrid WSN-NGPON2 is a slow and steady task because the next generation users need to be constantly educated for challenges and induced to adapt the digital world. To overcome these challenges

between smart world and users', more research gaps can be addressed for smart lifestyle application. Although the various smart applications supported by the hybrid WSN-NGPON2 network can enhance quality of life and lots of benefits from rural to urban areas. But the attentions need to be taken to hold problems at both the user and developer ends. Thus, the inspiration and long term success of hybrid WSN-NGPON2 network in the growing smart world lies in the coordination of researchers and users to overcome the challenges.

Thus, besides the WSN-NGPON2 requires maintaining the high data quantity, system robustness, realistic system, simple system implementation, cost effectiveness, privacy and power, it has numerous future energy efficient applications. Some of the potential advance applications are in tele-medical, surveillance, industry, transportation, agriculture, green communication, urban and rural areas. In future, it can be used to transreceive the different type of data such as sound, taste, smell, images etc. for critical applications. Apart from this it can be used for IoTs, big data, fuzzy logic in embedded systems, heterogeneous networks and time critical applications by using energy efficient, secure and spectrum management algorithms.

References

1. Wu, J.U.N., Ota, K., Dong, M., Li, C.: A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. IEEE Access. **4**, 416–424 (2016)
2. He, D., Chan, S., Guizani, M.: Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. IEEE Wirel. Commun. **24**(6), 2–7 (2016)
3. Li, W., Kara, S.: Methodology for monitoring manufacturing environment by using Wireless Sensor Networks (WSN) and the Internet of Things (IoT). Procedia CIRP **61**, 323–328 (2017)
4. Zhang, R., Ma, J.: Optik full-duplex hybrid PON/RoF link with 10-Gbit/s 4-QAM signal for alternative wired and 40-GHz band wireless access based on optical frequency multiplication. Opt. - Int. J. Light Electron. Opt. **138**, 55–63 (2017)
5. Abbas, H.S., Gregory, M.A.: The next generation of passive optical networks: a review. J. Netw. Comput. Appl. **67**, 53–74 (2016)
6. Kachhatiya, V., Prince, S.: Optical fiber technology four-fold increase in users of time-wavelength division multiplexing (TWDM) passive optical network (PON) by delayed optical amplitude modulation (AM) upstream. Opt. Fiber Technol. **32**, 71–81 (2016)
7. Hossen, M., Hanawa, M.: Adaptive limited DBA algorithm for multi-OLT PON-based FTTH and wireless sensor netwroks. In: APCC 2012 - 18th Asia-Pacific Conferenec on Communications Green Smart Commun. IT Innov., pp. 372–377 (2012)
8. Saini, R.K., Ritika, M., Vijay, S.: Data flow in wireless sensor network protocol stack by using bellman-ford routing algorithm. Bull. Electr. Eng. Inf. **6**, 81–87 (2017)
9. Nathali, B., Khan, M., Han, K.: Towards sustainable smart cities: a review of trends, architectures, components, and open challenges in smart cities. Sustain. Cities Soc. **38**, 697–713 (2018)
10. Hong, Y.-W.P., Hsu, T.-C., Chennakesavula, P.: Wireless power transfer for distributed estimation in wireless passive sensor networks. IEEE Trans. Signal Process. **64**, 5382–5395 (2016)

11. Chang, C.H., Lin, W.H., Lu, D.Y.: All-passive optical fiber sensor network with self-healing functionality. In: Proceedings of 2016 Progress Electromagnetic Research Symposium PIERS 2016, pp. 3788–3791 (2016)
12. Yu, Q., Li, G., Hang, X., Fu, K., Li, T.: An energy efficient MAC protocol for wireless passive sensor networks. Futur. Internet. **9**, 1–12 (2017)
13. Kumar, L., Singh, A., Sharma, V.: Performance analysis for downstream next generation converged WSN-PON ODN network incorporating diverse phase delay. Fiber Integr. Opt. **36**, 242–251 (2017)
14. Kumar, L., Sharma, V., Singh, A.: Bidirectional multi-optical line terminals incorporated converged WSN-PON network using M/M/1 queuing. Opt. Fiber Technol. **39**, 78–86 (2017)
15. Chang, C.H., Lin, W.H., Lu, D.Y.: All-passive optical fiber sensor network with self-healing functionality. In: Proceedings of 2016 Progress in Electromagnetic Resarch Symposium PIERS 2016, vol. 10, pp. 3788–3791 (2016)
16. An, C., An, Y.K., Yoo, S.M., Wells, B.E.: Efficient data association to targets for tracking in passive wireless sensor networks. Ad Hoc Netw. **75–76**, 19–32 (2018)
17. Akerele, M., Al-Anbagi, I., Erol-Kantarci, M.: A fiber-wireless sensor networks QoS mechanism for smart grid applications. IEEE Access **7**, 37601–37610 (2019)
18. Wang, Y., Zhu, Z., Wang, L., Bai, J.: A novel proposal of GPON-oriented fiber grating sensing data digitalization system for remote sensing network. Opt. Commun. **366**, 1–7 (2016)
19. Singh, P.K., Paprzycki, M., Bhargava, B., Chhabra, J.K., Kaushal, N.C., Kumar, Y. (eds.): Futuristic Trends in Network and Communication Technologies. Springer, Singapore (2019)
20. Rozas, A., Araujo, A.: An application-aware clustering protocol for wireless sensor networks to provide QoS management. J. Sens. **2019**, 1–11 (2019)
21. Chen, D.R.: An energy-efficient QoS routing for wireless sensor networks using self-stabilizing algorithm. Ad Hoc Netw. **37**, 240–255 (2016)
22. He, D., Ye, R., Chan, S., Guizani, M., Xu, Y.: Privacy in the Internet of Things for smart healthcare. IEEE Commun. Mag. **56**, 38–44 (2018)
23. Amin, R., Islam, S.K.H., Biswas, G.P., Khan, M.K., Kumar, N.: A robust and anonymous patient monitoring system using wireless medical sensor networks. Futur. Gener. Comput. Syst. **23**, 1–23 (2016)
24. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything you wanted to know about smart cities: the Internet of things is the backbone. IEEE Consum. Electron. Mag. **5**, 60–70 (2016)
25. Xu, K., Qu, Y., Yang, K.: A tutorial on the Internet of Things: from a heterogeneous network integration perspective. IEEE Netw. **30**, 102–108 (2016)
26. Myint, C.Z., Gopal, L., Aung, Y.L.: Reconfigurable smart water quality monitoring system in IoT environment. In: 2017 IEEE/ACIS 16th International Conference on Computer Information Science, pp. 435–440 (2017)
27. Sisinni, E., Depari, A., Flammini, A.: Design and implementation of a wireless sensor network for temperature sensing in hostile environments. Sens. Actuators A: Phys. **237**, 47–55 (2015)
28. Fernström, M.: Investigation of smart parking systems and their technologies. In: Thirty Seventh International Conference on Information Systems, Dublin, pp. 1–14 (2016)
29. Ramson, S.R.J., Moni, D.J.: Wireless sensor networks based smart bin. Comput. Electr. Eng. **64**, 337–353 (2017)
30. Georgakopoulos, D., Jayaraman, P.P.: Internet of Things: from internet scale sensing to smart services. Computing **98**, 1041–1058 (2016)

Internet of Things in Forensics Investigation in Comparison to Digital Forensics

Bhoopesh Kumar Sharma[1(✉)], Mayssa Hachem[1], Ved P. Mishra[2], and Maninder Jeet Kaur[2]

[1] Department of Forensic Sciences, Amity University Dubai, Dubai, UAE
{bsharma, mhachem}@amityuniversity.ae
[2] Department of Computer Sciences, Amity University Dubai, Dubai, UAE
vmishra@amityuniversity.ae, mani356@gmail.com

Abstract. The Internet of Things (IoT)-based forensic investigations have raised new challenges with the increase in the number of objects of legal significance, the applicability of identified and collected devices, indistinct network boundaries, and edgeless networks. IoT releases new opportunities in forensic investigations. Relying on pieces of evidence from the IoT environment, forensic investigators and examiners can face many challenges from the identification, collection, organization and the preservation of shreds of evidence and the clues encountered besides, to the security challenges of IoT devices. Understanding different entities and approaches of IoT, as well as the differences between digital and IoT forensics, is becoming a crucial skill for forensic investigators. In the present manuscript, a plan has been clearly explained to assess different features of IoT forensics. An elucidation has been proposed to foster the connection and support for realistic investigations and challenges in different areas of forensic investigations in forensic science.

Keywords: Digital forensics · Forensic investigation · Internet of Things (IoT) · Approaches to IoT forensics · Wireless Sensor Network (WSN)

1 Introduction

Digital technologies related crimes are pacing up. With the development of new technologies, criminals discover ways to use these techniques to commit offenses. The Internet is constantly transforming itself into certain unique kinds of software and hardware as a groundbreaking development, which means that no one can avoid it [1]. The kind of communication we are witnessing now is either human-device communication or human-human communication. However, the Internet of Things (IoT) has promise to deliver a fantastic future for the Internet as it provides Machine-Machine (M2M) communication [2]. Besides its tremendous benefits for the sector and the Internet of Things (IoT) community, it also presents its customers with countless difficulties. The expanding amount of IoT devices present possibilities and hazards from a forensic view in private settings such as smart homes. At the same moment, current digital forensic instruments and techniques do not support newer IoT devices. It makes it difficult for experts to extract data from them without the help of a forensic

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 672–684, 2020.
https://doi.org/10.1007/978-3-030-40305-8_32

consultant with knowledge in this field. Furthermore, these traces may pose difficulties for forensic scientists to evaluate and may contain vulnerabilities that pose hazards to privacy. In this chapter, we examine digital forensics from the IoT perspective. IoT is the use of intelligently coupled devices with the help of an internet system, sensors, actuators in machines, and other physical objects. It makes the smart devices identifiable, intelligent, communicable, and information accessible. The IoT allows individuals and smart devices to be linked anytime, anywhere with anything by using any path or network, as shown in Fig. 1.

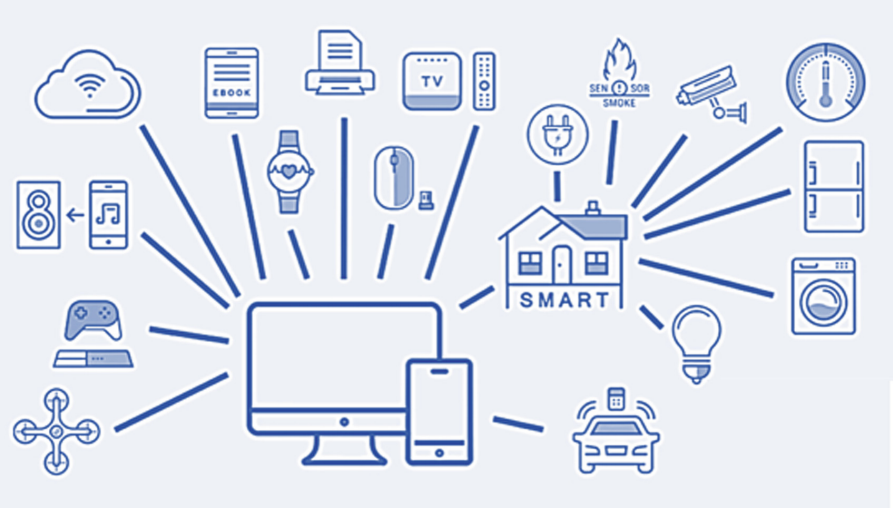


Fig. 1. Internet of things connected anytime anywhere with anchor device.

IoT framework is a complex network of different systems where, traditionally, countless, sensors and gadgets are associated with one another through interchanges channel and data foundation. IoT has an Radio-frequency identification RFID sensor network concerning the conventional form of networks like wired networks, Wi-Fi networks, cable, and mobile networks. IoT framework offers some benefits included administrations through astute information preparing [3]. The measurable computerized examination has turned out to be more difficult because of the enormous increment in registering gadgets, giving new experiences and difficulties in processing advanced information. The expanding utilization of cloud benefits in everyday tasks by associations and the heightened development and use of savvy gadgets are indicating the new difficulties the advanced legal specialists [4]. The dynamic nature of IoT alternatives introduces the primary challenge in detecting an IoT crime. As discussed in previous studies that, virtualization sterilizes the resources. Therefore, traditional analysis of remaining artifacts could be inadequate for the investigators.

According to a report published by Tillman in 2013, we have more than 5 billion "things" connected to the network. This number is further expected to be increased by

nearly 50 billion by 2020 [5]. Taking advantage of RFID and Wireless Sensor Network WSNs, physical objects such as computers, phones, smartphones, wearable technologies, home appliances, vehicles, medical devices, and industrial systems can be easily connected, tracked and managed by a single system [6].

Considering the high usage and complex functioning of the IoT devices, it creates numerous opportunities for cybercriminals, consequently causing a direct influence on consumers. For example, on October 21, 2016, a considerable cyberattack cracked out major websites across the Internet, which included Amazon, Twitter, Netflix, Etsy, Github, and Spotify [7]. Further to this, most IoT technologies are not manufactured with high-security parameters, and there are restricted regulations implemented on the consumer devices for the data collection; the main concern is the safety and security of the data [8]. Because of this scarcity, all security parameters cannot be amalgamated in IoT devices, as there is a requirement of considerable space and process to function for the same, which makes these devices easy prey for cybercriminals [9]. The perpetrators find an easy way to infect such devices so they can use them as tools to attack targeted individuals [10]. For instance, if any cloud computing technology is being used, the data is customarily written on a particular operating system. In such cases, pieces of evidence can be gathered in the form of short-term or temporary internet files, and be stored within the cybernetic atmosphere. This evidence usually lost as soon as the user exits the cloud [11].

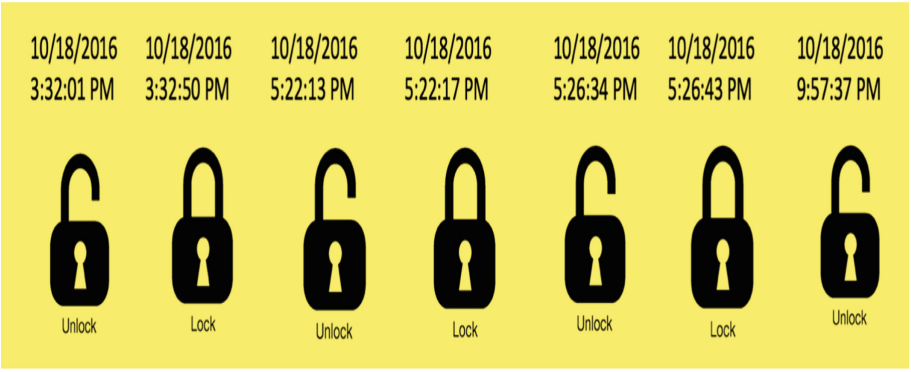


Fig. 2. Accessed data log of a Bluetooth embedded door lock controlled through smart phone.

Primarily, it is no more a difficult task to find potential evidence related to criminal activity through accessibility to network log, chatting details, emails, and other social networking inputs. Whether it is called IoT or WSN, there has been a lot of studies to secure these networks, starting from the mode level to the network level [12]. The security services provided in IoT include confidentiality, integrity, authentication, access control, anonymity, and availability. However, the major challenge is to

accumulate and analyze bulk data correctly and to gather forensic evidence related to the crime, along with detecting the existence of IoT activity (Fig. 2).

Mainly the evidence sources in the case of IoT's can be divided into three categories:

a. Shreds of evidence retrieved from smart devices and sensors;
b. Evidence gathered from software and hardware that provides communication between intelligent machines and the outside world (e.g., computers, mobile phones, and firewalls) included in established forensic networks;
c. Evidence unruffled outside the network from the investigated hardware and software. This group includes social networks, cloud, mobile system providers and ISPs, virtual online identities, and the internet.

With the increasing prevalence of IoT devices in many real-life applications, there is a need for conducting digital/network forensics to be able to understand the reasons for challenges and various attacks. In this study, we examine different features of IoT forensics and the challenges faced by the investigators due to this advancement in technology and systematically put them for better understanding and future research.

In the Sect. 2 of this chapter, we will give detailed background information with discussion on IoT entities and WSNs as well as Forensics of IoT. In the Sect. 3, we will discuss various approaches to IoT Forensics. The Sect. 4 will give us insight into Digital Forensics followed by IoT *vs.* Digital Forensics in Sect. 5.

2 Background

2.1 IoT Entities and WSNs

IoT devices usually comprise of specific embedded software, communication network, computing, sensor, and security devices. IoT devices use specially equipped software as essential features, can provide exclusive services based on their designs and purposes. Another critical part is the robust communication networks through which the IoT can communicate anytime and anywhere in the world (Fig. 3). All the devices are then interconnected in the IoT network using computing technologies, such as Edge, Fog, and Roof computing. The interacting mechanisms, with the aid of specific embedded software, sensors, and system supporting components, realize the presence of any physical entity using particular software. These devices gather the information required for the interaction. The Internet performs the role of communication media of various distributed physical entities. Each physical object is provided with a unique identification number. The gathered information from physical devices with the unique identification number will be processed using storage servers on the web and they will be delivered at the desired place in the desired time using different applications [13]. IoT functional safety blocks secure the system by offering multiple features such as authentication, approval, integrity of messages, privacy, content integrity, and data security.

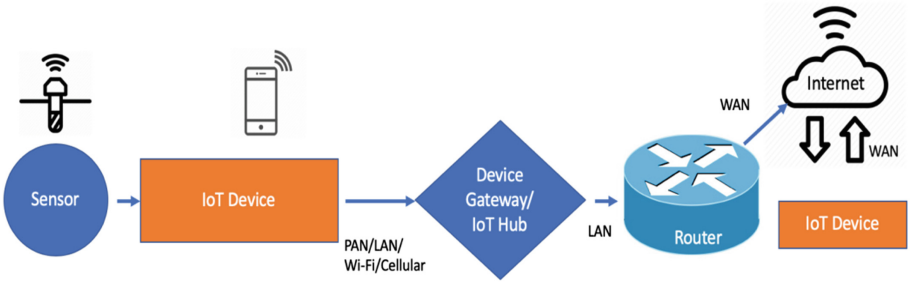


Fig. 3. Basic working structure of an IoT device

The background and evolution of IoT lie in the encroachment of the technology on microsensor devices in the late 90 s. These devices include microprocessors, memory technology, and other micro sensing devices, which led to the development of tiny sensors. These small sensors are equipped with communication capabilities that make them intelligent sensing devices to gather, process, and transmit data [14]. The other sensor component that is of interest to forensics would be a communication module. The amount of cyber-offense cases related to IoT has been increasing ever since [15]. The incidents such as ransomware, fraud, malicious attacks, node tempering, phishing, SQL injections and many more have been detected either by depleting the IoT devices or misusing applications and devices to commit a crime [16]. Since these instruments are linked through the networks, it is quite difficult to use static digital forensic tools compared to other computer forensics methods [17]. In addition, due to the constraints of IoT systems and the varying characteristics of digital evidence, adequate handling is needed; therefore, the IoT forensics require real-time inquiry [18]. In the next section, we familiarize with the concepts of Forensics of IoT.

2.2 Forensics of IoT

Forensics of IoT's is one of the main branches of digital forensics. Therefore, the investigation process must support the IoT infrastructure [19]. IoT has created a multitude of new problems for the field of digital forensics. In IoT-based instances, researchers need to cope with three distinct levels more often: forensic cloud, network, and device level [20]. During the forensic investigations using IoT, the identification of evidence, the collection of potential pieces of evidence, their organization, and their presentation deal with the IoT structures to solve a case of criminal activity. While there are no specified principles for IoT forensics, analysis will depend considerably on the smart device's mechanical and physical nature, as identifying sources of proof is a significant task. Certain necessary steps usually taken by an investigator during IoT forensics have been shown in Fig. 4. Recently, Servida & Kasey., 2019. have highligten the importance of traces from IoT devices in a smartphone for forensic investigation [21].

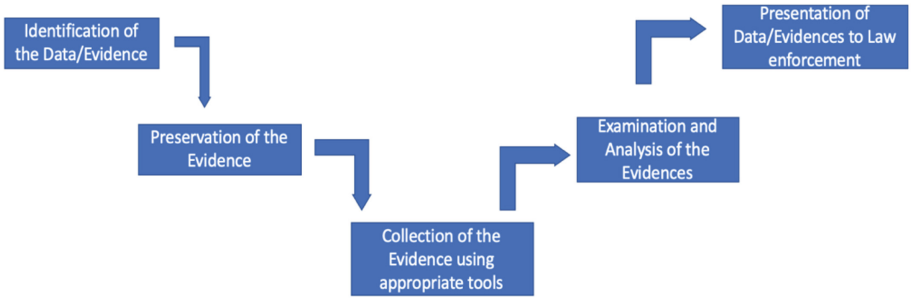


Fig. 4. Various steps followed by the cyber investigator during forensic investigation

Considering a forensic viewpoint, each IoT device will provide several crucial elements that might be useful during the investigation. Even though IoT has massive sources of evidence, it often poses some difficulties for forensic examiners, including information location and heterogeneity of IoT systems, such as operating system variations and communication protocols [22]. Currently, available researches mainly focus on IoT security and protection. However, few essential components, such as response to incidents and investigative processes, were not effectively covered by scientists. This section therefore focuses on this aspect.

Forensics of IoT is considered as a mixture of three digital parameters including the forensics at the device level, Forensics at the network level and the cloud forensic [19].

- ***Device forensics:*** Most recent IoT gadgets are being produced and progressed to make our lives simpler. These gadgets are worked by various working frameworks and may interface with various system advancements at one time. From the forensic viewpoint, the modern heterogenous gadgets, working framework, and correspondence section may influence the forensic examination. Typically these devices employ processing units, memory, a communication module, and sensing modules, which could be smartphones, smart meters, cameras, wearable devices, drones, etc. The specialist needs to gather information from the restricted memory of the IoT gadgets. At the point when important details should be picked from the IoT gadgets, it comprises of the gadget crime scene investigation [23]. Although it creates a burden on the investigation in terms of long time and increased learning curve, evidence must be collected from these sensing devices. Thus there is a need of standardization at device level investigations for IoT/WSN environments [24].
- ***Network forensics:*** IoT structures comprise of different types of various network systems, for example, Local Area Networks (LAN), Wide Area Networks (WAN), Body Area Network (BAN), Personal Area Network (PAN) and Home Area Networks (HAN). Huge confirmations can be gathered from these systems [23]. For each type there will be customized methods to conduct cyber forensics after an incident. Regardless of which form of network is used, most of the data in networks is volatile, which causes serious issues in forensic investigations. Most of the hardware used in networks record transmitted data itself or some information about the data in logs. These logs are indespensible to the forensic investigators as they may contain information which can eventually be used as evidence. Firewalls

capture and record the information about network traffic and keep the logs of events and transmitted data which goes through them while preventing unauthorized access to the systems [24].

- ***Cloud forensics:*** The cloud crime scene investigation is considered as one of the first capacities in the IoT criminology field. Information created from the IoT gadgets and utilizing IoT systems are put away in the cloud criminology. Cloud arrangements have numerous favorable circumstances, including availability, the substantial limit of capacity and on-request openness [24]. Data stored in the cloud raises severe issues in forensic investigations performed in IoT/WSN environment. Authors defines cloud forensics in three dimensions – legal dimension, organizational dimension, and technical dimension [25]. For similar reasons and to provide efficient service availability and reduce the cost of services, major service providers like Google, Amazon, and HP locate their data centers all around the world. Different countries and different states have different jurisdictions. A crime will be treated differently in different jurisdictions. Due to these issues, investigators may have to deal with multi-jurisdiction issues when data from IoT and WSNs are stored in the cloud [24].

3 Approaches in IoT Forensics

IoT legal sciences have been communicated as a real area of computerized criminological concern where the examination procedure must be under the IoT innovation and framework. This is essential for understanding the structure entirely and to explore the occurrence that is identified with IoT. The expedient advancement of this innovation, the IoT scientific must be prepared to confront the new difficulties, particularly in the worry of security and protection. The essential strides in legal examination incorporate the ID, legitimate gathering, conservation, intensive study and investigation of recuperated proves in advanced crime scene investigation. In any case, these procedures must serve for the Internet of Things and its conditions [26]. For example, some of the methods for data extraction are mentioned in Table 1.

Table 1. Data extraction methods [27].

Method	Process
Manual	The exclusive system of the device is used to show the information in its storage
Logical	A part of the storage of the device is extracted
File system	Access to the file system of the device
Physical (Non-Invasive)	Physical data acquisition without damaging the device
Physical (Invasive)	To access the circuit board, the device is physically tempered
Chip-Off	Removal and reading of the storage device to carry out data analysis
Micro-read	Extracting data from device's memory cells using a high magnification microscope for physical view

In context of IoT, mainly two approaches have been identified by the researchers [28]:

Pre-investigation Phase: Preparing for the IoT forensic readiness during this phase is the foundation of the investigation. Pre-investigative preparedness is essential to ensure the acquisition and evaluation process. It includes the preparation of the plan of investigation strategy, procedures, standard tools, operational and infrastructural support for the investigation. In addition to this, the scoping is very much required. Scoping is a method to narrow down the possible evidence that helps the investigator to identify, appropriately collect and preserve the evidence accurately. The investigator must be aware of what to obtain, how to determine, and how to protect the evidence (Fig. 5)?

Fig. 5. IoT Forensic planning and overview for the investigators.

Real-time Investigation: The real-time investigation is a spontaneous, automatic and live investigation process on any IoT device. It facilitates the handling of various tools and also the way to deal with them within IoT limitations. The next step will focus on applying a detection mechanism that triggers the main forensic phase to look for any strange activities on the IoT devices. Once it is detected, the Real-Time systems will perform the pre-investigation process to identify, collect and preserve the evidence for further investigation process.

4 Digital Forensics

Digital forensics is described as the discipline of locating, extracting and analyzing information from various interpretation instruments as legal proof in law [29, 30]. In the years following the technological revolution that began around the 1960s, the number of crimes perpetrated using computers has grown significantly.

Digital forensics is utilized differently that mostly depends upon the case scenario, event, organizations, and type of the system used in the crime. However, the primary goal of a digital forensic investigation is to obtain forensically significant evidence that can be used further to determine the activity or mode of operation in the case under investigation [27]. The NSIT guide recommends four phases of the digital forensics approach, i.e. collection, examination, analysis, and reporting of the evidence [29]. In IoT/WSN context, the digital forensics approach with a different set of processes as explained in Table 2.

Table 2. Digital forensics IoT specific steps [27].

Phases of digital forensics	IoT application
Collection of Data	For collecting information from things, proprietary hardware and software tool kits are needed
Examination of Data	Examining the information using exclusive instruments or gathering interesting proof manually
Analysis of Data	Depends on the nature of the stuff physically, technically and mechanically
Reporting of Data	Demonstration with the items engaged of the suitable proof

The main objective of Digital forensics (DF) is usually to obtain as much as evidence from electronic devices or media with the use of various forensic techniques and tools that are admissible in the court of law. The very nature of digital evidence means it is sensitive and can be altered, damaged, or destroyed if it is handled or examined inappropriately. Indeed, examining a copy of the initial proof is best practice. Such initial proof should be acquired in a manner that protects and maintains the integrity of the proof [31]. There are number of methods use to collect the data and transfer to the forensic workstation. Commercially accessible software like EnCase and FTK (forensic toolkit from accessdata.com) along with other open source instruments are the most widely used techniques for information collection. DF operates on gathering two data types. The persistent data stored on a local hard drive and the data stored when the computer is switched off are preserved. When the computer or device is switched off, volatile data stored in memory will be lost. Volatile data resides in the system's registries, cache, and RAM. Forensic investigation usually consists of three processes, i.e., using Live Acquisition Tools, Imaging Tools, and Analysis Tools. With the aid of EnCase, a live image of the data is created that can be used further for forensic investigations. EnCase usually supports all types of operating systems. The MD5 database is used to crack the encrypted files with a password.

5 IoT *Vs.* Digital Forensics

The Digital Forensics discipline deals with identifying, collecting, analyzing and presenting digital evidence from multiple types of digital/electronic storage media in an incident involving litigation/cybercrime or data security. Digital forensics utilizes the

concept of electronic discovery of evidence which includes the processes of gathering the data from electronic documents and to prepare that data in an admissible form for the presentation in a court room in any given case [32]. Digital evidence is very delicate in forensic investigation. Numerous researches in the area of digital forensic investigation process have been made those usually focused on studying the different phases in an investigation. These phases include the pre-investigation phase, the investigation phase and the post-investigation phase [33]. Inappropriate preservation and examination of any evidence can alter or destroy it [34].

In IoT forensics, device interactions and users produce information of enormous forensic value in a smart environment. It is accomplished with the help of several sensors, objects, and intelligent nodes that are capable of communicating among each other with human intervention or in the absence of any human intervention [35]. Digital forensics are no longer restricted to storage systems such as USB drives, pcs, smartphones, etc. with IoT evolution. The data is often used for forensic reasons from instruments such as sensors, IT clouds, and the smartwatch. There are many differences and similarities between digital and IoT forensics from the characteristics of IoT and digital forensic processes. Concerning the evidence sources, digital evidence can be computers, mobile devices, hard drives, network, whereas, in IoT forensics, the evidence can be sensors on buildings or cars, home appliances, humans or animal implantations, or in other IoT incorporated devices. The evidence data can be in any possible format in IoT forensics; however, in digital forensics, these will be electronic documents or standard file formats. The differences between IoT forensics and Digital Forensics mainly lies in the steps involved in the investigation from identification until the presentation of data, as mentioned in Table 3.

Table 3. Different steps involved in the investigation process in digital and IoT forensics.

Digital evidence/data	Digital forensics	IoT forensics
Identification	Cell phones, hard drives, network etc.	Sensors over buildings, surveillant videos, IT clouds, hearing aids etc.
Preservation	Standard software such as SANS SIFT, FTK Imager, CAINE	Hardware and Software among the IoT devices
Analysis	Based on the information technology principles and theories	Mostly works on various mechanical and physical nature of the things
Presentation	On computers systems or mobile phones with verbal presentation	Investigational demonstration with objects involving in oral presentation

6 Conclusion

Internet has showed its vital presence in human lives, from connections at a virtual level to the public associations. Researchers have used a AI techniques i.e. Knowledge based system for design of deep drawing dies for manufacturing of components for various industrial applications [36]. Firstly, the Internet of Things has added a new prospective into the world of internet by establishing communications between smart

objects and the humans. This communication has created the vision of "anytime, anyway, anywhere, anything" interactions [37, 38]. There is no doubt that the IoT will provide a more physical world evidences than standard computer systems [39]. Consequently, the large amount of evidence generated by a huge quantity of IoT devices will cause scientists extra difficulties in gathering appropriate proof from individually distributed IoT infrastructures. Newer methods are needed to rationalize information and determine what can be inferred from big data sets, as well as methods to explore instances where there are alleged "aggregation offenses." IoT Forensics has implemented the digital forensics techniques in the IoT infrastructure. In this artefact, we attempted to explain the entities, different approaches of IoT forensics and to identify the various challenges of reliable forensic sources in the IoT. Deciphering all the challenges of IoT forensics appropriately can help in the identification of many new insights in forensic investigations. Moreover, to acquire forensic information and then analyze the information quickly, a combination of network forensics instruments and computer forensics instruments is needed. Traditional forensic tools can be used to collect active information while maintaining the integrity of such information as well [40]. In the IoT evidence procurement phase, there are significant issues and challenges – the first phase of IoT forensics. Unless resolved in a timely way, these problems and difficulties can lead to incomplete or inaccurate forensic inquiry of IoT offenses, which can offer criminals a advantage as they can readily escape due to absence of evidence or false positive/negative evidence. We realized that digital forensic tools presently available can be used in the entire IoT process to some part and at certain phases, But a general and efficient IoT justice model or process is still needed to assist scientists overcome the challenges.

References

1. Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.B.: Blockchain with Internet of Things: benefits, challenges, and future directions. Int. J. Intell. Syst. Appl. **6**, 40–48 (2018)
2. Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A review on Internet of Things (IoT). Int. J. Comput. Appl. **113**(1), 1–7 (2015)
3. Index IEEE Internet of Things Journal vol. 4. IEEE Internet Things J. **4**(6), 2362–2392 (2017)
4. Taylor, M., Haggerty, J., Gresty, D., Hegarty, R.: Digital evidence in cloud computing systems. Comput. Law Secur. Rep. **26**(3), 304–308 (2010)
5. Tillman, K.: How Many Internet Connections are in the World? Right. Now (2013). https://blogs.cisco.com/news/cisco-connections-counter
6. Jiang, L., Da Xu, L., Cai, H., Jiang, Z., Bu, F., Xu, B.: An IoT-oriented data storage framework in cloud computing platform. IEEE Trans. Ind. Inf. **10**(2), 1443–1451 (2014)
7. Williams, W.: How friday's cyberattack shut down netflix, twitter, and spotify (2016). http://www.csmonitor.com/Technology/2016/1023/How-Friday-s-cyberattack-shut-down-Netflix-Twitter-and-Spotify
8. Herold, R.: The criticality of security in the Internet of Things. Inf. Syst. Audit Control Assoc. J. **6**, 18–24 (2015)
9. Truong, H., Narendra, N., Lin, K.: Notes on ensembles of IoT, network functions and clouds for service-oriented computing and applications. SOCA **12**(1), 1–10 (2018)

10. Blumenthal, E., Weise, E.: Hacked home devices caused massive Internet outage (2016). https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/
11. Hegarty, R.C., Lamb, D.J., Attwood, A.: Digital evidence challenges in the internet of things. In: Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis, pp. 163–172 (2014)
12. Zawoad, S., Hasan, R.: FAIot: towards building a forensics aware eco system for the Internet of Things. In: 2015 IEEE International Conference on Services Computing (SCC), pp. 279–284 (2015)
13. Kolias, C., Stavrou, A., Voas, J., Bojanova, I., Kuhn, R.: Learning Internet-of-Things security "Hands-On". IEEE Secur. Priv. **14**(1), 37–46 (2016)
14. Riazul Islam, S.M., Kwak, D., Kabir, M.H., Hossain, M.S., Kwak, K.S.: The Internet of Things for health care: a comprehensive survey. IEEE Access **3**, 678–708 (2015)
15. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer **44**(9), 51–58 (2011)
16. Sun, X., Wang, C.: The research of security technology in the Internet of Things. In: Advances in Computer Science, Intelligent System and Environment, vol. 105, pp. 113–119 (2011)
17. Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P.: Internet of Things forensics: challenges and approaches. In: Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, pp. 608–615 (2013)
18. Zareen, M.S., Waqar, A., Aslam, B.: Digital forensics: latest challenges and response. In: 2013 2nd National Conference on Information Assurance, NCIA, pp. 21–29 (2013)
19. Gao, L., Liu, L., Zhang, J., Hou, L.: Building of smart home medical system based on Internet of Things. Internet Things Cloud Comput. **4**(3), 34–38 (2016)
20. Alenezi, A., Hussein, R.K., Walters, R.J., Wills, G.B.: A framework for cloud forensic readiness in organizations. In: 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 199–204 (2017)
21. Servida, F., Casey, E.: IoT forensic challenges and opportunities for digital traces. Digit. Invest. **28**(Supplement), S22–S29 (2019)
22. Perumal, S., Norwawi, N.M., Raman, V.: Internet of Things (IoT) digital forensic investigation model: top-down forensic approach methodology. In: 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 1923 (2015)
23. Tilva, M., Rohokale, V.: Network forensics for detection of malicious packets in Internet of Things (IoT). Int. J. Recent Innov. Trends Comput. Commun. **4**(6), 114–118 (2016)
24. Karabiyik, U., Akkaya, K.: Digital forensics of IoT and WSNs. In: Lecture Notes in Computer Science: Authors' Instructions (2018)
25. Ruan, K., Carthy, J., Kechadi, T., Baggili, I.: Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit. Invest. **10**(1), 34–43 (2013)
26. Clint, M.R., Reith, M., Carr, C., Gunsch, G.: An examination of digital forensic models (2002). Int. J. Digit. Evid. **1**(3), 1–12 (2002)
27. Zia, T., Liu, P., Han, W.: Application-specific digital forensics investigative model in Internet of Things (IoT). In: Proceedings Of The 12th International Conference On Availability, Reliability And Security - ARES 2017, pp. 1–7 (2017)
28. Hunton, P.: The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Comput. Law Secur. Rev. **27**(1), 61–67 (2011)

29. Grance, T., Chevalier, S., Scarfone, K.K., Dang, H.: Guide to integrating forensic techniques into incident response. National Institute of Standards and Technology (NIST). Special Publication 800–86 (2006)
30. Hassan, N.A.: Digital Forensics Basics: A Practical Guide Using Windows OS, 1st edn. Apress, New York (2019)
31. Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C.: Systematic digital forensic investigation model. Int. J. Comput. Sci. Secur. (IJCSS) **5**(1), 118–131 (2011)
32. Zulkipli, N., Alenezi, A., Wills, G.: IoT forensic: bridging the challenges in digital forensic and the Internet of Things. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, pp. 315–324 (2017)
33. Garfinkel, S.L.: Digital forensics research: the next 10 years. Digit. Invest. **7**, S64–S73 (2010)
34. Casey, E.: Triage in digital forensics. Digit. Invest. Int. J. Digit. Forensics Incident Response **10**(2), 85–86 (2013)
35. Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S., Rahmani, A., Liljeberg, P.: On the feasibility of attribute-based encryption on Internet of Things devices. IEEE Micro Spec. Issue Internet Things **36**(6), 25–35 (2016)
36. Naranje, V., Kumar, S.: Knowledge-based system for design of deep drawing die for axisymmetric parts. In: Kumar, S., Hussein, H. (eds.) AI Applications in Sheet Metal Forming. Topics in Mining, Metallurgy and Materials Engineering, pp. 93–119. Springer, Singapore (2017)
37. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol 958. Springer, Singapore
38. Attwood, A., Merabti, M., Abuelmaatti, O.: IoMANETs: mobility architecture for wireless M2M networks. In: 2011 IEEE GLOBECOM Workshops (GC Wkshps), pp. 399–404 (2012)
39. Grobler, T., Louwrens, C.P., Von Solms, S.H.: A multi-component view of digital forensics. In: 2010 International Conference on Availability, Reliability and Security, pp. 647–652 (2010)
40. Alqahtany, S., Clarke, N., Furnell, S., Reich, S.: Cloud forensics: a review of challenges, solutions and open problems. In: 2015 International Conference on Cloud Computing (ICCC), pp. 1–9 (2015)

A Review on the Artificial Intelligence Algorithms for the Recognition of Activities of Daily Living Using Sensors in Mobile Devices

Ivan Miguel Pires[1,2,3], Gonçalo Marques[1,4(✉)], Nuno M. Garcia[1,5], Nuno Pombo[1], Francisco Flórez-Revuelta[6], Eftim Zdravevski[7], and Susanna Spinsante[8]

[1] Instituto de Telecomunicações, Universidade da Beira Interior, Covilhã, Portugal
impires@it.ubi.pt, goncalosantosmarques@gmail.com, {ngarcia,ngpombo}@di.ubi.pt
[2] Altranportugal, Lisbon, Portugal
[3] Polytechnic Institute of Viseu, Viseu, Portugal
[4] Polytechnic Institute of Guarda, Guarda, Portugal
[5] Universidade Lusófona de Humanidades e Tecnologias, Lisbon, Portugal
[6] Department of Computer Technology, Universidad de Alicante, San Vicente del Raspeig, Spain
francisco.florez@ua.es
[7] Faculty of Computer Science and Engineering, University Ss Cyril and Methodius, Skopje, Macedonia
eftim.zdravevski@finki.ukim.mk
[8] Department of Information Engineering, Marche Polytechnic University, Ancona, Italy
s.spinsante@univpm.it

Abstract. Smart environments and mobile devices are two technologies that when combined may allow the recognition of Activities of Daily Living (ADL) and its environments. This paper focuses on the literature review of the existing machine learning methods for the recognition of ADL and its environments, by means of comparison jointly with a proposal of a novel taxonomy in this context. The sensors used for this purpose depends on the nature of the system and the ADL to recognize. The available in the mobile devices are mainly motion, magnetic and location sensors, but the sensors available in the smart environments may have different types. Data acquired from several sensors can be used for the identification of ADL, where the motion, magnetic and location sensors handle the recognition of activities with movement, and the acoustic sensors handle the recognition of activities related with the environment.

Keywords: Activities of Daily Living · Mobile devices · Pattern recognition · Sensors · Methods · Review

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 685–713, 2020.
https://doi.org/10.1007/978-3-030-40305-8_33

1 Introduction

The recognition of ADL is of great importance for a number of reasons, among which one can find the need to monitor the activities of an elderly or a diseased person, as to allow the definition of adequate therapies not only as an improvement of that person's health, but also as an improvement to her/his wellbeing or quality of life. In addition, these features may be included for the development of a personal digital life coach (Garcia 2016), extending the identification of ADL.

An ADL (Foti and Koketsu 2013) may be identified with several types of sensors, including the motion, magnetic, vision, acoustic and location sensors usually found in off-the-shelf devices such as smartphones, allowing this identification to be performed in uncontrolled environments. While the recognition of ADL in controlled environments is related to the activities performed in smart environments equipped with several sensors, the recognition of ADL in uncontrolled environments is related to the use of several sensors attached to the subject's body or carried by the subject during the ADL. In this last scenario, the sensors used can be the ones that are widely available in a variety of off-the-shelf mobile devices such as smartwatches and smartphones. Several studies have been performed using the imaging sensors for the recognition of ADL, as presented in (Aggarwal and Ryoo 2011), but the main focus of this paper consists in the use of the sensors available in the mobile devices in order to promote the recognition of ADL in mobility.

The review of the methods for the development of an approach for the framework for the recognition of the ADL (Foti and Koketsu 2013) was started in the previous studies (Pires, Garcia et al. 2015, Pires, Garcia et al. 2016a, b, c, Pires, Garcia et al. 2016a, b, c, Pires, Garcia et al. 2018a, b, c, Pires, Garcia et al. 2018a, b, c, Pires, Garcia et al. 2018a, b, c, Pires, Santos et al. 2018, Pires, Teixeira et al. 2018), and the proposed framework includes the research of methods on data acquisition, data processing, data fusion and artificial intelligence methods for the recognition of ADL. The study (Pires, Garcia et al. 2016a, b, c) presented the review of the methods related to data acquisition, data processing and data fusion methods. However, the study (Pires, Garcia et al. 2016a, b, c) extends the research about data processing, including the research of methods about data cleaning and data imputation.

This paper present a review of the artificial intelligence methods for the recognition of ADL, published between 2007 and 2017, starting with the research of the methods used in smart environments, and, finally, the implemented in mobile devices for the recognition of ADL, where the most used sensors is the accelerometer for the recognition of simple activities, such as walking, running, walking on stairs, jumping, among others.

The remaining sections of this paper are organized as follows: Sect. 2 presents the methods for the recognition of ADL in smart environments. The methods for the recognition of ADL using mobile devices are presented in the Sect. 3. Section 4 presents the applicability of these methods and the results of the researched methods. Finally, the discussion and conclusions of this study are presented in the Sect. 5.

2 Background of the Recognition of Activities of Daily Living Using Sensors

The recognition of ADL was studied with the use of several types of sensors placed in the body of the individuals or available in smart environments. The authors of (Chernbumroong, Atkins et al. 2011) used Artificial Neural Networks (ANN) and decision tree for the recognition of simple activities, such as walking, running, standing, sitting and lying based on the data acquired from a single wrist-worn sensor, reporting an accuracy of 94.13%.

In (Bao and Intille 2004), a single wrist-worn sensor is also used for the recognition of several activities, including walking, sitting, working on computer, standing, eating, drinking, watching TV, reading, running, cycling, stretching, vacuuming, folding laundry, lying, brushing teeth, walking on stairs and riding an elevator, using decision tables, Instance-based learning (IBL), C4.5 decision tree and Naïve Bayes with reported accuracy of 84%.

Related to the recognition of ADL in smart environments, the Radio-frequency identification (RFID) sensors in different placements are used. The authors of (Naeem and Bigham 2007) used the RFID sensors for the recognition of making a tea, making a toast, drinking water, making coffee, warming a meal, washing dishes, using a dishwasher, and having a snack activities with Hidden Markov Model (HMM).

The Adaptive Learning Hidden Markov Model (ALHMM) was used with the data acquired from RFID sensors for the recognition of several activities, including making a tea, using the bathroom, phone calling, making a meal, taking out the trash, making soft-boiled eggs, setting the table, preparing orange juice, eating, making coffee and clearing the table (Cheng, Tsai et al. 2009).

The authors of (Hoque and Stankovic 2012) used the RFID sensors' data applied to HMM and Naïve Bayes for the recognition of sleeping, eating, preparing a breakfast, preparing a dinner, getting a drink, getting a snack, using a dishwasher, using a washing machine, taking a shower, using toilet, brushing teeth, leaving house and receiving guest.

In (Danny, Matthai et al. 2005), the C4.5 decision tree, Naïve Bayes and Support Vector Machine (SVM) are implemented with the data acquired from the RFID sensors, recognizing several activities with an accuracy around 42%, these are using a microwave, adjusting the thermostat, boiling a pot of tea, boiling water, brushing hair, brushing teeth, cleaning a toilet, cleaning the kitchen, doing laundry, drinking water, using a dishwasher, making a snack, reading, shaving face, using microwave, phone calling, vacuuming, using toilet, washing hands and watching TV.

The accelerometer is another sensor used for the recognition of ADL in smart environments. The authors of (Liming, Hoey et al. 2012) used several methods, including HMM, Dynamic Bayesian Network (DBN), SVM, Conditional random field (CRF), ANN, Logical formula, Naïve Bayes and decision tree, for the recognition of making coffee, brushing teeth and boiling water with accelerometer.

In (Wang, Chen et al. 2012), a method using the accelerometer data for the recognition of standing, walking, running, jumping, falling and sitting activities using Gaussian Mixture Model (GMM), HMM, and SVM was presented, reporting an accuracy between 96.43% and 98.21%.

The lying, sitting, standing, walking, cycling and running activities may be recognized with the accelerometer data, implementing the SVM, feed-forward neural network and decision tree (Gyllensten and Bonomi 2011). The eating and drinking activities may be recognized with the Extended Kalman Filter (EKF) applied to the accelerometer data (Zhang, Ang et al. 2009).

Only with the accelerometer data, the authors of (Khan, Lee et al. 2010) implemented the ANN and autoregressive (AR) model for the recognition of lying, sitting, standing, walking, walking on stairs and running activities, reporting an average accuracy of 97.9%.

The cameras are also used in smart environments for the recognition of ADL. The authors of (Botia, Villa et al. 2012) used the data retrieved from camera with the HMM for the recognition of movements in home office, kitchen, living room and outdoors, and activities, such as walking on stairs, making coffee and working on computer. Based on the use of cameras, the authors of (Aggarwal and Ryoo 2011) proposed a taxonomy for the recognition of ADL, separated in two different approaches, such as single-layered approaches and hierarchical approaches. The single-layered approaches can be Space-time approaches and Sequential approaches. Firstly, the space-time approaches are the Space-time volume, Trajectories and Space-time features. Secondly, the sequential approaches are the Exemplar-based and State-based. Finally, the hierarchical approaches are the Statistical, Syntactic and Description-based.

Other authors used the cameras for the recognition of several ADL, such as combing hair, making up, brushing teeth, washing hands, washing dishes, making a tea, making coffee, drinking, making a snack, vacuuming, watching TV, using a computer and using a smartphone, implementing SVM (Ramanan 2012).

The remaining studies related to the recognition of ADL presented in this section use a combination of sensors. The authors of (Szewcyzk, Dwan et al. 2009) used the data acquired from the accelerometer, camera and RFID sensors with the Naïve Bayes for the recognition of preparing dinner, working on computer, sleeping and watching TV activities, reporting an accuracy of 73.6%.

In (Chikhaoui, Wang et al. 2011), the authors used motion (e.g., accelerometer) and RFID sensors in different placements (i.e., door, light, temperature and item) for the recognition of several activities, such as having breakfast, waking up, preparing breakfast, toileting and preparing tea, with HMM, reporting a lowest accuracy of 86.08%.

The accelerometer and RFID sensors are also used for the recognition of several activities, such as making cereals, making a sandwich, making coffee, reading a book, watching TV, cleaning windows, using telephone, brushing teeth and sleeping, implementing HMM (Buettner, Prasad et al. 2009).

The authors of (Stikic, Huynh et al. 2008) used the accelerometer and RFID sensors for the recognition of dusting, ironing, vacuuming, brooming, mopping, cleaning windows, making the bed, watering plans, washing dishes and setting table activities, implementing HMM, Naïve Bayes and Joint Boosting.

In (Chernbumroong, Cang et al. 2013), the authors implemented the recognition of feeding, brushing teeth, dressing, walking, walking on stairs, sleeping, lying, washing dishes, ironing, sweeping and watching TV activities with the acquisition of data from the temperature, altimeter and accelerometer sensors, reporting an accuracy of 90% with SVM and ANN.

The authors of (Banos, Damas et al. 2012) implemented some variants of HMM, i.e., Two-level hierarchical HMM (HHMM), Bottom-level HMM and Top-level HMM, for the recognition of hoovering, sweeping, washing clothes, serving, making coffee, making a snack, brushing hair, phone calling, watching TV, knitting, listening music, brushing teeth and washing dishes activities with the data acquired from accelerometer and cameras.

In (Maurer, Smailagic et al. 2006), the implementation of the C4.5 decision tree reported an accuracy around 92.5% for the recognition of running, walking, walking on stairs, standing and sitting activities with data acquired from accelerometer, light, temperature and microphone sensors.

The combination of the accelerometer and the Global Positioning System (GPS) receiver for the recognition of lying, sitting, standing, walking, using a mouse, typing on a keyboard, flipping a page and eating activities with ANN and Bayesian networks (Zhu, Chen et al. 2010, Zhu and Sheng 2012). In (Libal, Ramabhadran et al. 2009), the GMM was used with data acquired from microphones and cameras in order to recognize eating, drinking, ironing, cleaning, phone calling and watching TV, reporting an accuracy of 57.64%.

According to (Tolstikov, Biswas et al. 2008), the eating activity may be recognized with camera, pressure, ultrasound and accelerometer sensors, implementing DBN and HMM. In (Kasteren and Krose 2007), the DBN is also used for the recognition of eating, bathing and toileting activities, using contact switches, pressure sensors and accelerometers. In (Suryadevara, Quazi et al. 2012), the authors used ZigBee wireless sensors with Naïve Bayes for the recognition of preparing a meal, watching TV and preparing tea.

The authors of (Ueda, Tamai et al. 2015) used the SVM with data acquired from power meters, ambient sensors, ultrasonic positioning sensor, door sensors and faucet sensors, reporting an accuracy of 82% in the recognition of several activities, such as watching TV, taking a meal, cooking, reading a book and washing dishes.

Based on the recognition of ADL with sensors available in smart environments and off-the-shelf mobile devices, the authors of (Hong, Kim et al. 2008) used the accelerometer and RFID sensors for the recognition of sitting, pushing a shopping cart, standing, phone calling, walking, taking picture, lying, put on skin conditioner, running, wiping, hand shaking, jumping, reading, hair brushing and cutting activities, reporting an accuracy of 84.36% with the decision tree.

The smart environments may have several types of sensors, where the authors of (Fulk, Edgar et al. 2012) used the accelerometer and the pressure sensor for the recognition of sitting, standing and walking activities, reporting an accuracy higher than 95% with the ANN.

Other authors (Ordonez, de Toledo et al. 2013) used the sensors available in smart environments, i.e., cameras and RFID sensors, and sensors available in off-the-shelf mobile devices for the recognition of leaving, toileting, sleeping, eating and drinking activities, implementing ANN, HMM and SVM.

Tables 1 and 2 summarize the ADL recognized in the literature and the methods used for the recognition of the ADL, concluding that the most recognized ADL are making a meal, eating, watching TV, brushing teeth, standing, sitting, lying, making

coffee, running, drinking, making a tea, washing dishes, phone calling, walking on stairs and cleaning, and the methods with best accuracy are the ANN and HMM.

Based on the methods presented in Table 2 and the analysis of the methods presented in (Pires, Garcia et al. 2016a, b, c, Pombo, Garcia et al. 2017), the methods used for the recognition of ADL can be grouped in Neural Networks, Reinforcement Learning, Decision, Bayesian and Instance-based methods, where the methods that report better accuracy and performance than others are the ANN.

Table 1. ADL recognized with the methods available in the literature.

ADL	Number of studies	Studies
Making a meal; eating; walking	11	Chernbumroong, Atkins et al. 2011; Bao and Intille 2004; Wang, Chen et al. 2012; Gyllensten and Bonomi 2011; Khan, Lee et al. 2010; Botia, Villa et al. 2012; Chernbumroong, Cang et al. 2013; Maurer, Smailagic et al. 2006; Zhu, Cheng et al. 2010, Zhu and Sheng 2012; Hong, Kim et al. 2008; Fulk, Edgar et al. 2012
Watching TV; standing; sitting	10	Bao and Intille 2004; Danny, Matthai et al. 2005; Ramanan 2012; Szewcyzk, Dwan et al. 2009; Buettner, Prasad et al. 2009; Chernbumroong, Cang et al. 2013; Banos, Damas et al. 2012; Libal, Ramabhadran et al. 2009; Suryadevara, Quazi et al. 2012; Ueda, Tamai et al. 2015
Brushing teeth	9	Bao and Intille 2004; Hoque and Stankovic 2012; Danny, Matthai et al. 2005; Liming, Hoey et al. 2012; Ramanan 2012; Buettner, Prasad et al. 2009; Chernbumroong, Cang et al. 2013; Banos, Damas et al. 2012; Hong, Kim et al. 2008
Lying	8	Chernbumroong, Atkins et al. 2011 Bao and Intille 2004; Zhang, Ang et al. 2009; Khan, Lee et al. 2010; Chernbumroong, Cang et al. 2013; Zhu, Cheng et al. 2010, Zhu and Sheng 2012; Hong, Kim et al. 2008
Making coffee; running; drinking; phone calling	7	Naeem and Bigham 2007; Cheng, Tsai et al. 2009; Liming, Hoey et al. 2012; Botia, Villa et al. 2012; Ramanan 2012; Buettner, Prasad et al. 2009; Banos, Damas et al. 2012

(*continued*)

Table 1. (*continued*)

ADL	Number of studies	Studies
Making a tea; washing dishes	6	Naeem and Bigham 2007; Ramanan 2012; Stikic, Huynh et al. 2008; Chernbumroong, Cang et al. 2013; Banos, Damas et al. 2012; Ueda, Tamai et al. 2015
Walking on stairs; cleaning; reading; sleeping	5	Bao and Intille 2004; Khan, Lee et al. 2010; Botia, Villa et al. 2012; Chernbumroong, Cang et al. 2013; Maurer, Smailagic et al. 2006
Working on computer; vacuuming; using toilet	4	Bao and Intille 2004; Botia, Villa et al. 2012; Ramanan 2012; Szewcyzk, Dwan et al. 2009
Using a dishwasher; ironing	3	Stikic, Huynh et al. 2008; Chernbumroong, Cang et al. 2013; Libal, Ramabhadran et al. 2009
Cycling; making a toast; having a snack; using the bathroom; using a microwave; Brushing hair; washing hands; sweeping; using a mouse; typing on a keyboard; flipping a page; leaving house; jumping	2	Bao and Intille 2004; Zhang, Ang et al. 2009
Stretching; folding laundry; riding an elevator; taking out the trash; making soft-boiled eggs; setting the table; preparing orange juice; clearing the table; getting a drink; getting a snack; using a washing machine; taking a shower; receiving guest; adjusting the thermostat; doing laundry; falling; combing hair; making up; waking up; dusting; brooming; mopping; making the bed; watering plants; setting table; feeding; dressing; hoovering; washing clothes; serving; knitting; listening music; pushing a shopping cart; taking picture; put on skin conditioner; wiping; hand shaking; hair brushing; cutting; toileting	1	Chernbumroong, Cang et al. 2013; Hoque and Stankovic 2012; Danny, Matthai et al. 2005; Wang, Chen et al. 2012; Gyllensten and Bonomi 2011; Aggarwal and Ryoo 2011; Chikhaoui, Wang et al. 2011; Buettner, Prasad et al. 2009; Banos, Damas et al. 2012; Tolstikov, Biswas et al. 2008; Kasteren and Krose 2007; Hong, Kim et al. 2008; Fulk, Edgar et al. 2012

Table 2. Methods implemented in the studies available in the literature.

Method	Number of studies	Average of the accuracy reported	Studies
Artificial Neural Networks (ANN)	9	94.13%	Chernbumroong, Atkins et al. 2011; Liming, Hoey et al. 2012; Gyllensten and Bonomi 2011; Khan, Lee et al. 2010; Chernbumroong, Cang et al. 2013; Zhu, Cheng et al. 2010, Zhu and Sheng 2012; Fulk, Edgar et al. 2012; Ordonez, de Toledo et al. 2013
Hidden Markov Model (HMM)	12	91.43%	Naeem and Bigham 2007; Cheng, Tsai et al. 2009; Hoque and Stankovic 2012; Liming, Hoey et al. 2012; Wang, Chen et al. 2012; Botia, Villa et al. 2012; Chikhaoui, Wang et al. 2011; Buettner, Prasad et al. 2009; Stikic, Huynh et al. 2008; Banos, Damas et al. 2012; Tolstikov, Biswas et al. 2008; Ordonez, de Toledo et al. 2013
Decision tables	1	84.00%	Bao and Intille 2004
Instance-based learning (IBL)	1	84.00%	Bao and Intille 2004
Gaussian Mixture Model (GMM)	2	77.93%	Wang, Chen et al. 2012; Libal, Ramabhadran et al. 2009
Decision tree (i.e., J48 and C4.5)	6	74.75%	Chernbumroong, Atkins et al. 2011; Bao and Intille 2004; Chetty and White 2016; Liming, Hoey et al. 2012; Gyllensten and Bonomi 2011; Maurer, Smailagic et al. 2006
Support Vector Machine (SVM)	8	74.07%	Danny, Matthai et al. 2005; Liming, Hoey et al. 2012; Wang, Chen et al. 2012; Gyllensten and Bonomi 2011; Ramanan 2012; Chernbumroong, Cang et al. 2013; Ueda, Tamai et al. 2015; Ordonez, de Toledo et al. 2013
Naïve Bayes	7	66.53%	Bao and Intille 2004; Hoque and Stankovic 2012; Danny, Matthai et al. 2005; Liming, Hoey et al. 2012; Szewcyzk, Dwan et al. 2009; Stikic, Huynh et al. 2008; Suryadevara, Quazi et al. 2012

3 Methods for the Recognition of Activities of Daily Living Using Mobile Devices

Mobile devices are equipped with several sensors (Pires, Garcia et al. 2016a, b, c) that are able to acquire data related to the ADL and handle the recognition of ADL using lightweight methods, because these devices have low memory and processing power. Most common sensors embedded on these devices are the accelerometer, the gyroscope, the magnetometer, the microphone and the GPS receiver (Salazar et al. 2013).

According to the previous studies in the literature, the accelerometer is the most used sensor for the recognition of ADL, because it allows the acquisition of the data related to the movement. The authors of (Vilarinho et al. 2015) implemented the Phone Acceleration Threshold (PAT), the Phone Pattern Recognition (PPR) and the Watch Threshold and Pattern Recognition (WTPR) for the recognition of different patterns of falling activities as well as the walking, sitting, walking on stairs, trying shoes and jogging activities with the use of accelerometer data, reporting a recognition accuracy of 63% for the recognition of falling activities, and 78% for the recognition of other activities.

Falling activities and ADL are also recognized in (Ivascu, Cincar et al. 2017), including the recognition of several types of falls and walking on stairs, sitting, standing, lying, getting up, jumping, walking and running activities with the accelerometer sensor, reporting an accuracy of 91.3% with decision tree, 95.96% with SVM, 86.54% with Naïve Bayes, 96.21% with Random Forest, 94.44% with Adaboost, 95.95% with k-Nearest Neighbour (k-NN), and 96.56% with Deep Neural Networks (DNN).

The authors of (Tsai, Yang et al. 2015) also used the accelerometer data for the recognition of several types of falls and other ADL, including walking, jogging, sitting, standing and lying activities, and, based on the placement of the smartphone, the results obtained using ANN are around 84.29%. In (Mashita, Komaki et al. 2012), the accelerometer sensor was also used for the recognition of standing, walking and running activities, implementing SVM.

The sports activities, *e.g.,* running, volleyball, handball, basketball and futsal, can be also identified with the accelerometer sensor, reporting an accuracy of 42.3% with the Multilayer Perceptron (MLP), 53.8% with the k-NN, 38.4% with the Naïve Bayes, 38.4% with the J48 decision tree and 50% with the SVM (Costa, Fazendeiro et al. 2016). In (Okour, Maeder et al. 2015), the recognition of sitting, walking, standing, sleeping and falling activities were also performed with a rule-based classifier applied to the accelerometer data, reporting an accuracy of 87.7%.

The authors of (Kelly and Caulfield 2012) implemented the C4.5 decision tree, MLP, Logistic Regression, Bayesian Networks and SVM for the recognition of standing, sitting, walking on stairs, and walking using the accelerometer sensors, and they reported an accuracy around 88.2%.

In (Büber and Guvensan 2014), the study recognizes walking, sitting, standing, walking on stairs, jogging, cycling and jumping with the implementation of several methods with the accelerometer data acquired, these are the J48 decision tree with an accuracy of 91.01%, the k-Start with an accuracy of 93.35%, the Naïve Bayes with an

accuracy of 80.55%, the Bayesian Network with an accuracy of 88.20%, the Random Forest with an accuracy of 93.13%, and the k-NN with an accuracy of 93.84%.

The authors of (Alam and Roy 2014) implemented the C4.5 decision tree for the recognition of talking, coughing, deglutition, silence and yawning, reporting an accuracy of 94.8% using accelerometer data. In the study (Khalifa, Lan et al. 2017), the rowing, cycling, running, walking, jumping, standing, sitting and walking on stairs activities were recognized with the accelerometer data, reporting an accuracy of 80.96% with the C4.5 decision tree, 61.27% with IBk Nearest Neighbour, 67.14% with Naïve Bayes, and 55.64% with SVM.

The authors of (Kilinc, Dalzell et al. 2015) used the ANN applied to the accelerometer data in order to recognize walking on stairs, drinking, getting up, sitting, standing and walking activities with a reported accuracy of 91%.

In (Nurwanto, Ardiyanto et al. 2016), the k-NN and Dynamic Time Warping Algorithm were implemented with accelerometer data for the recognition of pushing up, sitting, squatting and jumping activities, reporting an average accuracy around 84%.

The accelerometer sensor was also used for the recognition of walking and sitting activities in the study (Prabowo, Mutijarsa et al. 2016), reporting 87.29% with Bayesian networks, 87.86% with MLP, 88.26% with C4.5 decision tree, and 89.48% with k-NN.

The walking, standing, sitting and walking on stairs activities were also recognized with several methods applied to the accelerometer data, which reported 97.08% with decision tree, 93.53% with Bayesian networks, 93.03% with Naïve Bayes, 99.27% with k-NN and 92.54% with a rule based learner (Lau and David 2010).

In (Shen, Li et al. 2013), the SVM reports an accuracy around 95.8% for the recognition of sitting, standing and walking activities using the accelerometer data. The use of the J48 decision tree with the accelerometer data for the recognition of walking, walking on stairs, sitting, standing and lying activities reports an accuracy of 86% (Silva 2013). Recognizing eating, shopping, entertainment and recreational activities, the authors of (Phithakkitnukoon, Horanont et al. 2010) implemented the Naïve Bayes to the data acquired from the accelerometer sensor, but its accuracy is not mentioned. The authors of (Bujari, Licar et al. 2012) used the ANN for the recognition of the walking pattern with accelerometer data, reporting an accuracy between 75% and 98%.

In (Saponas, Lester et al. 2008), the Naïve Bayes classifier was used for the recognition of walking, running, cycling and sitting activities based on the accelerometer data, reporting an accuracy around 97%. Additionally, in (Kuspa and Pratkanis 2013), the recognition of walking on stairs, jogging, sitting, standing and walking activities was performed with the application of the Principal Component Analysis (PCA) and Gaussian Discriminant Analysis (GDA) to the accelerometer data, reporting an accuracy around 92%.

The standing, walking, cycling, driving and running activities were recognized by the authors of (Siirtola and Röning 2012) with the accelerometer data, applying the k-NN, Quadratic Discriminant Analysis (QDA) and SVM and reporting an average accuracy of 90%.

The accelerometer sensor was also used in (Kmiecik 2013) for the recognition of jogging, walking and walking on stairs, implementing Naïve Bayes classifier. The k-NN was used for the recognition of sitting and standing, reporting an accuracy of 100% with the accelerometer data (Kaghyan and Sarukhanyan 2012).

Based on the accelerometer data, the authors of (Anguita, Ghio et al. 2012) implemented the SVM for the recognition of standing, walking, laying and walking on stairs activities. In (Awan, Guangbin et al. 2013), the authors used the accelerometer data for the implementation of the J48 decision tree, the logistic regression and the Naïve Bayes, recognizing the sitting, standing, walking and jogging activities with an accuracy around 96%. In another study (Lara and Labrador 2012), the C4.5 decision tree was implemented for the recognition of running, walking and sitting activities, reporting an accuracy of 92.6% with the accelerometer data.

A system named Centinela, described in (Lara, Pérez et al. 2012), is a system that implements the Naïve Bayes for the recognition of walking, running, sitting and walking on stairs activities, reporting an accuracy up to 95.7%.

For the recognition of simple activities, *i.e.,* walking, running, standing and walking on stairs, and complex activities, *i.e.,* cooking and cleaning, another implementation of the ANN was presented in (Dernbach, Das et al. 2012), reporting an accuracy of 93% in the recognition of simple activities, and 50% in the recognition of complex activities. The authors of (Zhu and Sheng 2010) also used the accelerometer sensor for the recognition of sitting, standing, walking and lying activities, implementing the HMM that reports an accuracy of 60%.

For the recognition of lying, sitting, standing and walking activities, the authors of (Zhu and Sheng 2011) implemented the Viterbi algorithm, HMM and Bayesian filter, reporting an accuracy of 85% with the use of the accelerometer data. In (Huynh 2008), the SVM and HMM were implemented for the recognition of shopping, doing housework, bathing, dressing, toileting, feeding, walking, sitting, vacuuming, standing, eating and washing dishes activities with the accelerometer data, reporting an accuracy higher than 90%.

Using only the accelerometer sensor, the authors of (Jie, Shuangquan et al. 2010) used the k-NN one-class classifier, Support Vector Data Description (SVDD) one-class classifier and Gauss one-class classifier in order to recognize standing, walking, running and walking on stairs activities.

In (Zhang and Sawchuk 2013), the accelerometer data was used with Linear Description Analysis (LDA) and PCA for the recognition of walking, running, walking on stairs, standing, jumping and sitting activities with a reported accuracy of 96.1%. The authors of (Allen, Roozbeh et al. 2009) implemented the distributed sparsity classifier (DSC) for the recognition of standing, sitting, lying, kneeling, bending, jumping and walking on stairs activities, using the accelerometer data.

The previous studies analysed only used the accelerometer sensor, but other combinations of sensors have been studied in the last years. The authors of (Chetty and White 2016) used the accelerometer and gyroscope sensors for the recognition of walking, walking on stairs, sitting, standing and lying activities, reporting an accuracy of 79% with the Naïve Bayes classifier, 60% with the k-Means Clustering, 94% with J48 decision tree, 96.3% with Random Forest Classifier, 96.9% with Random Committee Classifier, and 97.89% with Lazy IBk Classifier.

In (Rasheed, Javaid et al. 2015), the Signal Magnitude Vector (SMV) algorithm was used for the recognition of standing, sitting, walking and running activities with accelerometer and gyroscope data. The lying and sitting activities were also recognized with the accelerometer and gyroscope sensors, reporting and accuracy of 80% with

Naïve Bayes, 87.5% with k-NN, 75.43% with Least Squares Method (LSM), 85.87% with ANN and 86.75% with SVM (Vallabh, Malekian et al. 2016).

The authors of (Roy, Misra et al. 2013) recognized the sitting, standing, walking, running, lying, walking on stairs, cleaning, cooking, taking medication, sweeping, washing hands and watering plants activities with the accelerometer and gyroscope sensors, reporting an accuracy between 50% and 85% with the HMM.

The ANN was also used to recognize the walking pattern with the accelerometer and gyroscope sensors, reporting an accuracy of 95.6% (Lorenzi, Rao et al. 2016). In (Shen, Chen et al. 2016), the accelerometer and gyroscope sensors are also used for the recognition of walking on stairs, walking, running and jumping activities, reporting an accuracy of 90.65% with Random Forest, 85.14% with SVM, 85.83% with ANN and 79.42% with k-NN.

The walking on stairs, walking, jogging and jumping activities are also recognized in (Chen and Shen 2017) with the accelerometer and gyroscope data, implementing several methods, such as the k-NN, which reports a minimum accuracy of 73.94%, the Random Forest, which reports a minimum accuracy of 83.59%, and the SVM, which reports a minimum accuracy of 69.21%.

The accelerometer and the gyroscope sensors are also used with SVM for the recognition of walking, running, and walking on stairs activities, reporting an accuracy of 92.5% (Hsu, Chu et al. 2015). The authors of (Anguita, Ghio et al. 2013) implemented the SVM for the recognition of walking, walking on stairs, sitting, standing and laying with the accelerometer and gyroscope data. An implementation of the SVM for the recognition of walking, standing, writing, smoking and jogging activities with accelerometer and gyroscope data was analysed in (Varkey, Pompili et al. 2011), reporting an accuracy of between 80 and 91%.

Another combination of sensors used for the recognition of ADL consists on the use of the accelerometer and the GPS receiver. The authors of (Fortino, Gravina et al. 2015) implemented the k-NN for the recognition of sitting, standing, walking, lying and falling activities with the accelerometer and the GPS receiver, reporting an accuracy of 96%.

In (Kwapisz, Weiss et al. 2011), the authors used the accelerometer and the GPS receiver for the recognition of walking, jogging, walking on stairs, sitting and standing activities with the J48 decision tree, logistic regression and MLP, reporting an accuracy of 90%. The walking, cycling, running and standing activities are recognized by the authors of (Chiang, Yang et al. 2013), which implemented the decision tree, k-NN, Naïve Bayes and SVM with the data acquired from the accelerometer and GPS receiver.

The authors of (Hong, Ramos et al. 2013) recognized the lying, sitting, standing, walking, walking on stairs and taking an elevator, implementing a system with ANN, SVM, GMM, HMM, k-NN, Random Forest and k-Means clustering with a reported accuracy of 90.4% using the accelerometer and GPS receiver. In (Ermes, Parkka et al. 2008), the ANN and decision tree were implemented for the recognition of lying, sitting, standing, walking, running, cycling, rowing and playing football based on the accelerometer and the GPS data, reporting an accuracy of 89%.

Another combination of sensors used for the recognition of ADL consists on the use of the accelerometer and the microphone. The authors of (Nishida, Kitaoka et al. 2014) implemented the GMM for the recognition of cycling, cleaning table, shopping,

toileting, cooking, watching TV, eating, working on a computer, reading, using a smartphone, driving and sleeping, reporting an accuracy of 76.9% with the accelerometer and microphone data.

The ANN was implemented with the use of the accelerometer and the microphone data for the recognition of walking, working on a computer, driving, cycling, running, jumping and watching TV (Bieber, Luthardt et al. 2011). The HMM also used with the accelerometer and the microphone data for the recognition of walking, running, cooking, reading, driving, eating, washing dishes, brushing teeth and watching TV activities (Ganti, Srinivasan et al. 2010).

The accelerometer and the camera is another combination of sensors used for the recognition of ADL, where the authors of (Zhan, Faux et al. 2014) implemented the LogitBoost and the SVM for the recognition of walking, walking on stairs, drinking, standing, sitting, reading, watching TV, writing and washing hands, reporting an accuracy of 77.4% with LogitBoost and 68.91% with SVM. Using also the accelerometer and the camera, the authors of (Nam, Rho et al. 2013) implemented the SVM for the recognition of walking, running, walking on stairs, taking an elevator, sitting and standing activities, reporting an accuracy of 92.78%.

Another combination of sensors is composed by the data acquired from the accelerometer and the digital compass, where the authors of (Cruz-Silva, Mendes-Moreira et al. 2013) recognized the walking on stairs, taking an elevator, running, walking and sitting reported on the Naïve Bayes, k-NN and Random Forest.

The accelerometer and the magnetometer sensors available in off-the-shelf mobile devices may be also used for the recognition of walking and running activities, where the authors of (Maekawa, Kishino et al. 2012) implemented the HMM. The eating activity was recognized by the accelerometer, light, temperature and barometer sensors by the authors of (Kim and Cho 2015) that implemented the Bayesian network, reporting an accuracy of 94.57%.

The accelerometer, light, temperature and microphone sensors were used by the authors of (He and Bai 2014), which implemented the HMM for the recognition of standing, running and walking activities with a reported accuracy higher than 80%. In (Eskaf, Aly et al. 2016), the authors used the accelerometer, gyroscope, gravity and rotational vector sensors for the recognition of walking, standing, sitting and bowing activities, reporting an accuracy of 83% with the J48 decision tree, 90% with the k-NN and 79% with the Naïve Bayes.

The gyroscope, accelerometer and magnetometer sensors available in off-the-shelf mobile devices may be used for the recognition of travelling by public transport, running, running, cycling and walking activities, where the authors of (Ravì, Lo et al. 2015) reported a minimum accuracy of 84.97% with the SVM.

The gyroscope, accelerometer and magnetometer sensors were also used in (Shoaib 2013) for the recognition of cycling, travelling by car, smoking, eating and taking an elevator activities with the use of the k-NN, the J48 decision tree, the rule based classifier and the SVM.

The authors of (Das, Green et al. 2010) used the accelerometer, GPS, gravity and communication sensors for the recognition of standing, walking, running, jumping and walking on stairs activities, reporting an accuracy of 93% with the 1-Nearest Neighbour classification algorithm.

The standing, walking and jogging activities may be recognized with accelerometer, gyroscope and GPS receiver, where the authors of (Fitz-Walter and Tjondronegoro 2009) reported an accuracy of 86.53% with ANN. The authors of (Gafurov, Snekkenes et al. 2007) also implemented the ANN and J48 decision tree for the recognition of jogging, walking on stairs and walking with the use of accelerometer, GPS receiver, camera, microphone, light, temperature and altitude sensors.

In (Kazushige and Miwako 2012), the implementation of the ANN reported an accuracy of 85% in the recognition of standing, walking, running, boarding, vacuuming and brushing teeth with the accelerometer, the microphone and the GPS receiver.

Table 3. Studies analysed.

Paper	Year of Publication	Number of ADL recognized	ADL	Sensors	Methods
Ivascu et al. (2017)	2017	9	Falling; walking on stairs; sitting; standing; lying; getting up; jumping; walking; running	Accelerometer	J48 decision tree; SVM; Naïve Bayes; Random Forest; Adaboost; k-NN; DNN
Khalifa et al. (2017)	2017	8	Rowing; cycling; running; walking; jumping; standing; sitting; walking on stairs	Accelerometer	C4.5 decision tree; IBk Nearest Neighbour; Naïve Bayes; SVM
Chen et al. (2017)	2017	4	Walking on stairs; walking; jogging; jumping	Accelerometer; Gyroscope	k-NN; Random Forest; SVM
Chetty et al. (2016)	2016	5	Walking; walking on stairs; sitting; standing; lying	Accelerometer; Gyroscope	Naïve Bayes; k-Means Clustering; J48 decision tree; Random Forest Classifier; Random Committee Classifier; Lazy IBk Classifier
Costa et al. (2016)	2016	5	Running; volleyball; handball; basketball; futsal	Accelerometer	ANN; k-NN; Naïve Bayes; J48 decision tree; SVM
Eskaf et al. (2016)	2016	4	Walking; standing; sitting; bowing	Accelerometer; gyroscope; gravity; rotational vector	J48 decision tree; k-NN; Naïve Bayes
Nurwanto et al. (2016)	2016	4	Pushing up; sitting; squatting; jumping	Accelerometer	k-NN; Dynamic Time Warping Algorithm
Shen et al. (2016)	2016	4	Walking on stairs; walking; running; jumping	Accelerometer; Gyroscope	Random Forest; SVM; ANN; k-NN

(*continued*)

Table 3. (*continued*)

Paper	Year of Publication	Number of ADL recognized	ADL	Sensors	Methods
Prabowo et al. (2016)	2016	2	Walking; sitting	Accelerometer	Bayesian network; ANN; C4.5 decision tree; k-NN
Vallabh et al. (2016)	2016	2	Lying; sitting	Accelerometer; Gyroscope	Naïve Bayes; k-NN; LSM; ANN; SVM
Lorenzi et al. (2016)	2016	1	Walking	Accelerometer; Gyroscope	ANN
Kilinc et al. (2015)	2015	6	Walking on stairs; drinking; getting up; sitting; standing; walking	Accelerometer	ANN
Fortino et al. (2015)	2015	5	Sitting; standing; walking; lying; falling	Accelerometer; GPS receiver	k-NN
Okour et al. (2015)	2015	5	Sitting; walking; standing; sleeping; falling	Accelerometer	rule-based classifier
Ravì et al. (2015)	2015	5	Travelling by public transport; running; running; cycling; walking	Accelerometer; gyroscope; magnetometer	SVM
Tsai et al. (2015)	2015	5	Walking; jogging; sitting; standing; lying	Accelerometer	ANN
Vilarinho et al. (2015)	2015	5	Walking; sitting; walking on stairs; trying shoes; jogging	Accelerometer	PAT; PPR; WTPR
Rasheed et al. (2015)	2015	4	Standing; sitting; walking; running	Accelerometer; Gyroscope	SMV algorithm
Hsu et al. (2015)	2015	3	Walking; running; walking on stairs	Accelerometer; Gyroscope	SVM
Kim et al. (2015)	2015	1	Eating	Accelerometer; light; temperature; barometer	Bayesian network
Nishida et al. (2014)	2014	12	Cycling; cleaning table; shopping; toileting; cooking; watching TV; eating; working on a computer; reading; using a smartphone; driving; sleeping	Accelerometer; Microphone	GMM
Zhan et al. (2014)	2014	9	Walking; walking on stairs; drinking; standing; sitting; reading; watching TV; writing; washing hands	Accelerometer; Camera	LogitBoost; SVM

(*continued*)

Table 3. (*continued*)

Paper	Year of Publication	Number of ADL recognized	ADL	Sensors	Methods
Büber et al. (2014)	2014	7	Walking; sitting; standing; walking on stairs; jogging, cycling; jumping	Accelerometer	J48 decision tree; k-Start; Naïve Bayes; Bayesian Network; Random Forest; k-NN
Alam et al. (2014)	2014	5	Talking; coughing; deglutition; silence; yawning	Accelerometer	C4.5 decision tree
He et al. (2014)	2014	3	Standing; running; walking	Accelerometer; light; temperature; microphone	HMM
Roy et al. (2013)	2013	12	Sitting; standing; walking; running; lying; walking on stairs; cleaning; cooking; taking medication; sweeping; washing hand; watering plants	Accelerometer; Gyroscope	HMM
Hong et al. (2013)	2013	6	Lying; sitting; standing; walking; walking on stairs; taking an elevator	Accelerometer; GPS receiver	ANN; SVM; GMM; HMM; k-NN; Random Forest; k-Means clustering
Nam et al. (2013)	2013	6	Walking; running; walking on stairs; taking an elevator; sitting; standing	Accelerometer; Camera	SVM
Zhang et al. (2013)	2013	6	Walking; running; walking on stairs; standing; jumping; sitting	Accelerometer	LDA; PCA
Anguita et al. (2013)	2013	5	Walking; walking on stairs; sitting; standing; laying	Accelerometer; Gyroscope	SVM
Cruz-Silva et al. (2013)	2013	5	Walking on stairs; taking an elevator; running; walking; sitting	Accelerometer; Digital compass	Naïve Bayes; k-NN; Random Forest
Kuspa et al. (2013)	2013	5	walking on stairs; jogging; sitting; standing; walking	Accelerometer	PCA; GDA
Shoaib (2013)	2013	5	Cycling; travelling by car; smoking; eating; taking an elevator	Accelerometer; gyroscope; magnetometer	k-NN; J48 decision tree; rule based classifier; SVM
Silva (2013)	2013	5	Walking; walking on stairs; sitting; standing; lying	Accelerometer	J48 decision tree

(*continued*)

Table 3. (*continued*)

Paper	Year of Publication	Number of ADL recognized	ADL	Sensors	Methods
Awan et al. (2013)	2013	4	Sitting; standing; walking; jogging	Accelerometer	J48 decision tree; logistic regression; Naïve Bayes
Chiang et al. (2013)	2013	4	Walking; cycling; running; standing	Accelerometer; GPS receiver	J48 decision tree; k-NN; Naïve Bayes; SVM
Kmiecik (2013)	2013	3	Jogging; walking; walking on stairs	Accelerometer	Naïve Bayes
Shen et al. (2013)	2013	3	Sitting; standing; walking	Accelerometer	SVM
Dernbach et al. (2012)	2012	6	Walking; running; standing; walking on stairs; cooking; cleaning	Accelerometer	ANN
Kazushige et al. (2012)	2012	6	Standing; walking; running; boarding; vacuuming; brushing teeth	Accelerometer; microphone; GPS receiver	ANN
Siirtola et al. (2012)	2012	5	Standing; walking; cycling; driving; running	Accelerometer	k-NN; QDA; SVM
Kelly et al. (2012)	2012	4	Standing; sitting; walking on stairs; walking	Accelerometer	C4.5 decision tree; ANN; Logistic Regression; Bayesian Network; SVM
Anguita et al. (2012)	2012	3	Standing; walking; laying; walking on stairs	Accelerometer	SVM
Lara et al. (2012)	2012	3	Walking; running; sitting; walking on stairs	Accelerometer	Naïve Bayes
Lara et al. (2012)	2012	3	Running; walking; sitting	Accelerometer	C4.5 decision tree
Mashita et al. (2012)	2012	3	Standing; walking; running	Accelerometer	SVM
Kaghyan et al. (2012)	2012	2	Sitting; standing	Accelerometer	k-NN
Maekawa et al. (2012)	2012	2	Walking; running	Accelerometer; Magnetometer	HMM
Bujari et al. (2012)	2012	1	Walking	Accelerometer	ANN
Bieber et al. (2011)	2011	7	Walking; working on a computer; driving; cycling; running; jumping; watching TV	Accelerometer; Microphone	ANN

(*continued*)

Table 3. (*continued*)

Paper	Year of Publication	Number of ADL recognized	ADL	Sensors	Methods
Kwapisz et al. (2011)	2011	5	Walking; jogging; walking on stairs; sitting; standing	Accelerometer; GPS receiver	J48 decision tree; logistic regression; ANN
Varkey et al. (2011)	2011	5	Walking; standing; writing; smoking; jogging	Accelerometer; Gyroscope	SVM
Zhu et al. (2011)	2011	4	Lying; sitting; standing; walking	Accelerometer	Viterbi algorithm; HMM; Bayesian filter
Ganti et al. (2010)	2010	9	Walking; running; cooking; reading; driving; eating; washing dishes; brushing teeth; watching TV	Accelerometer; Microphone	HMM
Das et al. (2010)	2010	5	Standing; walking; running; jumping; walking on stairs	Accelerometer; GPS receiver; gravity; communication	1-Nearest Neighbour
Jie et al. (2010)	2010	4	Standing; walking; running; walking on stairs	Accelerometer	k-NN one-class classifier; SVDD one-class classifier; Gauss one-class classifier
Lau et al. (2010)	2010	4	Walking; standing; sitting; walking on stairs	Accelerometer	J48 decision tree; Bayesian network; Naïve Bayes; k-NN; rule based classifier
Zhu et al. (2010)	2010	4	Sitting; standing; walking; lying	Accelerometer	HMM
Phithakkitnukoon et al. (2010)	2010	3	Eating; shopping; entertainment and recreational activities	Accelerometer	Naïve Bayes
Allen et al. (2009)	2009	7	Standing; sitting; lying; kneeling; bending; jumping; walking on stairs	Accelerometer	DSC
Fitz-Walter et al. (2009)	2009	3	Standing; walking; jogging	Accelerometer; gyroscope; GPS receiver	ANN
Huynh (2008)	2008	12	Shopping; doing housework; bathing; dressing; toileting; feeding; walking; sitting; vacuuming; standing; eating; washing dishes	Accelerometer	SVM; HMM

(*continued*)

Table 3. (*continued*)

Paper	Year of Publication	Number of ADL recognized	ADL	Sensors	Methods
Ermes et al. (2008)	2008	8	Lying; sitting; standing; walking; running; cycling; rowing; playing football	Accelerometer; GPS receiver	ANN; J48 decision tree
Saponas et al. (2008)	2008	4	Walking; running; cycling; sitting	Accelerometer	Naïve Bayes
Gafurov et al. (2007)	2007	3	Jogging; walking on stairs; walking	Accelerometer; GPS receiver; camera; microphone; light; temperature; altitude	ANN; J48 decision tree

Table 4. Summary of the methods and accuracies reported.

Method	Average of the accuracy reported
Random Committee Classifier	96.90%
DNN	96.56%
LDA	96.10%
Adaboost	94.44%
PCA	94.05%
k-Start	93.35%
1-Nearest Neighbour	93.00%
GDA	92.00%
Random Forest	91.71%
Logistic Regression	91.40%
ANN	91.12%
Bayesian Network	90.36%
Rule-based classifier	90.12%
QDA	90.00%
k-NN	87.40%
Decision trees (i.e., J48 and C4.5)	86.56%
Viterbi algorithm	85.00%
Bayesian filter	85.00%
Dynamic Time Warping Algorithm	84.00%
GMM	83.65%
SVM	82.27%
HMM	81.73%
Naïve Bayes	81.12%
IBk Nearest Neighbour	79.58%

(*continued*)

Table 4. (*continued*)

Method	Average of the accuracy reported
LogitBoost	77.40%
LSM	75.43%
k-Means Clustering	75.20%
PAT	70.50%
PPR	70.50%
WTPR	70.50%

Tables 3 and 4 present the summary of the studies analysed related to the recognition of the ADL.

4 Applicability and Results

The recognition of ADL (Foti and Koketsu 2013) is included on the research of the development of Ambient Assisted Living (AAL) systems (Garcia and Rodrigues 2015, Dobre, Mavromoustakis et al. 2016) that can be performed with the framework proposed in (Pires, Garcia et al. 2015, Pires, Garcia et al. 2016a, b, c, Pires, Garcia et al. 2016a, b, c, Pires, Garcia et al. 2016a, b, c), where the concepts related to data acquisition, data processing and data fusion were analyzed in (Pires, Garcia et al. 2016a, b, c), consisting this research in the last stage of the development of the framework for the automatic recognition of ADL, which can be included the development of a Personal Digital Life Coach (Garcia 2016).

The automatic recognition of ADL may be used for several purposes, including the prediction of the functional capacity in healthy adults and elderly people, the training of the lifestyle with the relation between the environment and the physical activities, the identification of some diseases (*e.g.,* low cognitive impairment, neurobehavioral dysfunction and/or other neurological disorder), the compensation of some disabilities (*e.g.,* helping the memory), the detection of harmful situations (*e.g.,* fall), the measurement of the levels of activity, the identification of needed emergency medicine with the identification of the patterns of ADL, and the identification of emergency situations (Vacher, Fleury et al. 2010; Urwyler, Rampa et al. 2015; Zdravevski, Lameski et al. 2017).

When compared with the use of the smart environments for the monitoring of ADL and its environments, the use of the mobile devices allows the creation of solutions to help the monitoring of several situations with low cost equipments, but it has some constraints and problems previously studied (Pires, Garcia et al. 2018a, b, c).

Following the studies related to the recognition of ADL using sensors available in off-the-shelf mobile devices, we analyzed 65 studies, where the major part of the studies have been performed between 2012 and 2017 with a total of 49 studies (75%), where 3 studies in 2017 (5%), 8 studies in 2016 (12%), 9 studies in 2015 (14%), 5 studies in 2014 (8%), 13 studies in 2013 (20%) and 11 studies in 2012 (17%).

Regarding the number of ADL recognized in each study analyzed, all studies recognized between 1 and 12 ADL, where 3 studies recognized 12 ADL (5%), 3

studies recognized 9 ADL (5%), 2 studies recognized 8 ADL (3%), 3 studies recognized 7 ADL (5%), 6 studies recognized 6 ADL (9%), 17 studies recognized 5 ADL (26%), 13 studies recognized 4 ADL (20%), 11 studies recognized 3 ADL (17%), 4 studies recognized 2 ADL (5%) and 3 studies recognized 1 ADL (5%), concluding that the major part of the studies analyzed recognize between 3 and 5 ADL (63%).

Related to the ADL recognized in the studies analyzed, several ADL were recognized, where the patterns related to the walking activity was recognized in 55 studies (85%), the standing activity was recognized in 41 studies (63%), the sitting activity was recognized in 37 studies (57%), the walking on stairs activity was recognized in 29 studies (45%), the running activity was recognized in 27 studies (42%), the lying activity was recognized in 12 studies (18%), the jogging activity was recognized in 11 studies (17%), the jumping and cycling activities were recognized in 10 studies (15%), the eating activity was recognized in 6 studies (9%), the driving, cooking, taking an elevator and watching TV activities were recognized in 4 studies (6%), the shopping, reading and falling activities were recognized in 3 studies (5%), the working on a computer, sleeping, drinking, rowing, toileting, washing hands, washing dishes, brushing teeth, vacuuming, writing, laying, smoking, travelling and cleaning activities were recognized in 2 studies (3%), and the remaining ADL were recognized only in 1 study (2%).

Related to the sensors used in the studies analyzed, the accelerometer was used in all studies analyzed (100%), but another sensors available in off-the-shelf mobile devices were used, including the gyroscope used in 14 studies (22%), the GPS receiver used in 9 studies (14%), the microphone used in 6 studies (9%), the magnetometer, light sensor, temperature sensor and camera used in 3 studies (5%), the gravity sensor used in 2 studies (3%), and the digital compass, rotational vector sensor, altitude sensor, barometer and communication sensor used in 1 study (2%).

Related to the methods with the best average accuracies reported presented in Table 4, these studies are used in 31 studies (48%) of studies analyzed, were 17 studies used the ANN (26%), 8 studies used the Random Forest (12%), 5 studies used the Bayesian Network (8%), 3 studies used the rule-based classifier and Logistic Regression (5%), 2 studies used the PCA (3%), and 1 study used the Random Committee Classifier, DNN, LDA, k-Start, 1-Nearest Neighbour, GDA, QDA and Adaboost (1%).

The solutions developed with the sensors available in the mobile devices allows the recognition of ADL. On the other hand, the processing and memory capabilities of these devices are very limited. Considering the use of the smart environments, the methods that reported higher accuracy than others are ANN (94.13%) and HMM (91.43%), where the most used sensors are the motions sensors and RFID sensors. However, considering the use of the mobile devices, the ANN and its variants, *i.e.,* DNN (96.56%) and ANN (91.12%) also reported some of the best accuracies, but the best accuracy was reported by the Random Committee Classifier (96.90%). All of the architectures have several limitations, such as limited power and processing capabilities of the mobile devices, and dependence of the constant network connection in smart environments. Regarding the costs of the different solutions, the use of mobile devices has lower costs in the implementation and maintainability.

5 Discussion and Conclusions

The recognition of ADL using mobile devices is a subject that has been researched in the last years with the recognition of simple and complex activities, including walking, running, jumping, standing, walking on stairs and others. This review is included in the conception of a new approach for the development of a framework for the recognition of ADL and their environments. The sensors available in off-the-shelf mobile devices are capable to acquire data related to the physical and physiological parameters of people, as well as data related to the environment, where the most used sensors are the motion, magnetic, acoustic and location sensors, handling the recognition of ADL only with a single mobile device and with commodity and non-invasive methods.

Based in the taxonomy proposed in (Aggarwal and Ryoo 2011) and the machine learning methods found in the literature, this paper proposes a new taxonomy for the recognition of ADL (see Fig. 1), whose the most used sensors are the accelerometers, cameras, and the RFID sensors. The sensors can be used alone and combined with

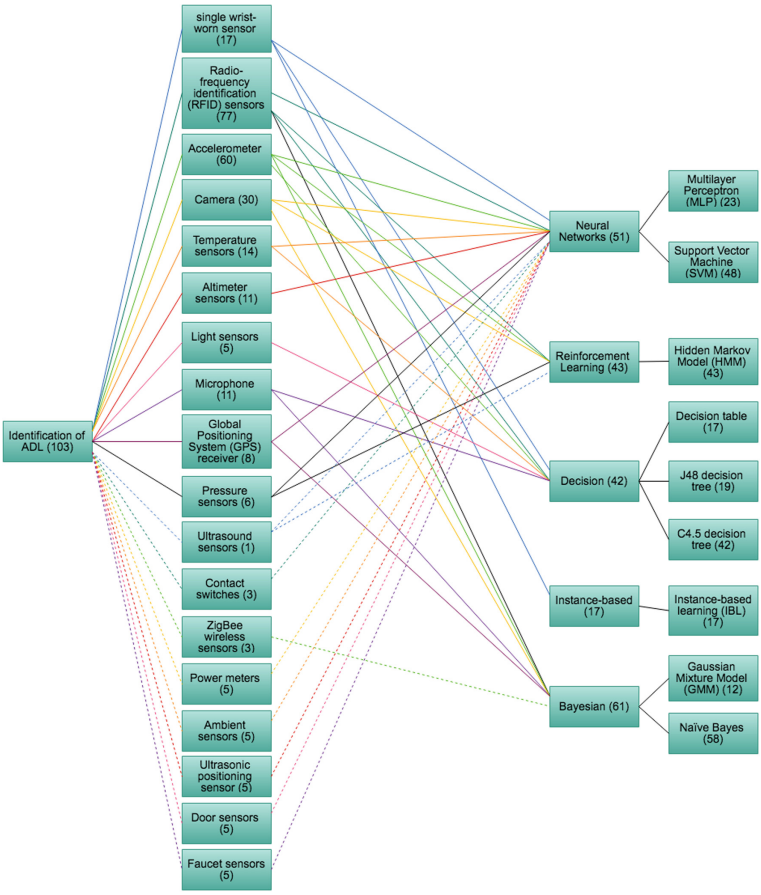


Fig. 1. Taxonomy proposed for the identification of ADL.

others, where the most used types of methods are the neural networks, reinforcement learning, decision, and the Bayesian methods.

Due to the high memory and power processing capabilities needed for the execution of the reinforcement learning methods, it is not adapted to the mobile devices. Related to the remaining methods, the neural networks show better accuracy than other methods. Using the sensors available in the mobile devices, the types of methods used are similar, where the neural network reported better results than others and the number of ADL recognized are higher with the ANN.

The most recognized ADL with mobile devices in the literature are the walking, standing, sitting, walking on stairs, running, lying, jogging, jumping and cycling activities, which are recognized in more than 10 studies analysed in this research. Therefore, the most implemented method in the literature is the ANN method, with is implemented in 17 studies and reported an average accuracy of 91.12%, but the three methods that report an average accuracy higher than 95% are the Random Committee Classifier, the DNN and the PCA.

The field related to the recognition of ADL has several purposes, including the training and monitoring of the lifestyles and people health.

Acknowledgments. This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/EEA/50008/2020 (Este trabalho é financiado pela FCT/MCTES através de fundos nacionais e quando aplicável cofinanciado por fundos comunitários no âmbito do projeto UIDB/EEA/50008/2020). This article/publication is based on work from COST Action IC1303 - AAPELE - Architectures, Algorithms and Protocols for Enhanced Living Environments and COST Action CA16226 - SHELD-ON - Indoor living space improvement: Smart Habitat for the Elderly, supported by COST (European Cooperation in Science and Technology). More information in www.cost.eu.

References

Aggarwal, J.K., Ryoo, M.S.: Human activity analysis: a review. ACM Comput. Surv. **43**(3), 1–43 (2011)

Alam, M.A.U., Roy, N.: GeSmart: a gestural activity recognition model for predicting behavioral health. In: 2014 International Conference on Smart Computing (SMARTCOMP) (2014)

Allen, Y.Y., et al.: Distributed recognition of human actions using wearable motion sensor networks. J. Ambient Intell. Smart Environ. **1**(2), 103–115 (2009). %@ 1876-1364

Anguita, D., et al.: Human activity recognition on smartphones using a multiclass hardware-friendly support vector machine. In: International Workshop of Ambient Assited Living (IWAAL 2012), Vitoria-Gasteiz, Spain (2012)

Anguita, D., et al.: A public domain dataset for human activity recognition using smartphones. In: European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN (2013)

Awan, M.A., et al.: A dynamic approach to recognize activities in WSN. Int. J. Distrib. Sens. Netw. **2013**, 1–9 (2013)

Banos, O., et al.: Daily living activity recognition based on statistical feature quality group selection. Expert Syst. Appl. **39**(9), 8013–8021 (2012)

Bao, L., Intille, S.S.: Activity Recognition from user-annotated acceleration data. In: Pervasive Computing, vol. 3001, pp. 1–17. Springer Heidelberg (2004)

Bieber, G., et al.: The hearing trousers pocket – activity recognition by alternative sensors. In: PETRA. ACM (2011)

Botia, J.A., et al.: Ambient assisted living system for in-home monitoring of healthy independent elders. Expert Syst. Appl. **39**(9), 8136–8148 (2012)

Büber, E., Guvensan, A.M.: Discriminative time-domain features for activity recognition on a mobile phone. In: 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) (2014)

Buettner, M., et al.: Recognizing daily activities with RFID-based sensors. In: Ubicomp 2009 Proceedings of the 11th International Conference on Ubiquitous Computing. ACM, New York (2009)

Bujari, A., et al.: Movement pattern recognition through smartphone's accelerometer. In: 2012 IEEE Consumer Communications and Networking Conference (CCNC). IEEE, Las Vegas (2012)

Chen, Y., Shen, C.: Performance analysis of smartphone-sensor behavior for human activity recognition. IEEE Access **5**, 3095–3110 (2017)

Cheng, B.-C., et al.: HMM machine learning and inference for Activities of daily living recognition. J. Supercomput. **54**(1), 29–42 (2009)

Chernbumroong, S., et al.: Activity classification using a single wrist-worn accelerometer. In: 2011 5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA). IEEE (2011)

Chernbumroong, S., et al.: Elderly activities recognition and classification for applications in assisted living. Expert Syst. Appl. **40**(5), 1662–1674 (2013)

Chetty, G., White, M.: Body sensor networks for human activity recognition. In: 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN) (2016)

Chiang, J.-H., et al.: Pattern analysis in daily physical activity data for personal health management. Pervasive Mob. Comput. **13**, 13–25 (2013)

Chikhaoui, B., et al.: A Frequent pattern mining approach for ADLs recognition in smart environments. In: 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA). IEEE, Biopolis (2011)

Costa, J., et al.: A mobile application to improve the quality of life via exercise. In: 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP) (2016)

Cruz-Silva, N., et al.: Features Selection for Human Activity Recognition with iPhone Inertial Sensors. In: 16th Portuguese Conference on Artificial Inteligence. Advances in Artificial Intelligence. APPIA, Angra do Heroísmo (2013)

Danny, W., et al.: Unsupervised activity recognition using automatically mined common sense. In: Proceedings of the 20th National Conference on Artificial Intelligence – vol. 1, pp. 21–27. AAAI Press, Pittsburgh (2005). %@ 1-57735-236-x

Das, S., et al.: Detecting user activities using the accelerometer on Android smartphones (2010)

Dernbach, S., et al.: Simple and Complex activity recognition through smart phones. In: 2012 8th International Conference on Intelligent Environments (IE). IEEE, Guanajuato (2012)

Dobre, C., et al.: Ambient Assisted Living and Enhanced Living Environments: Principles, Technologies and Control. Butterworth-Heinemann, Oxford (2016)

Ermes, M., et al.: Detection of daily activities and sports with wearable sensors in controlled and uncontrolled conditions. Trans. Info. Tech. Biomed. **12**(1), 20–26 (2008)

Eskaf, K., et al.: Aggregated activity recognition using smart devices. In: 2016 3rd International Conference on Soft Computing and Machine Intelligence (ISCMI) (2016)

Fitz-Walter, Z., Tjondronegoro, D.: Simple classification of walking activities using commodity smart phones. In: OZCHI 2009 Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7. ACM, New York (2009)

Fortino, G., et al.: Activity-aaService: cloud-assisted, BSN-based system for physical activity monitoring. In: 2015 IEEE 19th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (2015)

Foti, D., Koketsu, J.S.: Activities of daily living. Pedretti's Occup. Ther.: Pract. Skills Phys. Dysfunct. **7**, 157–232 (2013)

Fulk, G.D., et al.: Identifying activity levels and steps of people with stroke using a novel shoe-based sensor. J. Neurol. Phys. Ther. **36**(2), 100–107 (2012)

Gafurov, D., et al.: Gait authentication and identification using wearable accelerometer sensor. In: 2007 IEEE Workshop on Alghero Automatic Identification Advanced Technologies. IEEE (2007)

Ganti, R.K., et al.: Multisensor fusion in smartphones for lifestyle monitoring. In: 2010 International Conference on Body Sensor Networks (2010)

Garcia, N.M.: A roadmap to the design of a personal digital life coach. In: ICT Innovations 2015. Springer (2016)

Garcia, N.M., Rodrigues, J.J.P.: Ambient Assisted Living. CRC Press, Boca Raton (2015)

Gyllensten, I.C., Bonomi, A.G.: Identifying types of physical activity with a single accelerometer: evaluating laboratory-trained algorithms in daily life. IEEE Trans. Biomed. Eng. **58**(9), 2656–2663 (2011)

He, Z., Bai, X.: A wearable wireless body area network for human activity recognition. In: 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN) (2014)

Hong, J.-H., et al.: An activity recognition system for ambient assisted living environments. In: Evaluating AAL Systems Through Competitive Benchmarking, vol. 362, pp. 148–158. Springer, Heidelberg (2013)

Hong, Y.-J., et al.: Activity recognition using wearable sensors for elder care. In: Second International Conference on Future Generation Communication and Networking, FGCN 2008. IEEE, Hainan Island (2008)

Hoque, E., Stankovic, J.: AALO: activity recognition in smart homes using active learning in the presence of Overlapped activities. In: 2012 6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) (2012)

Hsu, H.H., et al.: Two-phase activity recognition with smartphone sensors. In: 2015 18th International Conference on Network-Based Information Systems (2015)

Huynh, D.T.G.: Human activity recognition with wearable sensors. Fachbereich Informatik, Darmstadt. Technische Universitat Darmstadt. Doktor-Ingenieur (Dr.-Ing.) (2008)

Ivascu, T., et al.: Activities of daily living and falls recognition and classification from the wearable sensors data. In: 2017 E-Health and Bioengineering Conference (EHB) (2017)

Jie, Y., et al.: Wearable accelerometer based extendable activity recognition system. In: 2010 IEEE International Conference on Robotics and Automation (ICRA). IEEE, Anchorage (2010)

Kaghyan, S., Sarukhanyan, H.: Activity recognition using K-nearest neighbor algorithm on smartphone with tri-axial accelerometer. In: International Journal of Informatics Models and Analysis (IJIMA), 146–156. ITHEA International Scientific Society, Bulgaria (2012)

Kasteren, T.V., Krose, B.: Bayesian activity recognition in residence for elders. In: 3rd IET International Conference on Intelligent Environments, IE (2007)

Kazushige, O., Miwako, D.: Indoor-outdoor activity recognition by a smartphone. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, pp. 537–537. ACM, Pittsburgh (2012). %@ 978-1-4503-1224-0

Kelly, D., Caulfield, B.: An investigation into non-invasive physical activity recognition using smartphones. In: 2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (2012)

Khalifa, S., et al.: HARKE: Human activity recognition from kinetic energy harvesting data in wearable devices. IEEE Trans. Mob. Comput. **PP**(99), 1 (2017)

Khan, A.M., et al.: A triaxial accelerometer-based physical-activity recognition via augmented-signal features and a hierarchical recognizer. IEEE Trans. Inf. Technol. Biomed. **14**(5), 1166–1172 (2010)

Kilinc, O., et al.: Inertia based recognition of daily activities with ANNs and spectrotemporal features. In: 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA) (2015)

Kim, K.H., Cho, S.B.: A dining context-aware system with mobile and wearable devices. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (2015)

Kmiecik, L.S.: Cloud centered, smartphone based long-term human activity recognition solution (2013)

Kuspa, K., Pratkanis, T.: Classification of mobile device accelerometer data for unique activity identification (2013)

Kwapisz, J.R., et al.: Activity recognition using cell phone accelerometers. ACM SIGKDD Explor. Newsl. **12**(2), 74 (2011)

Lara, Ó.D., et al.: Centinela: a human activity recognition system based on acceleration and vital sign data. Pervasive Mob. Comput. **8**(5), 717–729 (2012)

Lara, S.D., Labrador, M.A.: A mobile platform for real-time human activity recognition. In: CCNC IEEE Consumer Communications and Networking Conference, pp. 667–671 (2012)

Lau, S.L., David, K.: Movement recognition using the accelerometer in smartphones. In: 2010 Future Network and Mobile Summit (2010)

Libal, V., et al.: Multimodal classification of activities of daily living inside smart homes. In: Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living, vol. 5518, pp. 687–694. Springer, Heidelberg (2009)

Liming, C., et al.: Sensor-based activity recognition. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) **42**(6), 790–808 (2012)

Lorenzi, P., et al.: Mobile devices for the real-time detection of specific human motion disorders. IEEE Sens. J. **16**(23), 8220–8227 (2016)

Maekawa, T., et al.: Activity recognition with hand-worn magnetic sensors. Pers. Ubiquit. Comput. **17**(6), 1085–1094 (2012)

Mashita, T., et al.: A content search system for mobile devices based on user context recognition. In: 2012 IEEE Virtual Reality Workshops (VRW) (2012)

Maurer, U., et al.: Activity recognition and monitoring using multiple sensors on different body positions. In: International Workshop on Wearable and Implantable Body Sensor Networks, BSN 2006. IEEE, Cambridge (2006)

Naeem, U., Bigham, J.: A comparison of two hidden markov approaches to task identification in the home environment. In: 2nd International Conference on Pervasive Computing and Applications, ICPCA 2007, pp. 383–388. IEEE, Birmingham (2007)

Nam, Y., et al.: Physical activity recognition using multiple sensors embedded in a wearable device. ACM Trans. Embed. Comput. Syst. **12**(2), 1–14 (2013)

Nishida, M., et al.: Development and preliminary analysis of sensor signal database of continuous daily living activity over the long term. In: 2014 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA) (2014)

Nurwanto, F., et al.: Light sport exercise detection based on smartwatch and smartphone using k-Nearest neighbor and dynamic time warping algorithm. In: 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE) (2016)

Okour, S., et al.: An adaptive rule-based approach to classifying activities of daily living. In: 2015 International Conference on Healthcare Informatics (2015)

Ordonez, F.J., et al.: Activity recognition using hybrid generative/discriminative models on home environments using binary sensors. Sens. (Basel) **13**(5), 5460–5477 (2013)

Phithakkitnukoon, S., et al.: Activity-aware map: identifying human daily activity pattern using mobile phone data. In: Human Behavior Understanding, vol. 6219, pp. 14–25. Springer, Heidelberg (2010)

Pires, I., et al.: From data acquisition to data fusion: a comprehensive review and a roadmap for the identification of activities of daily living using mobile devices. Sensors **16**(2), 184 (2016a)

Pires, I.M., et al.: Multi-sensor data fusion techniques for the identification of activities of daily living using mobile devices. In: Proceedings of the ECMLPKDD 2015 Doctoral Consortium, European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, Porto, Portugal (2015)

Pires, I.M., et al.: Identification of activities of daily living using sensors available in off-the-shelf mobile devices: research and hypothesis. In: Ambient Intelligence-Software and Applications–7th International Symposium on Ambient Intelligence (ISAmI 2016). Springer, Cham (2016b)

Pires, I.M., et al.: Limitations of the use of mobile devices and smart environments for the monitoring of ageing people. In: ICT4AWE 2018 4th International Conference on Information and Communication Technologies for Ageing Well and e-Health, Madeira, Portugal (2018a)

Pires, I.M., et al.: Validation techniques for sensor data in mobile health applications. J. Sens. **2016**, 1687–1725 (2016c)

Pires, I.M., et al.: Approach for the development of a framework for the identification of activities of daily living using sensors in mobile devices. Sensors (Basel) **18**(2), 640 (2018b)

Pires, I.M., et al.: Identification of activities of daily living through data fusion on motion and magnetic sensors embedded on mobile devices. Pervasive Mob. Comput. **47**, 78–93 (2018c)

Pires, I.M., et al.: Recognition of activities of daily living based on environmental analyses using audio fingerprinting techniques: a systematic review. Sensors (Basel) **18**(1), 160 (2018a)

Pires, I.M., et al.: Android library for recognition of activities of daily living: implementation considerations, challenges, and solutions. Open Bioinf. J. **11**(1), 61–88 (2018b)

Pombo, N., et al.: Classification techniques on computerized systems to predict and/or to detect apnea: a systematic review. Comput. Methods Programs Biomed. **140**, 265–274 (2017)

Prabowo, O.M., et al.: Missing data handling using machine learning for human activity recognition on mobile device. In: 2016 International Conference on ICT For Smart Society (ICISS) (2016)

Ramanan, D.: Detecting activities of daily living in first-person camera views. In: Proceedings of the 2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2847–2854. IEEE Computer Society (2012)

Rasheed, M. B., et al.: Evaluation of human activity recognition and fall detection using android phone. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (2015)

Ravì, D., et al.: Real-time food intake classification and energy expenditure estimation on a mobile device. In: 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN) (2015)

Roy, N., et al.: Infrastructure-assisted smartphone-based ADL recognition in multi-inhabitant smart environments. In: 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom) (2013)

Salazar, L.H.A., et al.: A systematic literature review on usability heuristics for mobile phones. Int. J. Mob. Hum. Comput. Interact. **5**(2), 50–61 (2013)

Saponas, T., et al.: ilearn on the iphone: real-time human activity classification on commodity mobile phones. University of Washington CSE Tech Report UW-CSE-08-04-02 (2008)
Shen, B., et al.: Motion intent recognition for control of a lower extremity assistive device (LEAD). In: 2013 IEEE International Conference on Mechatronics and Automation (2013)
Shen, C., et al.: On motion-sensor behavior analysis for human-activity recognition via smartphones. In: 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (2016)
Shoaib, M.: Human activity recognition using heterogeneous sensors. In: Adjunct Publication of the 2013 ACM Conference on Ubiquitous Computing, UbiComp 2013 Adjunct. ACM, Zurich (2013)
Siirtola, P., Röning, J.: Recognizing human activities user-independently on smartphones based on accelerometer data. Int. J. Interact. Multimed. Artif. Intell. **1**(5), 38 (2012)
Silva, J.R.C.D.: Smartphone based human activity prediction. Faculdade de engenharia, Universidade do Porto, Master in Bioengineering, Porto (2013)
Stikic, M., et al.: ADL recognition based on the combination of RFID and accelerometer sensing. In: 2008 Second International Conference on Pervasive Computing Technologies for Healthcare (2008)
Suryadevara, N.K., et al.: Intelligent sensing systems for measuring wellness indices of the daily activities for the elderly. In: 2012 8th International Conference on Intelligent Environments (IE) (2012)
Szewcyzk, S., et al.: Annotating smart environment sensor data for activity learning. Technol. Health Care **17**(3), 161–169 (2009)
Tolstikov, A., et al.: Eating activity primitives detection - a step towards ADL recognition. In: 10th International Conference on e-health Networking, Applications and Services, HealthCom (2008)
Tsai, P.Y., et al.: Gesture-aware fall detection system: design and implementation. In: 2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin) (2015)
Ueda, K., et al.: A method for recognizing living activities in homes using positioning sensor and power meters. In: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (2015)
Urwyler, P., et al.: Recognition of activities of daily living in healthy subjects using two ad-hoc classifiers. Biomed. Eng. Online **14**, 54 (2015)
Vacher, M., et al.: Complete sound and speech recognition system for health smart homes: application to the recognition of activities of daily living (2010)
Vallabh, P., et al.: Fall detection using machine learning algorithms. In: 2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (2016)
Varkey, J.P., et al.: Human motion recognition using a wireless sensor-based wearable system. Pers. Ubiquit. Comput. **16**(7), 897–910 (2011)
Vilarinho, T., et al.: A combined smartphone and smartwatch fall detection system. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (2015)
Wang, J., et al.: Generative models for automatic recognition of human daily activities from a single triaxial accelerometer. In: The 2012 International Joint Conference on Neural Networks (IJCNN). IEEE, Brisbane (2012)
Zdravevski, E., et al.: Improving activity recognition accuracy in ambient-assisted living systems by automated feature engineering. IEEE Access **5**, 5262–5280 (2017)
Zhan, K., et al.: Multi-scale conditional random fields for first-person activity recognition. In: 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom) (2014)

Zhang, M., Sawchuk, A.A.: Human daily activity recognition with sparse representation using wearable sensors. IEEE J. Biomed. Health Inf. **17**(3), 553–560 (2013)

Zhang, S., et al.: Detection of activities by wireless sensors for daily life surveillance: eating and drinking. Sensors (Basel) **9**(3), 1499–1517 (2009)

Zhu, C., et al.: Human activity recognition via motion and vision data fusion. In: 2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers (ASILOMAR). IEEE, Pacific Grove (2010)

Zhu, C., Sheng, W.: Recognizing human daily activity using a single inertial sensor. In: 2010 8th World Congress on Intelligent Control and Automation (WCICA), pp. 282–287. IEEE, Jinan (2010)

Zhu, C., Sheng, W.: Realtime recognition of complex daily activities using dynamic Bayesian network. In: 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). IEEE, San Francisco (2011)

Zhu, C., Sheng, W.: Realtime recognition of complex human daily activities using human motion and location data. IEEE Trans. Biomed. Eng. **59**(9), 2422–2430 (2012)

Author Index

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 715–716, 2020.
https://doi.org/10.1007/978-3-030-40305-8