Development of Energy Efficient and Location-aware approaches for IoT and WSN based framework for Precision Agriculture

Thesis submitted

by

Arindam Giri

DOCTOR OF PHILOSOPHY (Engineering)

Department of Computer Science and Engineering,

Faculty Council of Engineering & Technology

Jadavpur University

Kolkata, India

2022

Development of Energy Efficient and Location-aware approaches for IoT and WSN based framework for Precision Agriculture

Thesis submitted

by

Arindam Giri

DOCTOR OF PHILOSOPHY (Engineering)

under the supervision of

Prof. Sarmistha Neogy

Department of Computer Science and Engineering

Jadavpur University

Kolkata, West Bengal, India

and

Dr. Subrata Dutta

Department of Computer Science and Engineering

National Institute of Technology

Jamshedpur, India

2022

JADAVPUR UNIVERSITY
KOLKATA-700032

Index No: 21/18/E

1. Title of the thesis:

Development of Energy Efficient and Location-Aware approaches for IoT and WSN based framework for Precision Agriculture

2. Name, Designation and Institution of the Supervisors:

(a) Prof. Sarmistha Neogy
Professor
Department of Computer Science and Engineering
Jadavpur University
Kolkata, West Bengal, India, 700032

(b) Dr. Subrata Dutta
Assistant Professor
Department of Computer Science and Engineering
National Institute of Technology
Jamshedpur, Jharkhand, India, 831014

3. List of Publications:

(a) Journal:

Published

i. **Giri, A.**, Dutta, S. and Neogy, S., "Information-theoretic approach for secure localization against sybil attack in wireless sensor network." *Journal of Ambient Intelligence and Humanized Computing*, 12(10), pp.9491-9497, 2021. DOI: https://doi.org/10.1007/s12652-020-02690-9

ii. **Giri, A.**, Dutta, S., Neogy, S., Koirala, B., and Dahal, K., "Adaptive Cross-Layer Routing Protocol for Optimizing Energy Harvesting Time in WSN." *Wireless Pers Commun*, 122(1), pp.825-843, 2021. DOI: https://doi.org/10.1007/s11277-021-08927-w

Communicated

i. **A. Giri**, S. Dutta, and S. Neogy, "An Optimized Fuzzy Clustering Algorithm for Wireless Sensor Networks," *Wirel. Pers. Commun.*, Springer (accepted).

(b) Conference:

i. **A. Giri**, S. Dutta, and S. Neogy, "Novel Range-free Localization for Wireless Sensor Networks using Fuzzy Logic," *Proceedings of International Conference on IoT and its Applications* ICIA, NIT Jamshedpur, December 26-27, 2020.

ii. **A. Giri**, S. Dutta, and S. Neogy, "Fuzzy Logic-Based Range-Free Localization for Wireless Sensor Networks in Agriculture." in *6th International Doctoral Symposium on Applied Computation and Security* ACSS, Kolkata, India, 12-13 March, 2019.

iii. **A. Giri**, S. Dutta, S. Neogy, K. Dahal, and Z. Pervez, "Internet of Things (IoT): A Survey on Architecture, Enabling Technologies, Applications and Challenges," *in Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 2017, pp. 7:1–7:12.

iv. **A. Giri**, S. Dutta, and S. Neogy, "Enabling agricultural automation to optimize utilization of water, fertilizer and insecticides by implementing Internet of Things (IoT)," *International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds.* pp. 125–131, 2016.

(c) Book chapter:

i. **A. Giri**, S. Dutta, and S. Neogy, "Fuzzy Logic-Based Range-Free Localization for Wireless Sensor Networks in Agriculture," in *Advanced Computing and Systems for Security*, Springer, pp. 3–12, 2020.

ii. **Giri, Arindam**, Subrata Dutta, Kailash Chandra Mishra, and Sarmistha Neogy, "IoT Middleware Technology: Review and Challenges," in *Interoperability in IoT for Smart Systems*, CRC Press, pp. 71-90, 2020.

4. List of Patents: NIL

5. List of Presentations in National / International Conference :

i. **A. Giri**, S. Dutta, and S. Neogy, "Novel Range-free Localization for Wireless Sensor Networks using Fuzzy Logic," *Proceedings of International Conference on IoT and its Applications* ICIA, NIT Jamshedpur, December 26-27, 2020.

ii. **A. Giri**, S. Dutta, and S. Neogy, "Fuzzy Logic-Based Range-Free Localization for Wireless Sensor Networks in Agriculture." in *6th International Doctoral Symposium on Applied Computation and Security* ACSS, Kolkata, India, 12-13 March, 2019.

iii. **A. Giri**, S. Dutta, and S. Neogy, "Enabling agricultural automation to optimize utilization of water, fertilizer and insecticides by implementing Internet of Things (IoT)," *International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds.* pp. 125–131, 2016.

“Statement of Originality”

I Arindam Giri registered on 08-06-2018 do hereby declare that this thesis entitled “Development of Energy Efficient and Location-aware Approaches for IoT and WSN based Framework for Precision Agriculture” contains literature survey and original research work done by the undersigned candidate as part of Doctoral studies.

All information in this thesis have been obtained and presented in accordance with existing academic rules and ethical conduct. I declare that, as required by these rules and conduct, I have fully cited and referred all the materials and results that are not original to this work.

I also declare that I have checked this thesis as per the “Policy on Anti Plagiarism, Jadavpur University, 2019”, and the level of similarity as checked by iThenticate software is 6 %.

Signature of the Candidate :

Date :

Certified by Supervisor(s) :

(Signature with date, seal)

1.

2.

CERTIFICATE FROM THE SUPERVISORS

This is to certify that the thesis entitled ***"Development of Energy Efficient and Location-aware Approaches for IoT and WSN based Framework for Precision Agriculture"*** *submitted by* ***Arindam Giri****, who got his name registered on* ***8th June 2018****, for the award of Ph.D. (Engineering) degree of Jadavpur University, is absolutely based upon his own work under the supervision of* ***Prof. Sarmistha Neogy*** *and* ***Dr. Subrata Dutta*** *and that neither his thesis nor any part of the thesis has been submitted for any degree/diploma or any other academic award anywhere before.*

Prof. Sarmistha Neogy,
Professor,
Department of Computer Science
and Engineering
Jadavpur University.

(Supervisor)

Dr. Subrata Dutta
Assistant Professor,
Department of Computer Science
and Engineering,
NIT, Jamshedpur.

(Co-Supervisor)

Dedicated

To my parents

Acknowledgements

At the time of initiating my research work, I was a bit nervous that if it is really possible to complete my PhD work. Once one my research works got accepted, I used to dream my PhD degree. Now, it is time to acknowledge those who support, advice, encourage and love me. Without their support my PhD thesis would have not been completed.

First and foremost, I like to express my sincere gratitude to my supervisor, Prof. (Dr.) Sarmistha Neogy for her constant advice and ever encouraging support. Throughout my tenure of PhD work, she spent her valuable time to critically review my works and advise me accordingly. I am grateful to her for her valuable advice, inspiring guidance, and cooperation to realize my dream.

My sincere gratitude goes to another supervisor Dr. Subrata Dutta for his valuable suggestion in finding research problems. He always encouraged me to carry on my work towards publication even in rejection. Without his help my PhD work could not have been completed. He gave an opportunity to pursue PhD at Jadavpur University. I have no words to give him thanks.

I would like to express my gratitude to the members of my research advisory committee, namely, Prof. (Dr.) Sarbani Roy, and Dr. Chandreyee Choudhury for their valuable advice to improve my research.

I express my deepest gratitude and thanks and to my parents, Sri Nilkanta Giri and Mrs. Alaka Giri for their love, encouragement and support. I am indebted to my parents for their sacrifice to make me educated. I strongly recognize my father's effort put towards possessing my mastery in all subjects. I express my gratitude to my elder sisters, Mrs. Manjusri Guria and Mrs. Anusri Pal for their love and best wishes. I could never forget my childhood with my sisters.

I grateful to my teachers, Sri Gopal Chandra Das, Mrs. Tapati Das, Sri Tarapada Pal, Sri Nagendranath Bhunia, Sri Haripada Panda, Sri Ardhendu Sekhar Guchhait, Late Sri , Sri Siddheswar Gole, Sri Samiran Sau, Sri Abanti Guchhait, Sri Abani Kumar Misra, Sri Biharilal Sen, Sri Kamala Kanta Giri, Late Sri Probodh Chandra Panigrahi, Late Sri Sripati Charan Maity, Late Sri Subimal Patra, Late Sri Biroja Bhusan Paria, Sri Sudhiranjan Sau, and Sri Bimal Kumar Paria. I express my sincere gratitude for their effort to make me a good student. I am indebted to all my beloved teachers.

I am also thankful to my wife Mrs. Bijaya Giri for her constant encouragement and cooperation in pursuing PhD. My children, Anirban and Aradhya supported me a lot by providing an environment to continue research work in home. I have no words to thank them.

I could never forget my school days with my friends, Pradip, Krishnapada, Soumya, and Kajal. I am very thankful to them for their love and well wishes.

Finally, I am thankful to all my teachers, friends from school to University and staff at Department of Computer Science and Engineering, Jadavpur University, and all my relatives for their well wishes. I am also thankful to staff members, and colleagues of Haldia Institute of Technology for providing me an environment to work with.

HIT, Haldia Arindam Giri

Date:

ABSTRACT

Internet of Things (IoT) has become an inevitable part of our life. Wireless sensor network (WSN) can be integrated into IoT to meet the challenges of seamless communication between things. IoT and WSN can be used in precision agriculture where data are collected from crop field and analyzed to take timely decision about farming. In precision agriculture application utilizing IoT and WSN, crop field can be better monitored. Farmers can take many decisions about farming like harvesting and irrigation. Sensors can be deployed in crop field to collect related data like humidity, temperature, nutrients, etc. with the help of IoT.

However, sensors have limited energy as they are battery-powered. Their limited energy is dissipated in sensing and sending data to other sensors. A sensor (known as mote) is generally battery powered with initial energy in the order of 1 Joule only. Generally, the battery is not replaced as the sensors are deployed in different environment and not easily reachable always. In smart precision agriculture using IoT and WSN, all operations like routing should be done in energy efficient way due to limited energy of sensors. To know the affected crop area, the sensors must be location-aware in precision agriculture. Again, as the sensors are vulnerable to many attacks like physical or network attacks the localization methods need to be secured in such application.

This thesis proposes a framework using IoT and WSN where agricultural processes will be automated. The application requirement for this is real-time monitoring and continuous sensing and transmission. These on the other hand require energy efficient WSN. An energy efficient routing protocol is to be developed for real time monitoring of agricultural field. Sensor nodes are vulnerable to many attacks also. For successful implementation of the framework the underlying WSN must be energy efficient and location-aware. Energy efficiency in data collection is achieved by clustering and routing while security is provided by a secure localization method. Hence, combining location-aware sensor nodes with energy-efficient clustering in WSN will be an effective IoT-based application in precision agriculture.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 WIRELESS SENSOR NETWORKS, APPLICATIONS, AND LIMITATIONS

Rapid development in electronics technology has made available low-cost tiny sensor devices, also called nodes. These available devices are capable of sensing many environmental parameters like temperature, humidity, pressure, etc. Large number of sensors may be deployed in a field. These are capable of communicating among themselves via radio channels. They form a network known as wireless sensor network (WSN) [1]. Application areas of WSNs vary from military surveillance, forest fire detection, precision agriculture, healthcare to smart transportation, and any many more [2]. For example, in a precision agriculture using WSN, sensors may be deployed in an agricultural field to gather soil moisture information along with location. Moisture data may be collected at sink node. Farmers may also get access data by using a customized application. Based on moisture data, farmers can understand which area in crop field becomes dried up. So, an automated sprinkler may be instructed to start irrigation soon in the dried up crop area.

The basic building block of a typical sensor is shown in Fig. 1.1. A sensor node is comprised of four basic components: sensing unit, processing unit, transceiver unit, and power unit. Based on applications, it can have additional components like location estimation unit, mobilizing unit, energy harvesting unit, etc. Sensing unit collects data from environment using sensor and converts analog data to digital form with the help of analog to digital converters (ADC). Sensed digitized data is processed by the processing unit in ord/er to be communicated by the transceiver.

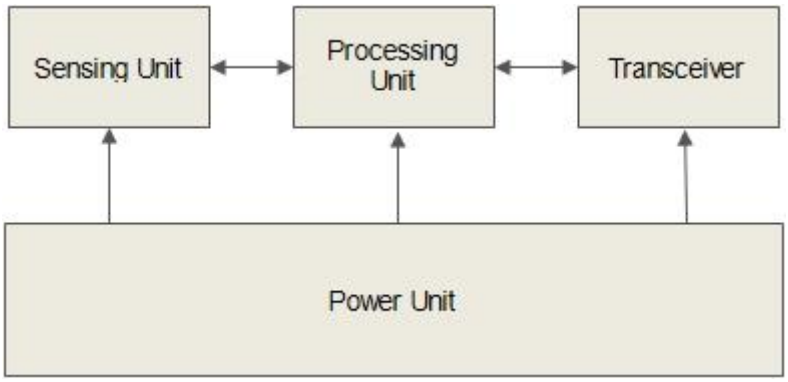


Fig. 1.1. Basic components of a sensor node

Sensors are battery powered tiny devices. Their limited energy is dissipated in sensing and sending data to other sensors. A sensor (known as mote) is generally battery powered with initial energy in the order of 1 Joule only. Generally, the battery is not replaced as the sensors are deployed in different environment and not easily reachable always. WSNs generally consist of one or more sink nodes which are responsible for collecting sensed data. Generally, it is likely that individual node sends data to sink node. In this process each node also loses energy. Closely placed sensors have redundant data. The nodes away from sink will require more energy to send to sink than those nodes which are nearer to sink. Thus nodes far away from sink dissipate more energy than that of nodes closer to sink. This fact makes far apart sensors die quickly, sometimes resulting in network partitioning. Not always nodes away from sink will be able to send data to sink without the help of other nodes that are relatively nearer to sink. So, a path needs to be formed from the source node to sink. All nodes in such a path will consume energy. However, the intermediate nodes in the path will act only as forwarders of the sensed data from the source. A WSN will last as long as its nodes live and not die. A node loses its energy as it senses data, sends data or forwards data. Hence, care must be taken to conserve energy in anode as long as possible, so that the WSN is able to function for long. Choosing an optimal path from source node to sink node and forwarding data along this path may save energy of sensor nodes. This process of finding a path for data to reach a destination node from source is known as routing. There is another topological view of WSN. The WSN is divided into the groups of nodes, called clusters, such that each cluster has a cluster head (CH) that oversees the gathering and forwarding of data to sink node. This technique is known as *clustering* which is depicted in Fig. 1.2. As individual nodes send data only to their CHs much energy is saved. Because sending sensed data directly to sink require more energy than that of sending to CHs. Although clustering offers an energy efficient way of data gathering, election of CH remains a burden. Cluster head election is based on the remaining energy, node density, etc. As CHs are computationally intensive nodes, overuse of them runs out of battery power. So, role of CHs is rotated among all nodes in the network to balance energy dissipation [3].

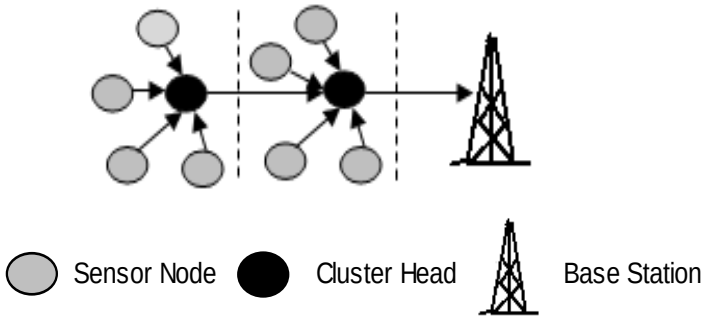


Fig. 1.2. Multi-hop clustering network

Internet of Things (IoT) is a new paradigm in Information and Communication Technology (ICT) today [4]. IoT is an interconnection of smart devices like cell phones, RFIDs, and sensors that are able to communicate among themselves using Internet. IoT provides seamless communication among smart devices. Some application areas of IoT are healthcare, smart city, agriculture, transportation and logistics. Better management of city resources like water, parking space, traffic etc. is possible in smart city towards serving citizens of a city. A traveller in a smart city may receive a message regarding available parking space or traffic pattern. By following free parking space, a visitor can park his or her car towards available space. Again, based on traffic pattern, a traveller can choose a route and drive his or her car accordingly. Wastage of water can also be restrained if usage pattern of water is observed in an area. Based on the usage pattern water delivery may be controlled centrally. For example, water supply time may be fixed for an area. Electric usage pattern can be obtained by deploying smart electric meters in houses. Load balancing of electric grid is possible if electric usage pattern in a city is known. WSN can act as the backbone of IoT. The potentiality of IoT may be explored in precision agriculture with the help of WSN. Different sensors for sensing various field parameters like temperature, soil moisture, and nutrients levels may be deployed in agricultural field in order to collect data of interest. A WSN can easily be formed with the deployed sensors in agricultural field. These data can then be made available to farmers through IoT. By analysing collected data farmers can control agricultural processes like irrigation, harvesting, etc. to produce higher crop yield and ensure better quality of crops. Economic growth of countries is possible by adopting smart precision agriculture. Effectiveness of such application can be improved by ensuring energy efficiency and location awareness of underlying WSN. Due to limited power, bandwidth, and computational capability of sensors, operations like routing, localization, etc. in WSN is challenging [5]. However, the challenges should be addressed for future potential WSN applications. In this work, energy efficiency of WSN deployed in precision agriculture is proposed to be achieved through clustering and routing protocols, while localization awareness is addressed by devising low cost and secure localization techniques.

Energy efficient WSN will serve such application for an extended period. On the other hand, localizing sensors precisely in field of interest will help farmers to take necessary steps. For example, a location-aware application will help farmers to precisely identify the affected area. Again, nodes in WSN are vulnerable to malicious attacks like sybil attack that may affect the accuracy of localization by forging one or more anchor identities. Hence, localization technique must adopt proper security measure to identify unreliable anchors and provide accurate localization against attacks in WSNs. If only reliable anchors are selected in localization, such a novel localization scheme can improve reliability of localization in terms of both security and accuracy. The more the accuracy of localization the higher become the QoS of WSN. Thus, combining location-aware sensor nodes with energy efficient clustering in WSN will provide an effective IoT-based application in precision agriculture.

1.2 MOTIVATION

Lifetime of WSN is measured in terms of the time to first node death (FND), time to half node death (HND), last node death (LND), ten percent node death (TND), etc. To obtain economic benefit, the lifetime of WSN deployed in crop field must be maximized. Clustering is one of the approaches to attain energy efficiency in WSN. Clustering divides the network into non-overlapping clusters each having one CH. Efficiency of clustering lies in electing the CHs. There are many CH election methods available in literature. Limitations of existing clustering techniques limit their usage in practical networks. Most of the techniques elect CH among all nodes in the network, thereby creating unbalanced clustering. Unbalanced clustering results in unbalanced energy dissipation which causes early death of a node. Efforts have been made towards balanced energy dissipation throughout the network by electing CHs based on various parameters such as residual energy of a node, node density around a node, distance of a node from sink, distance from centroid, etc. However, none of these has been accepted as the optimum. Clustering protocols are not generally adjusted based on application specifications. Fuzziness in network parameters addressed in [6] outperforms existing clustering algorithms.

As sensor nodes are battery operated, conservation of energy is important. The energy of a sensor node can be saved by many techniques like energy efficient routing [7], duty cycle scheduling [8], energy efficient MAC (Medium Access Control) [9], energy harvesting [10], and energy balancing. Energy efficient routing techniques [11] play an important role in doing so. Most of the routing protocols consider sensor nodes and the sink node as stationary nodes. However, in some situations the sink or the sensor nodes may be mobile. Hence, routing algorithms have to be able to handle mobility and topology changes in an energy efficient way. Several QoS aware WSN routing protocols are also proposed [12]. Thus, a variety of proposed WSN routing protocols are available that deal

separately with different parameters. The application requirement for these protocols is not look into always. This work focuses on precision agriculture. The application requirement for this is real-time monitoring and continuous sensing and transmission. These on the other hand require energy efficient WSN. An energy efficient routing protocol is to be developed for real time monitoring of agricultural field. However, a few research exists that addresses application requirements in sensor networks.

In precision agriculture, knowing the location in field of interest is sometimes needed to take timely decision about farming. Localization without GPS is made possible by estimating the distance between two nodes from the received signal strength indicator [13], time-of-arrival, angle-of-arrival. This process involves uncertainty and approximation error. Soft computing techniques like genetic algorithms, fuzzy logic, neural network, and ant colony optimization can solve the problems with uncertainty. Performance of localization algorithms depends on factors like number of anchor nodes, node density, computation overhead, accuracy, etc. Each algorithm has its own merits and demerits, making it suitable for different applications. Localization algorithms in WSN are either centralized or distributed. Centralized algorithms are suitable for applications requiring absolute accuracy as they provide more accurate locations. On contrary, distributed algorithms do not rely on large centralized system and potentially support better scalability, making them suitable for agricultural application. In distributed localization, the network is not flooded with the location messages by all nodes. So, due to low communication cost, sensors energy can be reserved and lifetime can be extended. Influence of factors like scalability, mobility, and heterogeneous data traffic as in IoT should be analysed here. Typical research challenges in localization include localization in ambient and noisy condition (e.g., humidity, interference), providing security during localization, localization in mobile wireless sensor network (MWSN) [14], and localization in three dimensional space. Localization may be affected if anchor nodes selected in localization are compromised by malicious attacks. Anchor nodes in localization must be secured against malicious attack. So, a secure localization method needs to be developed so as to defend malicious attacks.

Motivated by the above requirements and challenges the key research question is identified in the thesis- "How to provide energy efficient data gathering, low-cost localization, and security to localization for the framework so as to extend lifetime of underlying WSN and to know affected crop area precisely?" In order to address the key question, the following research problems are focused in the thesis:

1. What would be the framework for precision agriculture using IoT and WSN?
2. How data from crop field can be collected at sink in an energy efficient way so as to extend lifetime of underlying WSN?
3. How to develop low-cost localization for the proposed framework?
4. How to secure localization in such an application framework?

1.3 OBJECTIVE

The main aim of the thesis is to develop an energy efficient balanced clustering and routing protocols for underlying WSN in order to extend lifetime for underlying network in large applications like precision agriculture. This is achieved by electing good CHs and proposing an adaptive routing protocol for WSN.

The second aim of the thesis is to devise localization schemes for underlying WSN to provide precise location estimation and securing localization against attacks in sensor networks. A secure localization method is developed to provide reliable and accurate location estimation of sensor nodes in spite of malicious attack in WSN.

1.4 CONTRIBUTION

Inspired by the above-mentioned challenges and motivations, this thesis makes the following contributions:

- This thesis proposes a framework for agricultural process automation. In doing so it tries to optimize resources like water, fertilizers, and insecticides. WSN is utilized as a backbone of IoT-based application in precision agriculture. Various issues in implementing such an IoT and WSN based application are dealt with here.
- An energy efficient clustering using fuzzy logic is proposed to prolong network lifetime. Fuzzy logic is used to elect cluster heads and estimate underlying communication radii. Optimum routing path is established from cluster head to sink utilizing particle swarm optimization.
- Scope of energy harvesting in WSN is investigated in this research. An adaptive cross layer routing protocol is devised that offers trade off between energy harvesting time and active time for message transmission with the aim of increasing network lifetime. A cluster head election method is also proposed to ensure maximum network life time and higher throughput.
- This thesis presents range-free localization methods using fuzzy logic. Accuracy of localization is enhanced after uncertainties associated with localization are dealt with.
- In order to improve security of localization, a secure localization technique for WSN is proposed using information theory. The proposed localization technique is able to provide accurate localization even in case of malicious attack in WSN.

1.5 ORGANISATION OF THE THESIS

The rest of the thesis is organised in several chapters as follows. Chapter 2 presents an IoT and WSN based framework for precision agriculture. This framework helps in optimizing resources like water,

fertilizers, and insecticides in crop field using IoT. The issues involved in implementing such a wide application of WSN using IoT are investigated in this chapter.

Chapter 2 presents a review of existing literature. This chapter includes literatures related to energy-efficient clustering, localization, and security works in localization.

Chapter 3 proposes a framework for precision agriculture based on WSN and IoT. As the framework is based on IoT, this chapter includes a comprehensive survey on architecture, enabling technologies, challenges and applications of IoT prior to the framework.

Chapter 4 proposes energy efficient clustering and routing approaches for WSNs. It consists of two sections. In the first section, balanced energy dissipation is achieved by electing good cluster heads throughout the network. Establishment of energy efficient routing path for multi-hop data forwarding is also presented in this chapter to extend network lifetime. In the next section, an adaptive routing protocol for optimizing energy harvesting time in WSN. In this section, different hierarchical network parameters are calculated to maintain an energy harvesting schedule.

Chapter 5 provides localization methods based on fuzzy logic. This chapter includes single and multi-parameter localization methods for WSN. Uncertainty in location estimation is addressed in this section by fuzzy logic.

Chapter 6 presents a secure localization approach which gives accurate location estimation of sensor nodes even in sybil attack. Anchor nodes compromised with sybil attack are identified by information entropy and restrained from taking part in localization.

Chapter 7 concludes with an overview of the thesis along with its results, limitations, and future research directions.

CHAPTER TWO

LITERATURE SURVEY

Internet of Things leads us to a new era of Information and Communication Technology (ICT). IoT is a world-wide network of interconnected devices relying upon the infrastructure of ICT. It connects objects like mobiles, refrigerators, RFIDs, sensors, and many more. For example, sensors in a smart home application may send temperature values of a room to an individual over IoT. The individual then control the air condition to vary the temperature in the house. Similarly, a smart refrigerator may send information seeking attention to a technician for malfunctioning. There is a big market opportunity for device manufacturers, service providers and application developers. By 2020, billions of smart objects are expected to join in IoT. In [15], the market shares of IoT by 2025 is depicted. It shows that healthcare and related sector possess majority share while rest of the share is occupied by electricity, agriculture and security. Devices like refrigerator, washing machine, oven, bulbs, etc. will act as smart devices with computing and communication capabilities. They can be controlled from anywhere. Not only that, the interconnected devices will communicate with each other over the Internet thereby yielding a pervasive computing environment. However, there are many challenges to confront because of the device constraints and heterogeneous nature of IoT devices. Countries like India can be benefitted with application in agriculture using IoT. Using such application farmers will be able to monitor different field parameters like moisture, temperature, nutrients, etc. It does not need physical supervision of crop field. Even farmers can get expert advice about harvesting, irrigation, pest control, etc. Such an application not only increases quality production but can also save natural resources like water. Another major IoT application is foreseen in the domain of healthcare. Healthcare services can be offered to remote patients with IoT. Devices attached to a patient are able to send data like sugar level, pulse rate etc. to a doctor. After getting various data pertaining to a patient the doctor can advise medicines via patient's smart phone. Such application will help patient in getting advice sitting at home and keep hospitals free of crowd. Medicines can be attached with smart labels so as to read information regarding date of expiry, doses, price, etc. This way

counterfeiting of medicines can be prevented. Transportation is another application which will become smart with integration of IoT. Real time tracking of goods is also possible now-a-days. Goods or shipment trucks, packages can be attached with sensors will be able to provide location. Thus, we can track the location the goods, and can estimate delivery time thereafter. Nowadays, smart electric meters have come to the market. These can keep track of household electricity consumption, among many other features. Smart meters can send reading or even usage pattern of a city to an electric grid. The grid will be able to distribute electricity efficiently over cities. Another contribution of IoT is Ambient Assisted Living (AAL). Elderly people living alone in house can be monitored remotely using IoT. Their near ones can be notified on emergency after analyzing condition by healthcare professionals. Some of the home appliances like air conditioner can be automatically turned on or off even remotely over the internet. IoT have been successfully used in smart cities too. Traffic lights, parking space, water distribution, etc. in a smart city can be controlled by the use of IoT.

Popularity of IoT is made possible with the advancement in enabling technologies of IoT including identifying, communication, sensing and the middleware. A software layer called middleware is positioned between the IoT technical and application layers in order to balance the technical gaps among manufacturers [16], [4].

WSN can be integrated into IoT to build novel application like precision agriculture. In IoT-based WSN application for precision agriculture, different sensors may be deployed in field to collect variety of data like moisture, nutrients, and temperature. Data collected at sink may be communicated through IoT to stakeholders. However, integrating WSN into IoT is challenging due to limited capacity of sensors. Sensors in WSN are limited in terms of energy, computing, and communication capabilities. Clustering may be used for gathering data in an energy-efficient way in WSN where nodes are grouped into clusters having one cluster head each. In clustering, the cluster heads are in charge of gathering data from member nodes. But, the sensors utilized as cluster heads use up their energy quickly, creating energy hole in network. Hence, electing cluster heads in WSN attracts researchers in this domain.

Again, locations of data need to be known to stakeholders in such IoT-based applications for various purposes. The application may be vulnerable to attacks like sybil attack. Hence, we need to address energy efficiency and security in WSN.

This chapter presents a comprehensive review on energy-efficient clustering, localization, and security works in localization. It is organized as follows: Section 2.1 includes review works related to WSN clustering, Section 2.2 presents review works related to localization in WSN, and Section 2.3 includes review related to security in localization.

2.1 CLUSTERING IN WSN

Clustering is an energy-efficient solution of data gathering in WSN [17]. WSN is organized into several clusters with one cluster head each [17]. Clustering increases lifetime of WSN. Based on the method of election of CHs existing cluster-based routing protocols can be classified as: classical methods and fuzzy logic-based methods as shown in Fig. 2.1.

2.1.1 CLASSICAL CLUSTERING

In classical clustering, CHs are elected based on probabilistic model. The first cluster-based routing protocol is Low Energy Adaptive Clustering Hierarchy (LEACH) [18]. In LEACH, each node takes an autonomous decision to be a CH. Each node generates a random number between 0 and 1. If the random number generated by a node n is smaller than a predefined threshold, $T(n)$ (eqn. 2.1), the node is elected as a CH.

$$T(n) = \begin{cases} \dfrac{p}{1 - p * (r * mod\ 1/p)} & , if\ n \in G \\ 0 & , \text{otherwise} \end{cases} \tag{2.1}$$

where p is the required percentage of CHs, r denotes round number, and G is the set of nodes those have not been elected as CHs in previous $1/p$ rounds.

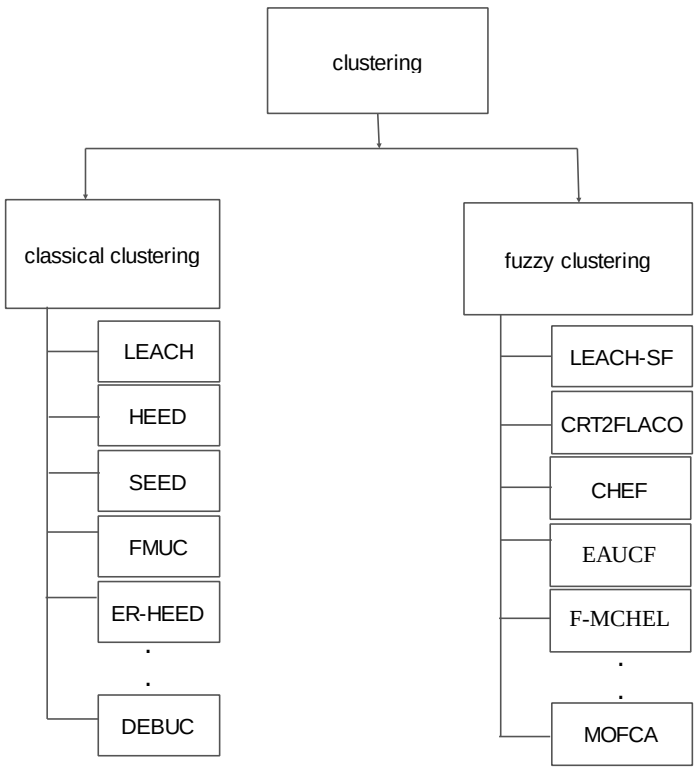


Fig. 2.1. Cluster-based routing protocols

Cluster heads gather data from member nodes and forward data to sink after aggregation. Although simple to implement, it causes early death of nodes. Residual energy of nodes is not considered in cluster head election. There are many improvements to LEACH like LEACH-C [19], LEACH-EP [20]. In LEACH-C, all nodes having energy higher than the average energy are considered as candidate CHs. The sink node runs a centralized simulated annealing algorithm to find the best CHs so as to reduce energy consumption by CHs. Election probability of CHs is optimized in LEACH-EP by introducing new threshold value. In fuzzy-based clustering, fuzzy logic is used to determine the chance of a node to become a CH based on parameters like residual energy [21], [6], [22]. In this section, an overview of recent clustering protocols used in WSN is provided.

Wang et al. [23] proposed a routing algorithm with mobile sink utilizing particle swarm optimization (PSO). PSO is used to form clusters in the WSN. One cluster head is elected in each cluster based on position of nodes and residual energy. To avoid hotspot problem in traditional multi-hop WSN, the sink is moved from one region to another. Simulation results demonstrate that this increases lifetime, transmission delay, packet delivery.

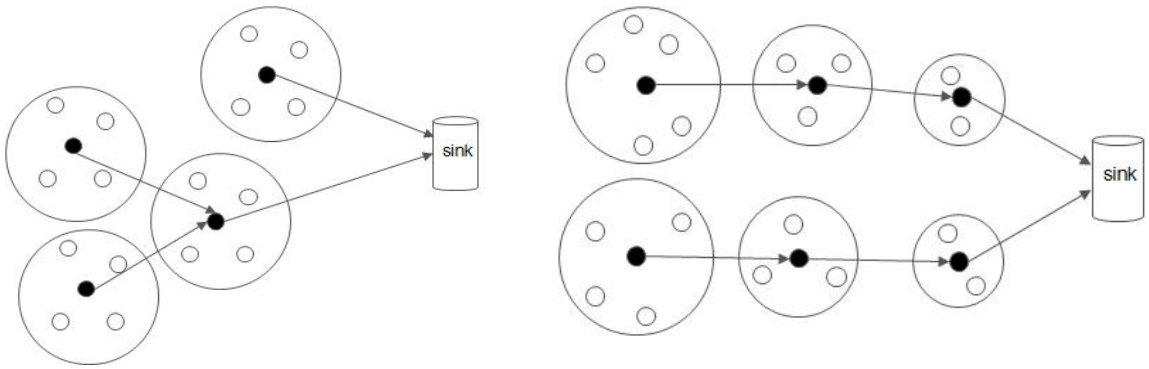
In [24], authors developed a hierarchical clustering algorithm to reduce network traffic towards sink. In the proposed secure energy efficient data transmission (SEED), cluster heads forward data directly to sink. The network is divided into three regions based on energy. Sensors with same application form sub-clusters in which only one awake node transmits data whereas others remain asleep. Following a sleep-awake scheduling provides prolonged network lifetime. Distributed energy efficient clustering (DEEC) [25] is a routing protocol developed for heterogeneous WSNs. Nodes are considered different with respect to battery energy and hardware complexities. In DEEC, the election of cluster head is based on the ratio of residual energy and the estimated average energy of network. There are many improvements to DEEC like EDDEEC and IDEEC. The authors in IDEEC [26], achieve better performance than DEEC and EDDEEC by improving cluster head election probability and optimizing estimated average energy of network.

In [27], optimum path selection in WSN routing is proposed using Honey Bee Optimization technique. It consumes less energy and transmission time. It outperforms other algorithms using ant colony optimization and particle swarm optimization in terms of throughput, link quality, and energy consumption.

An uneven clustering algorithm for WSN in IoT-based applications is developed in [28]. It achieves energy efficiency through uneven clustering. Cluster head rotation is followed in order to balance energy dissipations among nodes in a cluster. To alleviate energy hole problem, a dynamic multi-hop routing algorithm is followed. This algorithm attains better throughput, lifetime, and energy efficiency. Authors in [29] provide a clustering algorithm for WSN used in IoT applications. For electing cluster head a modified equation for threshold value calculation is used using initial energy

and residual energy. This ensures electing a node with higher energy as cluster head. Optimum number of clusters in WSN is also estimated by an equation. This algorithm outperforms low energy adaptive clustering hierarchy protocol in terms of energy consumption, lifetime, and throughput.

A distributed clustering algorithm for multi-target WSN is demonstrated in [30]. Nodes with same target form cluster in the network. An effort is also made for topology optimization in view of minimizing limited sensor resources. Simulation results prove that this approach is well suitable in fusion and tracking. Network lifetime is also enhanced due to distributed clustering approach. In [31], an algorithm for energy efficient clustering in WSN using game theory and dual cluster head election method is proposed. Reduction in energy consumption through rotation of cluster head is made possible by dual election of cluster head. Energy consumption among cluster heads is balanced by a proposed non-cooperative game model. Simulation results demand energy efficiency of clustering approach.



(a) (b)

Fig. 2.2. Size-based WSN clustering: (a) equal size clustering (b) unequal size clustering

Based on the size of clusters clustering protocols are of two types: equal and unequal clustering, as shown in Fig. 2.2. In equal size balanced clustering protocol like ER-HEED [3] and HEED [32] each cluster has same size. This means that each CH has same communication radius, no matter how apart they are from BS. In equal clustering, CHs closer to BS use up their energy quickly than other CHs due to inter-cluster and intra-cluster traffic. In this situation, energy hole is created near BS. This protocol elects CHs based on remaining energy. Lifetime of network is extended as nodes join with clusters with minimum communication cost. Hybrid Energy-Efficient Distributed Clustering (HEED) [32] is an efficient algorithm in WSN routing. It follows multi-hop data communication to sink. Unlike LEACH protocol, residual energy of nodes is considered to elect a cluster head. Tie breaking is done based on degree of node, distance to neighbor, and intra-cluster energy. But, due to more number of cluster heads hotspot problem remains in the WSN. Authors in [33] presents a cross layer routing protocol with energy harvesting. This research proposed an energy efficient routing protocol

based on cross layer. An energy harvesting method is also prescribed to help nodes gaining energy from non-conventional energy sources like thermal energy. This approach outperforms LEACH and HEED in terms of remaining energy, and lifetime of WSN.

Energy hole problem exists in equal clustering since nodes closer to BS die quickly due to inter-cluster communication. In unequal clustering, clusters closer to BS has smaller radius than that of the clusters away from BS. In unequal clustering protocols like UHEED [34], CHs are elected based on residual energy and node degree or node proximity to its neighbor. This protocol calculates competition radius to create unequal clusters based on distance from BS. As a result, there are more inter-cluster traffic and less intra-cluster traffic closer to BS. It prevents early death of nodes closer to BS. Thus, it overcomes the energy hole problem as faced in HEED. RUHEED [35] is an improvement of UHEED with introduction of rotation of CHs to reduce number of cluster head election phases. The current CH elects one of its member nodes with highest residual energy. The election process is deferred until one of the nodes dies. Ullah et al. proposed ER-HEED [3] (energy based rotated HEED), which reduces number of HEED election phases by rotating CHs among cluster members based on remaining energy.

Qiang et al. proposed Distributed Energy Balanced Unequal Clustering (DEBUC) [36] where radius of each cluster is calculated based on distance to BS. Clusters closer to BS have smaller radius, hence, hoptspot problem is addressed. Election of CHs is made by a competition algorithm based on time. The broadcast time of CH is calculated depending on residual energy of CH and neighbor nodes. Energy-aware multi-hop routing is considered in DEBUC to avoid hot-spots problem. In [37], a Feedback Mechanism-based Unequal Clustering (FMUC) is proposed to avoid energy hole problem in heterogeneous network. In each round, cluster sizes are dynamically adjusted based on feedback calculated by the BS to balance energy dissipation of each nodes. In [38], Rotating Energy Efficient Clustering for Heterogeneous Devices (REECHD) is proposed where CHs are elected based on residual energy and node induced work. The node induced work is determined by transmission rate of nodes. Network lifetime is extended by introducing intra-traffic limit rate (ITLR) and CH rotation. All clusters are supposed to follow ITLR. REECHD outperforms HEED and ER-HEED in heterogeneous WSN.

2.1.2 FUZZY LOGIC-BASED CLUSTERING

Uncertainty in choosing CHs in WSN clustering is managed by fuzzy logic. This section presents fuzzy logic-based literature. Fuzzy inference system (FIS) is a mathematical model which maps inputs to outputs based on fuzzy set theory. In existing fuzzy-based clustering protocols equal clusters are formed in the network [39], [6]. So, the CHs near to BS dissipate more energy due to intra-cluster and

inter-cluster traffic forwarding which creates energy holes. Hence, these protocols can't contribute in extending lifetime of WSN. In [6], the authors propose an equal clustering where CHs are elected utilizing type-1 fuzzy logic (T1FL). However, CHs follow single-hop communication to send aggregated data to BS, so may create energy hole near BS. This protocol does not support large application like crop monitoring as multi-hop data forwarding is not considered. In [22], authors proposed an adoptive and flexible unequal clustering algorithm for multi-hop WSN using T2FL.

CHEF [40] is a clustering protocol which considers two fuzzy parameters: remaining energy of nodes and local distance to elect a CH locally. Local distance of a node N is defined as the sum of distances between N and the nodes within r distance from N. It is a distributed approach in which nodes generate random number. If the random number is smaller than a threshold, the node calculates chance to be CH using fuzzy inference system. Rest of the phases is similar to LEACH [18].

The authors in F-MCHEL [41] used two fuzzy parameters-energy and proximity distance to elect CH. This algorithm is an extension of CHEF. Among the elected CHs one Master Cluster Head (MCH) is elected with maximum energy. Only the MCH aggregates messages and forwards to sink. LEACH-ERE [21] is a distributed fuzzy clustering algorithm which similar to CHEF except in determining fuzzy chance to be CH. In this work, fuzzy logic is used to elect CHs based on residual energy as well as expected residual energy (ERE). To the best our knowledge, this is the first algorithm to use expected residual energy. The expected residual energy of a node to be CH after steady state is calculated as the difference between the residual energy and the expected consumed energy after steady state. LEACH-FL [39] is an improved version of LEACH which elects CHs using fuzzy logic based on residual energy, distance from sink, and node density.

In iCSHS [42], authors proposed an integrated clustering and routing using meta-heuristic algorithms. The PSO-UFC, a PSO based unequal and fault tolerant clustering protocol is developed in [43]. CRT2FLACO [44] is proposed using both type-2 fuzzy logic (T2FL) and ant colony optimization (ACO). Mamdani type-2 inference system is utilized to find a node's probability to become CH based on residual energy, node density, and distance from BS. Packets are sent to BS following multi-hop path via selected CHs using ACO. Then, CHs are elected using T1FL based on remaining energy, distance from sink, and concentration of nodes.

In Energy Aware Unequal Clustering with Fuzzy (EAUCF) [45], CHs are periodically rotated by considering fuzzy descriptors: residual energy and distance to sink, and probabilistic models. However, EAUCF is not able to address hotspot and energy hole problems in static and mobile WSN.

Multi-objective fuzzy clustering algorithm (MOFCA) [46] solves the limitation of EAUCF. MOFCA is an energy-efficient distributed unequal clustering approach which addresses both hotspot and energy hole problem in stationary as well as evolving network. MOFCA elects final CHs via

energy-based competition among tentative CHs, chosen initially by a probabilistic model based on remaining energy, distance to sink, and node density. Fuzzy logic is used in estimating competition radius of sensor nodes. It outperforms other equal and unequal clustering algorithms like LEACH, CHEF, EAUCF in terms of FND, HND, and total remaining energy.

The work in [22] describes an adaptive and flexible fuzzy clustering algorithm for enhancing lifetime of WSN. Uncertainties in WSN are handled through T2FL in electing efficient CHs based on remaining battery power, distance from sink, and concentration. It provides better scalability and lifetime in comparison with LEACH single-hop and multi-hop, and T1FL-based protocol. However, optimum routing path selection is not taken care of in this work.

In LEACH-SF [6], initially, FCM is used to create balanced clusters over the network. Then, CHs are elected via type-1 Sugeno fuzzy inference system based on residual energy, distance from sink, and distance from cluster centroid. The fuzzy rules of LEACH-SF are adjusted by artificial bee colony (ABC) algorithm. The fitness function of ABC is designed as a linear combination of FND, HND and LND. However, it generates equal clusters which causes energy hole near BS. Moreover, this clustering technique doesn't follow multi-hop path while sending packets to BS. A cuckoo optimization-based routing algorithm is proposed in [47]. The authors in [48] propose static clustering by FCM method where fuzzy logic is used to elect CH and multi-hop routing.

Load balancing in clustering is addressed in [49] by approximation method in grid structure. A mobility assisted adjustable range based clustering is proposed in [50].

2.2 LOCALIZATION IN WSN

Knowing the accurate location of nodes in WSN is a major concern in many location-dependent applications. Especially in agricultural monitoring, accurate location of affected crop area is required for effective use of fertilizers or pesticides. Low cost and accurate localization algorithms need to be developed for such applications.

Broadly, localization algorithms can be classified as: range-based and range-free. The range-based algorithms estimate locations of sensors by measuring absolute range measurements like distance [51], time of arrival [52], RSSI value [53], and angle of arrival of received signal [54],[55],[56]. Though range-based algorithms provide accurate location estimation, they need additional hardware. On the other hand, range-free algorithms do not rely on absolute range measurement but on other metrics like proximity and hop count. They provide lower location accuracy than that of the former, but do not require additional hardware. So, localization using range-free method is cheaper than the former.

One of the classical localization algorithms is DV-Hop [57]. The positions of unknown nodes are estimated after getting position information from nearby anchor nodes. The DV-Hop is based on the concept of distance vector routing. It works in three phases. In first phase, all nodes in the network get distances to anchor in hops by exchanging distance vector. In the second phase, each node calculates the average hop size. Then unknown nodes estimate their positions with the help of known anchor positions in the last phase. The limitation of DV-Hop algorithm is that it assumes all anchors contribute equally in localization process. Range-free localization like DV-Hop has become popular over the years due to its simplicity and that too without complicated hardware. To get rid of the problem, the anchors are assigned weights reflecting their impact on location estimation for an unknown node. In weighted DV-Hop algorithm [58], the weight of an anchor is calculated as the inverse of hop-count. In [59], each anchor node calculates its own hop-size as the weighted sum of all average one-hop distances (HWDV-Hop) to all anchors. The proposed algorithm estimates the average hop-size for the network by average hop-size weighted mean. HWDV-Hop demands that it outperforms DV-Hop in terms of localization accuracy.

Improved Weighted DV-Hop (IWDV-Hop), proposed by Guadane et al. [58] is an improved version of DV-Hop algorithm which uses inversely weighted hop-count in location estimation. It considers not only a closer anchor to estimate unknown location but also it uses a far away anchor with accurate hop-count. It outperforms DV-Hop and HWDV-Hop in terms of localization errors.

A range-free location estimation technique is proposed using a proximity metric and regulated signature distance (RSD) [60]. RSD is introduced in order to overcome weakness RSSI measurement. RSSI measurements are irregular due to multipath effect, radio propagation loss, or other hardware failure. Here, a node performs an ordering of 1-hop neighbor nodes based on the decreasing values of RSSI values. Then, proximity relationship is established by introducing signature distance. This algorithm provides accuracy in location estimation even in unevenly distributed radio path loss. In [61], a range-free localization based on sequential Monte Carlo is proposed for WSN. The well localized nodes help in knowing the locations of other unknown nodes. The limitation of distance estimation using hop count is addressed in [62]. The authors in [62] use existing information communicated between anchor and sensor node pair. This approach improves accuracy of localization in terms of average location estimation error.

A range-free localization using mobile anchor node is proposed in [63]. Initially, a sensor node estimates its position within the region covered by two distant anchor nodes. Later on, the sensor node verifies its position within the region using third anchor node. The anchor node is moved in the localization following a predefined trajectory. This algorithm is simulated with many varying parameters like deployment density, communication range, and trajectory. It outperforms other algorithms in terms of average localization error.

In [64], authors proposed a range free APIT localization method which divides the network into overlapping triangles. An unlocalized node elects three anchor nodes to form a triangle and performs

a point-in-triangle (PIT) test if it lies inside the triangle. PIT test is applied again to find another combination of anchor nodes to form triangle. Finally, the location of unlocalized node is calculated as the centre of gravity of all intersecting triangles. Due to simplicity and high accuracy of location estimation, APIT becomes one the most widely use localization algorithms. However, selecting suitable triangles of anchor nodes in APIT is an issue. Triangles with inappropriate sides (e.g., narrow triangle) generate error in location estimation. There are many improvements to APIT in order to improve location accuracy [65],[66],[67], [67]. In [68], a cost-effective localization is proposed using APIT, RSSI values, and particle swarm optimization (PSO). The distance of sensors from anchor nodes are initially determined from the RSSI values. Locations of neighbour nodes are estimate using the measured distances. Then, the accuracy of location estimations are improved by PSO algorithm.

Localization error in RSSI-based localization is effectively reduced by applying outlier detection in [69]. This algorithm removes non-line-of-sight anchor node with outlier distance in estimation of location. It performs a clustering on location estimates by trilateration. The centroid of the grid with highest number of mapped location is considered as the final location of a sensor. As it removes outlier, localization error is significantly reduced.

Nature-inspired metaheuristic algorithms are also used perform node localization in WSN. In [70], a localization scheme is proposed using butter fly optimization algorithm. Particle swarm optimization (PSO) [71], genetic algorithm (GA) [72], firefly algorithm [73], and hybrid algorithm [74] used in literature to improve accuracy of localization.

The role of medium access control (MAC) protocol in WSN localization is investigated in [75]. This range based localization method divides the network into clusters. Then, MAC protocol is modified to conserve energy by limiting coverage of nodes up to a certain hops. The performance of the algorithm is analysed in terms of average location error and average energy consumption.

Fuzzy logic is also used in WSN node localization. Different anchor nodes have different influences on node localization. Fuzzy logic is used to assess the weights of anchor nodes based on RSSI values in [76]. Expected energy consumption of nodes in localization is also calculated based on RSSI distance and residual energy of nodes. Finally, locations of nodes are estimated trilateration and weighted centroid method. Simulation results reveal that this algorithm provides an energy efficient and accurate localization technique.

2.3 SECURITY RELATED WSN WORK

Due to inherent limitations of WSN nodes and deployment environment, security remains a challenge. The nodes in WSN are vulnerable to many attacks. Nodes once compromised by attackers, become threat in network. This section presents a comprehensive review of security related works in WSN. In *selective forwarding*, attackers compromise nodes to forward selective messages while dropping few messages. The selective dropping attack tricks neighbouring nodes that they lie in shorter route as

packet delivery latency is decreased. On the contrary, attackers in *sinkhole attack* compromise one node to attract traffic destined for BS towards itself, then forward all or selective traffic to BS. The compromised node gains influence over neighbours in such attack by providing a high quality route. For example, an adversary uses a powerful transmitter in forwarding traffic to BS in a single hop so to offer a high quality route. Sinkhole attack creates a scope to other attacks like selective forwarding to tamper messages. *Wormholes* are another attack that prevails in wireless sensor network. In wormhole attack, an adversary tunnels messages received in one part of the network and replays them in another part. This attack convinces the nodes that they are closer to BS (one or two hops away) although they are far away from BS. An adversary close to BS may completely disrupt routing by creating a well-placed wormhole. In *sybil attack*, a single node forges many identities to the network. In geographic routing in WSN, packets destined to specific location may be sent to compromised nodes as a sybil node belong to many geographical locations simultaneously. Anchor nodes in WSN localization may be compromised by sybil attack. Localization with the help of compromised anchor nodes leads to location estimation error and may collapse location-aware application in no time. In Fig. 2.3, malicious node S forges two sybil identities $S1$ and $S2$. The sensor nodes send data to sybil nodes. Among all attacks in WSN, sybil attack dangerous in the sense that it could not be detected easily. As the aim of the thesis is to develop a location-aware application of WSN in precision agriculture, this thesis concentrates on addressing sybil attack to secure localization.

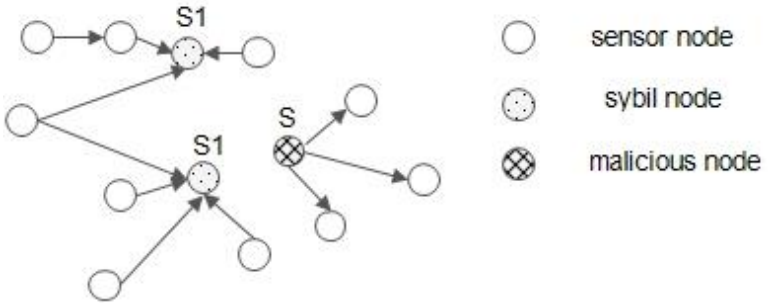


Fig. 2.3. Sybil attack model in WSN

In ROPE [77], localization is secured through verification of sensor locations prior to data gathering. However, the requirement of a nanosecond precision counter makes it unsuitable for WSN. A secure localization based on RSSIs and multi-dimensional scaling is proposed in [78]. With fewer hardware, it can only fight against naive adversaries. A local semi-definite programming technology was adopted in [79] to improve the localization accuracy. In [80], an attempt is made to detect uncontrolled enlargement attacks by monitoring the accuracy of position estimates and by increasing the precision of the multi-lateration scheme. In order to achieve security this research defines a minimum number of anchor nodes. Based on [80], authors in [81] provides secured localization by

eliminating anchors with a single mobile drone. However, path planning for the drone remains a challenge.

Lazos et al. [82] proposed a secure localization scheme, SeRLoc which detects sybil attack using reliable locators. The locators send beacon messages to sensors and sensors in turn, calculates their location based on locations of anchors. By using majority-voting, an overlapping antenna region is calculated. Each unknown node estimates its location as the center of gravity of the overlapping area. This work employs two security mechanisms: encryption of beacon messages and locator ID authentication by symmetric key. SeRLoc can protect against wormhole and sybil attack in localization.

An improvement of SeRLoc [82] was proposed in HiRLoc [83]. A sensor node computes its location (an area rather than a single point) as the region of intersection (ROI) of all the sectors covered by antenna. In order to provide better location estimation, this work reduces size of ROI by antenna rotations and variable transmission powers. Authentication of the beacon transmissions is made possible by symmetric key cryptography. Though HiRLoc can address sybil attacks, it is costly in terms of computational and communication complexity.

In [84], authors devised a sybil detection scheme based on RSSI measurement. The receiver node calculates RSSI ratio with the help of three cooperating nodes. Whenever the difference of RSSI ratios of two nodes becomes less than a predefined limit, the senders are treated sybil nodes. Wen et al. [85] followed time difference of arrival (TDOA) of packets in order to detect sybil attack. If two identities possess the same TDOA ratios for two sessions, they are called sybil nodes. In [86], attack detection is based on angle of arrival (AOA). Sybil attack creates multiple identities with the same physical location. To detect sybil attack, a trust value among the adjacent nods are calculated based on signal phase difference. Whenever the signal phase difference goes below a trusted threshold for adjacent sensor nodes, they are considered as sybil nodes. In [87], a robust localization called TMCA is proposed to defend against well-known attacks including sybil attacks, wormhole attack, and sinkhole attack in WSN. To do so, this algorithm first partitions the set of all location references into two clusters: malicious cluster and normal cluster. The malicious reference cluster consists of compromised anchor nodes. Then, malicious anchor nodes are determined by running a simple test.

Liu et al. [88] devised an improved RSSI-based sybil detection scheme using reputation module and adaptive threshold. This algorithm consists of suspicious node screening phase and sybil verification phase. In the first phase, monitoring nodes find neighbours as suspicious nodes whenever the difference between any two measured distances lies below a predefined threshold error. The monitoring nodes use a reputation model to evaluate the reputation values of neighbours based on transmitted and received packets. A node with highest reputation value is elected as a detection node. In the second phase, the detection node verifies the RSSI values of suspicious nodes to finally detect sybil nodes. This work is a low cost sybil detection scheme. However, this work assumes that monitoring nodes are not compromised.

In SF-APIT localization [89], sybil attack is detected based on RSSI values. In this work, two anchors are detected as sybil nodes if their RSSI difference lies below a threshold value of error. The threshold value of RSSI error is obtained by adding the sum of mean error of RSSI readings to a small tolerance value. In a hostile WSN environment, radio signal is subject to physical obstacles or associated with different propagation errors like multi-path fading. Hence, RSSI values calculated by a node are not necessarily correct; rather they are uncertain and random. However, to detect sybil attack, SF-APIT depends solely on the difference between two uncertain RSSI values. Thus, in the above-mentioned circumstances, scheme like SF-APIT does not guarantee secure localization against sybil attack in distributed WSNs, rather sybil nodes may remain undisclosed.

2.4 CHAPTER SUMMARY

This chapter presents a state-of-the-art of clustering and localization in WSN. As the aim of the thesis is to propose an energy-efficient and location-aware application of WSN over IoT, this thesis includes literatures related to clustering and localization. However, in doing so, the thesis has also considered secure localization. In clustering, cluster head election attracts more research efforts as energy is depleted more by the cluster heads than other nodes. Electing a cluster head in harsh environment involves uncertainty in many respects. So, applying fuzzy logic may be considered as the best approach in electing cluster heads. Again, locations of sensors need to be estimated in many applications of WSN. Such a localization technique must be accurate and light weight. Even though the sensors are compromised by attackers, localization techniques must be capable of providing accurate location estimation.

As the thesis considers IoT-based large scale application of WSN in Chapter 1, an exhaustive survey of IoT is included in the next chapter. Chapter 3 presents the architecture, underlying technologies, and popular applications of IoT along with a framework.

CHAPTER THREE

FRAMEWORK FOR IOT-BASED APPLICATION OF WSN IN PRECISION AGRICULTURE

The Internet of Things (IoT) [90] is a novel paradigm in Information and Communication Technology (ICT) today. IoT is seen as a world-wide network of different heterogeneous physical objects: devices, vehicles, buildings, sensors, actuators, mobile phones, Radio Frequency Identifiers (RFID) [91] and many more for making a smart environment. This ultra modern technology is going to make daily life easier by providing smart technological environment. Though the term Internet of Things is widely used today but it is hard to find from the existing literature what IoT means and what are the implications of IoT on social, economic and technology fronts. Irrespective of the fuzziness around the term IoT, it is obvious that in near future we shall be accompanied by any-time, any-thing, any-where content and services that will yield a new a way of living. Thus it can be easily predicted that IoT will reduce human effort and it will also ensure the smartness of an application by optimizing resource utilization of any environment. The IoT reference model can be represented by four layers (application, service support / application support, network, and device layers). Each layer is accomplished with management module and security module for providing efficient and secure system.

IoT has different fields of application areas, like smart home environment, smart health care system, smart precision agricultural system etc. [4]. However, no such evidence is found towards wide use of IoT in agriculture in third world countries. Therefore we are in need of a framework for the same. This chapter presents a framework for precision agricultural system. The precision agricultural system will be the result of integrating existing agriculture system with IoT and WSN.

This chapter consists of two sections. Section 3.1 includes a comprehensive survey on IoT as the framework is based on IoT. As the framework is IoT-enabled this section includes a comprehensive survey on IoT. Based on the survey a framework is proposed in the next section. Section 3.2 gives a framework of IoT-based WSN application for optimizing resources (water, fertilizers, insecticides and manual labour) in agriculture [92].

3.1 IOT ARCHITECTURE, ENABLING TECHNOLOGIES, AND APPLICATIONS

"Internet of Things" is envisaged to be a world-wide network of interconnected unique Internet-enabled e-devices, based on standard communication protocols. Objective is to have internet-enabled things including computers, mobile phones, RFID tags, to name a few, with unique address connected to the network dynamically, and interact on collaborative basis to fulfil different tasks like e-health, precision agriculture, smart city, ambient assistant living, and many more. IoT offers a big market opportunity for device manufacturers, service providers and application developers. It is estimated that 212 billion smart objects will join the IoT by 2020 [93]. Authors in [15] have given a clear picture on different market shares of IoT by 2025. Out of $2.7 to $6.2 trillion economic growth by IoT itself, healthcare and related sectors (possessing 41%share) are expected to create an annual growth of $1.1- $2.5 globally by 2025. The impact areas next to healthcare are manufacturing 33%, electricity 7%, agriculture and security 4% each of total economic impact of IoT. In the near future, all devices like refrigerator, washing machine, microwave oven, etc., will be turned into smart devices with computing and communication capabilities. The interconnected devices will keep on sharing information globally over the Internet. This will develop a pervasive computing environment. Transportation and home automation industries are growing rapidly with IoT. Wireless Sensor Network (WSN) is implemented in many application areas for collecting environmental or physiological information. Without WSN, IoT cannot be built. But due to scalability and heterogeneity of IoT, there are challenges to incorporate them within the WSN. The potentiality of IoT can be exploited in many domains like healthcare, transportation, environmental monitoring, personal and social, smart city, industrial control, and many more.

Several survey works have been done on IoT. These cover many aspects of it. IoT architecture and challenges to develop applications are included in [94]. A state of the art review on enabling technologies, protocols, application and research challenges is detailed out in [4], [95]. Existing IETF standards and challenges are included in [96] while communication technology and WSN elements are discussed in [1]. The middleware is a software layer interposed between the technological and the application levels. The middleware for IoT is surveyed in [97],[98]. Recent advances in IoT protocol stack unveil a possibility of future IoT based on the stable and scalable Internet Protocol (IP). Service composition which is essential for efficient exchange and aggregation of data and events has also been introduced by IP networked things in various application domains. Han et al. explain the practicability of the future full-IP IoT with real-time Web protocols and discuss the research challenges of service composition in [99]. To the best of our knowledge, no survey covering all aspects of IoT like enabling technologies, protocol stack, standards, middleware solution, related projects, application, and research challenges is available in literature. This chapter presents a comprehensive survey on recent advances in IoT including the mentioned above, while pointing out their limitations.

The rest of this section is organized as follows: Section 3.1.1 describes state-of-the-art of IoT architectures. Enabling technologies of IoT are presented in Section 3.1.2. Section 3.1.3 presents important application areas of IoT. Section 3.1.4 explains IoT initiatives by different countries and organizations through related projects and standardization activities. Challenges and research directions in IoT are mentioned in Section 3.1.5.

3.1.1 IOT ARCHITECTURE

As IoT deals with heterogeneous connected devices, a flexible layered architecture is needed to support them. In spite of many proposed architectures none of them can be accepted as a general architecture. Even the existing TCP/IP based Internet architecture is not able to handle such a large and often complex network as IoT. There is a need for a new architecture that will be able to handle such a huge IoT network and address challenges like scalability, Quality of Service (QoS), privacy and security of stakeholders and information/data. As IoT handles data belonging to various devices (owned by stakeholders), security aspects particularly, confidentiality and integrity along with privacy become utmost important. It must have security measures against unauthorized use/change of personal data. Individual IoT devices and service providers must be secured from attackers. For example, tampering of smart meter or smart watch must be brought to the knowledge of provider or owner immediately. Hence, security may be considered to be more than necessary in an IoT network.

In Fig. 3.1, different architectures proposed for IoT are depicted. Among the architectures for IoT proposed so far-[16], [90], [100], [101], some of them are application-specific while others are general purpose. The generic architectures are proposed as multi-layered concept. Multi-layered IoT architectures can be classified as: 3-layer architecture, 4-layer architecture, 5-layer architecture, and 6-layer architecture [4]. Among the recently proposed IoT architectures [16], [90], [101], the Service Oriented Architecture (SOA)-based model is most prominent in the 5-layer category. It encourages middleware technology. More details about middleware technology can be found in Section 4.2.

A comparison of different architectures based on reliability, security, scalability and QoS is done in Table 3.1.

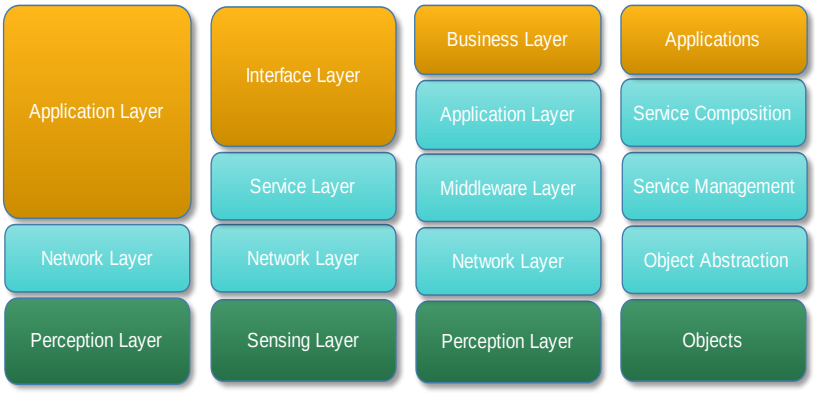


Fig. 3.1. IoT Architectures: a) Three layer, b) 4-layer, c) 5-layer, and d) SOA-based [4]

Table 3.1. Comparison of layered architectures

Model	Reference	Security	Scalability	Reliability	QoS
3-layer	[91]	X	x	x	x
4-layer	[102],[90],[103]	√	x	x	√
5-layer	[4]	√	x	x	x
SOA	[98],[97]	√	x	√	√

3.1.2 ENABLING TECHNOLOGIES

Realization of IoT is made possible through the integration of information and communication technologies (ICT) in the form of hardware and software. This section briefly discusses state-of-the-art of key players in IoT and mentions the design challenges.

A. IDENTIFICATION, SENSING AND COMMUNICATION TECHNOLOGIES

Every object in IoT must be identifiable. Electronic Product Code (EPC) and ubiquitous code (uCode) [104] are popular in IoT for this purpose. Addressing is performed in order to make IoT objects globally identifiable. IPv4 and IPv6 provide addressing in the communication network. 6LoWPAN [105] is used over IPv6 for low power wireless network. Development in wireless technologies has led us to a new era where almost all objects are attached with radios. Radio Frequency Identification (RFID) [91] plays a major role in this context. RFID promotes development of a cost effective solution for universal pervasive computing [106]. RFID system is composed of one or more RFID readers and several RFID tags. Tags provide unique identification while readers transmit appropriate signals to and from the tag. The detailed physical configuration of RFID system can be found in [107].

WSN plays a significant role in IoT. WSN is a network of large number of intelligent sensors that are able to collect, process, disseminate and analyze data [1]. WSN has been successfully used in environmental monitoring, military applications, precision agriculture, smart health, automation and control, etc. Nodes in WSN communicate among themselves to transmit data in single or multi-hop to the sink.

Typically, WiFi, Bluetooth, IEEE 802.15.4 are used for communication in IoT. WiFi uses radio signal to provide communication among smart devices within 100 m range [108]. Near Field Communication (NFC), which works at 13.56 MHz, is also used in IoT. It provides a data rate of 424 kbps and an application range upto 10 cm [109].

Bluetooth encourages low power communication over short distances among devices [110]. IEEE 802.15.4 standard has limitation that it defines physical layer and Medium Access Control (MAC) layer for low power wireless personal area network, but doesn't have specifications for higher layers in protocol stack. A glimpse on existing wireless communication standards that may be used in IoT, is shown in Table 3.2.

Beside the aforementioned wireless communication standards, different groups formed by World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), EPC Global, Institute of Electrical and Electronics Engineers (IEEE) and European Telecommunications Standards Institute (ETSI) have devised M2M communication protocols. The Constrained Application Protocol (CoAP) [111], [112] is an application protocol developed by IETF. It defines web transfer protocol based on REpresentational State Transfer (REST) on top of Hyper Text Transfer Protocol (HTTP). CoAP enables tiny devices with low power and computational capabilities to utilize RESTful interactions.

Table 3.2. Communication technologies in IoT

Communication protocol	Transmission range	Transmission rate	Spectrum
RFID	50 cm/50 cm/3 m/1.5 m	424 kbps	135 KHz/13.56 MHz/960MHz/2.4 GHz
Bluetooth	10 m	1 Mbps	2.4 GHz
WiFi	100 m	50 – 320 Mbps	2.4/5.8 GHz
NFC	10 cm	100 kbps – 10 Mbps	2.45 GHz
ZigBee	10 m	256 kbps/20 kbps	2.4 GHz/900 MHz
Wi-Max	50 km	70 Mbps	2 – 11 MHz
UMTS/CDMA/EDGE	~	2 Mbps	896MHz
IEEE 802.15.4	10 m	20/24/250 kbps	868/915/2400 MHz

The Message Queue Telemetry Transport (MQTT) is a lightweight messaging transport protocol developed by Andy Standford Clark of IBM and Arlen Nipper of Eurotech [113]. It connects embedded devices and networks with applications and middleware. MQTT is said to be an optimal connection protocol for the IoT and M2M as it uses different routing mechanisms like, one-to-one, one-to-many or many-to-many for connection operation. The Extensible Messaging and Presence Protocol (XMPP) is an IETF Instant Messaging (IM) standard which is used for voice and video calling, multi-party chatting [114]. It promotes open, secure and spam-free communication between users by instant messaging. Authentication, privacy management and access control are also supported by XMPP. To address high scalability in IoT efficient dynamic resource management protocols are needed. Multicast DNS (mDNS) and DNS Service Discovery (DNS-SD) are two prominent protocols that aim at discovering resources and services provided by IoT [115]. The Routing Protocol for Low Power and Lossy Networks (RPL) developed by IETF is an IPv6-based routing protocol. It was designed to support minimum routing requirements by providing a strong topology over lossy links. The IETF working group also developed IPv6 over Low power Wireless Personal Area Network (6LoWPAN). This protocol acts as an adaptation layer and is designed to fit IPv6 packets to IEEE 802.15.4 specifications. The IEEE 802.15.4 is a protocol developed for specifying a sub-layer for Medium Access Control (MAC) and physical layer for Low-Rate Wireless Private Area Networks (LR-WPAN) [116]. Due to its low power consumption, low cost, low rate, and high message throughput, LR-WPAN it is used in IoT, WSN, and M2M. A classification of IoT protocols along with their specifications can be found in [4].

From IoT perspective, wireless sensor nodes and network should address three limiting factors for their wide acceptance. The first one is to support heterogeneous devices. In spite of advances in embedded electronics and software [117], this factor remains burden for smart devices. The second factor is associated with the need of equipping sensor nodes with battery. In spite of several energy harvesting techniques [118][119] including energy aware routing protocols [7][12] and deployment techniques[120],[121] being devised, replacement of batteries from time to time is still a limiting factor for widespread use. The third one relates to the electronics needed to be embedded in IoT objects. Currently, considerable reduction in size brought by recent development in microelectronics is not enough to achieve the full benefit of IoT. So, research in nanotechnology which is in infancy can contribute much in extending scope and applicability of IoT in society [122].

B. MIDDLEWARE TECHNOLOGY

Lots of heterogeneous objects are expected to connect and communicate in IoT. In order to hide the details of different technologies, a software layer is introduced between the technology layer and the application layer. The service oriented architecture (SOA)-based IoT architecture as shown in Fig.3.1 uses a middleware technology. It is successfully used in research areas such as cloud computing, WSNs and vehicular network [100], [123] and is currently being used in IoT. This section discusses functional components and classification of the state-of-the-art of middleware solutions.

An IoT middleware consists of four functional blocks: 1) interface protocols, 2) device abstraction, 3) central control, context detection and management, and 4) application abstraction, as depicted in Fig. 3. 2 [4].

Interface protocols- define protocols for information exchange among different things across different networks. These deal with connectivity issues in physical layer to upper layers in TCP/IP protocol stack.

Device abstraction- defines abstract model of devices to facilitate interaction among heterogeneous devices. This abstraction includes syntactic and semantic interoperation. Interoperation among devices is served through several APIs. APIs defined in middleware performs syntactic or semantic interoperation. Syntactic interoperation looks into format of the information while semantic interoperation looks into meaning of the exchanged information.

Central control, context detection and management- Context awareness is essential for middleware in IoT. In IoT, a context is a situation about a device or thing. This functional block performs context-aware computing to better understand sensor data and then make decision based on data [124]. But most of the IoT middleware solutions proposed recently are not able to perform context-aware

computing. So, context-aware IoT computing is a promising area of research which is being promoted by the European Union during 2015-2020 [125].

Application abstraction- provides an interface to interact with devices. The interface with a device can be implemented by query language.

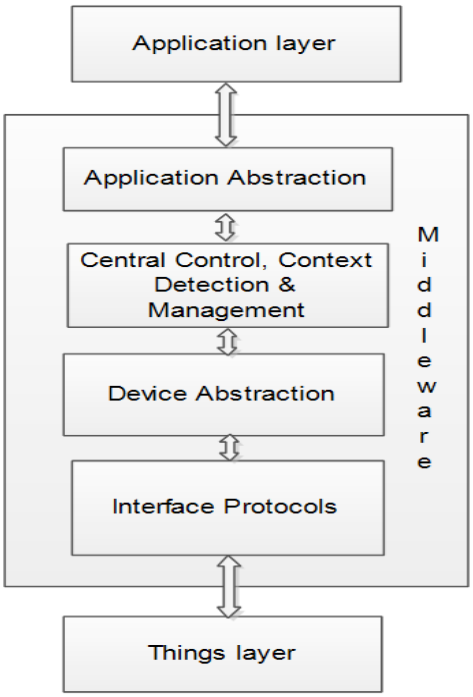


Fig. 3.2. Functional components of IoT middleware

TinyDB [126] is a middleware that provides query language for end users to enquire different parameters from sensors. The middleware for IoT has a number of service requirements categorized as functional, non-functional, and architectural as found in [127]. Functional requirements deal with discovery and management of resource and data, non-functional requirements manage scalability, reliability, availability, security and privacy while architectural requirement is concerned about interoperability, context-awareness, etc. Many types of middleware solutions have been proposed for different functions like context-awareness, adaptability and in various application domains like WSN, RFID.

The existing middleware solutions for IoT can be grouped into a number of classes based on their design approaches as summarized in Table 3.3.

- Event-based middleware such as RUNES[128], Hermes [129] interact through events. They meet non-functional requirements such as reliability, scalability, and security.

- Service-oriented middleware develops applications based on services. HYDRA [130], TinySOA [131], and SENSEI [132] are examples of service-oriented middleware.
- Service-oriented computing (SOC) is inspired by technology neutrality, service reusability, service discoverability, and service composability. However, it suffers from global syntax and semantics, scalability, and security issues.
- Virtual Machine (VM)-based middleware such as MagnetOS [133], Sensorware [134] provides a programming environment by virtualizing infrastructures.
- In agent-based design, applications are broken down into modules which are distributed among mobile agents. Modules may be migrated to another agent in order to support fault tolerance. Agilla [135], UbiROAD [136] are among agent-based middleware solutions. Context aware functionality is supported by HYDRA [130], UBIWARE.
- Tuple-space middleware like LIME [137], TS-Mid [138] allow applications to communicate by sharing data. A tuple-space is a data repository maintained by each member of infrastructure.
- Database-oriented middleware considers WSN as a virtual relational database system. Here, SQL-like statements are used by applications to know sensor data. Sensation, KSpot+ [139], IrisNet [140] are among database-oriented middleware solutions for IoT.
- Application-driven middleware such as MiLAN [141], AutoSec [142] are strongly coupled with a specific applications. So, such middleware fails to support all IoT middleware requirements mentioned above.

A comparison of IoT middleware solutions based on various features like interoperability, device management, portability, context awareness, security and privacy is provided in Table 3.4.

Middleware architectures [97], are mostly inspired by SOA-based IoT architecture as discussed above. The current state-of-the-art of middleware for IoT reveals that research effort is required towards developing a generic middleware for IoT. Middleware solutions like ASPIRE, WHEREX, GSN, and UBIWARE lack in security and privacy. ASPIRE, UBIWARE, GSN do not support interoperability. Context awareness is not supported by SOCRADES, WHEREX, SIRENA, GSN, and ASPIRE. Only few middleware solutions like HYDRA and UBIROAD support all features. In the current scenario, most prominent research problems which attract further research in this area include dynamic resource discovery, scalability, security and privacy, interoperability, embedded intelligence, and context-awareness.

Table 3.3. Classification of middleware design approaches

Middleware Type	Examples
Event-based	Hermes[129],RUNES[143],EMMA[144],GREEN[145]
Service-oriented	Hydra[130],TinySOA[131],SENSEI[132]
VM approach	MagnetOS[133],Sensorware[134],TinyVM[146]
Agent-based	Smart mssages[147],Agilla[135],UbiROAD[136]
Tuple-space approach	LIME[137],TS-Mid[138],A3-TAG[148]
Database approach	COUGAR[149],Sensation[150],TinyDB[126],KSpot+[139]
Application-specific	MiLAN[141],MidFusion[151],AutoSec[142]

Table 3.4. Comparison of middleware solutions [98]

IoT middleware	Features of Middleware				
	Interoperability	Device management	Portability	Context awareness	Security and privacy
HYDRA	√	√	√	√	√
ASPIRE	x	√	√	x	x
UBIWARE	x	√	√	√	x
UBIROAD	√	√	√	√	√
GSN	x	√	√	x	√
SIRENA	√	√	√	x	√
SOCRADES	√	√	√	x	√
WHEREX	√	√	√	x	x

3.1.3 APPLICATIONS AND SOCIAL IMPACT OF IOT

IoT has been successfully applied in many applications like healthcare, smart city, precision agriculture, etc. One of the fastest growing areas where IoT can be used is healthcare [152]–[154]. IoT can be used to monitoring patients, collecting patients' data, and controlling medical devices. Not only the patients but also the healthcare staff can be monitored and managed by IoT in healthcare. An elderly man woman living alone can be monitored and helped by an IoT-based application, ambient assisted living (AAL) [155], [156]. An IoT-based healthcare application must secure personal information pertaining to patients. So, enforcement of policies and regulations in promoting IoT-

based healthcare services is needed for its wide acceptance. In [154], authors address e-Health policies and regulations across the world in accessing healthcare services and pointed out open issues and challenges in IoT-based healthcare services.

Smart city is an application of IoT where resources of a city are best managed [157]–[160]. For example, car parking space of a city can be monitored and travellers can avail of the free space. Leakage of water in city wide water supply path can also be detected so as to avoid wastage of water. Using smart electric meters usage pattern of electricity in a city may be assessed and accordingly load can be distributed in an electric grid.

Precision agriculture is an application of IoT where crop field can be better monitored for irrigation, harvesting, and taking timely decisions [92], [161], [162]. Different sensors may be deployed in field to collect many parameters like moisture, nutrients, temperature, and many more. The farmers can easily access those data not even reaching physically to the agricultural field. Based on the data they can start irrigation, harvesting, or spraying fertilizers, etc. Such an application not only saves manual labour but also minimizes wastage of natural resources like water.

3.1.4 IOT INITIATIVES

A number of IoT initiatives are taken by many countries like US, Europe, China, Japan, Korea, and others. Here, this section mentions the most relevant ones. All initiatives are classified in two main categories- related projects and standardization activities, which are shown in Fig. 3.3. In order to support wide range of applications across industries, individuals, societies and environment, standards is needed for IoT. As of now, various bodies put their efforts towards standardization. This section gives a summary of related projects and standardization activities with regard to IoT paradigm.

A. RELATED PROJECTS

Over the years, a number of IoT projects are active in Europe, Japan, US, China and other countries. Especially in Europe, numerous projects have been funded to conduct research on certain aspects of Internet of Things. Among the key players in IoT initiatives is European Commission which allotted funds for several projects like HYDRA [130], RUNES [143], IoT-A and iCORE [163], IoT6 [164]. Open Interconnect Consortium (OIC) founded by Intel, Samsung, and others, released IoTivity [165], an open source software framework that enables seamless device-to-device connectivity to address the emerging needs of Internet of Things. A state-of-the-art of such projects is given in Table 3.5.

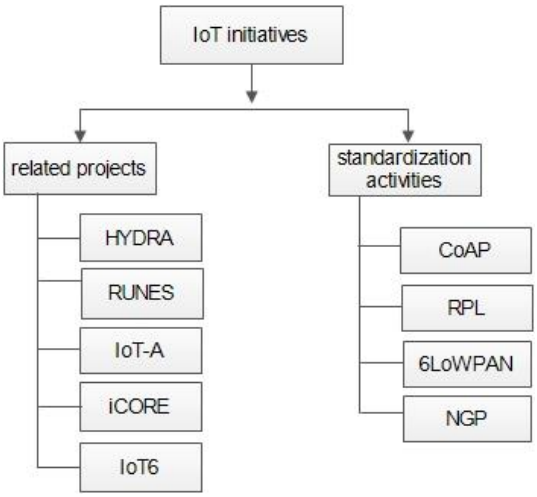


Fig. 3.3. IoT initiatives: related projects and standardization activities

Table 3.5. IoT-related projects

Project	Source
HYDRA[130]	www.hydramiddleware.edu
RUNES[128]	www.ist-runes.org
IoT-A	www.iot-a.edu
e-Japan strategy[170]	http://japan.kantei.go.jp/it/network/0122full_e.html
iCORE[163]	www.iot-icore.edu
SENSEI[132]	http://www.ict-sensei.org/index.php
IoT6[164]	http://www.iot6.eu
IoTivity[165]	https://www.iotivity.org
Alljoyn[171]	https://allseenalliance.org

B. STANDARDIZATION ACTIVITIES

Many Standards Developing Organizations (SDOs) have been formed to develop standards in IoT to facilitate providers and application developers for simplifying and smoothing IoT solutions. Internet Engineering Task Force (IETF) has developed communication standards for IoT physical layer, specifically for MAC layer. Constrained Application Protocol (CoAP), Routing Protocol for Low Power and Lossy Networks (RPL) [166], IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) [105]. RFID standards [91] are developed by EPCglobal. In [96], authors provide a survey on protocol stack developed by IETF for IoT. The M2M group of ETSI is responsible for developing standards for M2M systems and sensor networks. But there is little standardization done

towards IoT. More standardization effort is required in QoS, cost model, management, application, and hardware interfaces [167].

From the current scenario, it is obvious that integrated effort is required towards development of a comprehensive framework. More research is needed in developing standards in data formats, data models, and service-level interfaces and protocols for application-layer interfaces. Academic and industrial research should work together towards achieving a reliable, efficient and practical communication system.

3.1.5 CHALLENGES AND RESEARCH DIRECTIONS

IoT is facing challenges to ensure scalability, interoperability, openness, security and privacy. This section points out some of the major research challenges. In each of the issues, the problem that IoT system may face is also identified.

A. MASSIVE SCALING

Due to the availability of low cost smart devices in the market, trillions of things will join the internet for making a massive IoT. Identification, addressing, authentication, securing, and accessing services of such huge network of things are major challenges in IoT paradigm. Trillions of things will generate enormous data in a moment. The pertinent question is how to handle such Bigdata? Is IPv6 sufficient to address those things? Will 6LoWPAN act as a protocol for future Internet? Can the need for battery be eliminated with sufficiently low power circuits? Which single or unified architecture will provide interoperability of heterogeneous devices supporting diverse applications? These are some of the questions that readily pop up in the minds of the researchers.

B. SECURITY AND PRIVACY

Security in terms of confidentiality, integrity, authentication, non-repudiation and access control of data is one of the key challenges in IoT [168]. Due to the inherent openness of IoT, devices are vulnerable to Internet attacks such as application attack, DDoS attack, wormhole, etc. In spite of these attacks, an IoT application must be able to perform its operation to the user's satisfaction. So, techniques for detecting and mitigating attacks are to be developed to cope with the situation. For example, eavesdropping in RFID system can be avoided by encryption. However, implementation of security techniques in IoT is challenging because of minimal capacity of things, physical inaccessibility to sensors, actuators, or objects, lack of powerful wireless communication. As the

devices lack computational resources, development of light weight efficient security techniques are of great interest [169]. Cryptography plays a major role in securing network infrastructure. Although standards such as AES might work well for some IoT devices; it has limited use in other devices such as RFID tags due to resource constraints. They must be designed efficiently without compromising security.

Much of the data collected and communicated in IoT pertains to personal information. Privacy is one of the most sensitive issues in IoT. Data is vulnerable to attacks due to IoT's anywhere, anything, anytime nature. Without proper privacy measure, users would have access to information not meant for all. Users must be provided with tools to manage their own data like sharing a part or all of their personal data available in social networking sites. To ensure that unauthorized use of data doesn't happen, identity management is also required.

So, social acceptability of most of the IoT applications employing Internet-integrated sensing devices depends on other security requirements such as privacy, anonymity, and trust. An exhaustive analysis on security protocols and state-of-the-art mechanisms to protect communications in IoT could be found in [168]-[172].

C. INTEROPERABILITY

Interoperability among heterogeneous devices is another challenge for IoT. This issue must be addressed not only by application developers but also by device manufacturers. Every IoT service must be designed so as to address interoperability issue in order to meet customer's requirements. Interoperation among devices is possible through defining several APIs. APIs defined in middleware performs syntactic or semantic interoperation. Syntactic interoperation takes care of format of the information while semantic interoperation looks into meaning of the exchanged information.

D. BIGDATA AND ITS MANAGEMENT

Bigdata is the large volume of complex and growing data collected from multiple, autonomous sources [173]. Enormous data is created, communicated and stored in IoT systems every moment thereby producing Bigdata. Real power of IoT lies in collecting and analyzing such data. Interpretation of such noisy, uncertain data and development of new inference techniques are the key challenges. For example, raw data sensed by sensors deployed in a human body must be converted to semantically meaningful information so that it is able to tell about a patient's depression, or respiratory disorder, or eating habits, and so on. Data mining techniques are expected to be capable of creating knowledge from Bigdata in IoT. One of the limitations of current data mining techniques lies in inherent centralized nature of data mining algorithms, which makes it unsuitable for IoT. A comprehensive survey on IoT data mining techniques including classification, clustering, pattern

mining and knowledge discovery in database (KDD) is done in [174]. Outlier detection performed by concurrent processing of multiple data streams is studied in [175]. Although Bigdata analytics platforms are provided by Apache Hadoop [176] and SciDB [177], they are not fit for Bigdata in IoT. An open source platform for large scale data processing is provided by Apache Spark [178] and Apache Strom [179].

Generally, Bigdata"3Vs" model [180] stands for volume, velocity, and variety. Volume means increasing generation and collection of data, velocity means rapid and timely collection and analysis of data, and variety means various types (structured, semi-structured or unstructured) of data. Different data processing approaches are initiated considering either individual or combination of these dimensions. Batch Processing and Stream Processing are two important methods for data analysis. In [181], a framework called Lambda Architecture is proposed that handles Bigdata processing for multiple applications. This framework consists of three layers, namely batch layer, serving layer, and speed layer. The first layer stores the master data set and batch views. Dynamic query creation and execution of batch views are performed by the serving layer through indexing and storing. The speed layer captures and processes recent data for delay-sensitive queries. Lambda Architecture supports easy extensibility, scale-out capabilities, low-latency query processing, and fault tolerance.

Bigdata applications face a number of challenges in data representation, redundancy reduction, and data confidentiality [182]. IoT generates data sets which are heterogeneous in types, structures, semantics, granularity, organizations and accessibility. Efficient data representation techniques are needed for better interpretation and analysis on such databases. Efficient format conversion methods should be developed to enrich quality of data. Redundancy in datasets is to be reduced to reduce the cost of maintenance and analysis of data. In WSN, aggregation is done at sensor nodes to reduce redundancy and energy consumption. Bigdata may contain sensitive data like personal security number, credit card number, transactional data, or other personal data. Data encryption is also challenging in Bigdata due to the 3Vs. At present, Bigdata service providers have adopted minimal security measures. They even share data with third party without enforcing proper security measures. That creates potential risk to sensitive data. Care must be taken to protect Bigdata generated in IoT.

E. STANDARDIZATION

Heterogonous devices constitute IoT and hence, without standards, services may not be accessible to stakeholders. The promising standards are developed by European Commission, IETF, ETSI, IEEE, and EPCglobal. The details of developed standards are included in Section 4.4.2.

3.2 PROPOSED FRAMEWORK

This section provides an application framework for precision agriculture. It employs WSN to collect field data through IoT. The proposed approach is called AgriTech with different components is shown in Fig. 3.4.

3.2.1 THINGS OR OBJECTS

In AgriTech, sensors, actuators, mobile phones, etc. constitute things layer. They are used to gather many parameters like nutrients, humidity, etc. from crop field. Different objects have to communicate with the local sink either in multi hop or single hop fashion. The layer must face challenges associated with sensing and communicating radio signal. Probability of message collision is also there, as there will be a number of nodes involved in communication in the system. The sensors must be location-aware in application. Without location information the collected data has no use. Sensor localization technique needs to be designed in this layer. Energy is one of the valuable and vital resources in WSN. So, data collection must be done in an energy efficient way in such application. This is required to enhance the lifetime of the WSN.

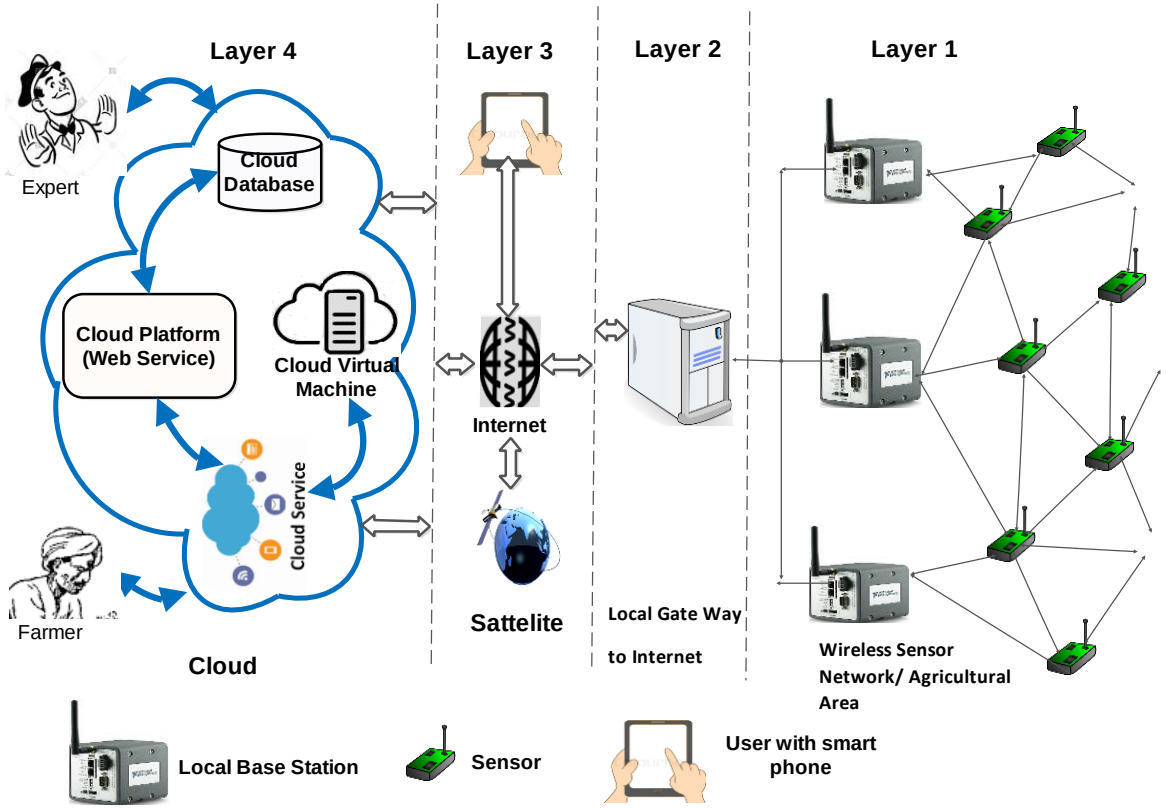


Fig. 3.4. Framework of AgriTech

3.2.2 LOCAL GATEWAY

The underlying WSN in precision agriculture sends data to local gateway. The local gateway applies aggregation on the collected data in order to avoid redundancy. Closely placed sensors send same parameter value. As processing of same parameter value consumes resources redundancy must be reduced. After aggregation local gateway forwards data to the cloud. The data on cloud can be accessed as per requirements by different shareholders.

3.2.3 INTERNET

Internet plays important role in AgriTech. Things layer uploads data to cloud through Internet. It enables data to be communicated with all stakeholders. Farmers can have access to their field data. Analysing data helps to identify affected crop area. For example, farmers come to know the area which becomes dried up. Irrigation can be initiated in the selective crop area. Selective irrigation minimizes natural resources like water. Based on data farmers can take decision for harvesting crops. AgriTech can access takes help of weather forecasting so as to decide irrigation or harvesting. If there is chance of raining, AgriTech may delay irrigation to save water.

3.2.4 DATA CLOUD AND MOBILE PHONE APPLICATION

AgriTech uses cloud services in storing and accessing agricultural data. All collected data are uploaded into data cloud. Cloud provides an architecture where data or services can be accessed pay per use. Cloud works in layer 4 of AgriTech. The application for precision agriculture may also be provided by cloud. Farmers can use the application as Software as a Service (SaaS) [184] from cloud. With the application installed in smart phones, farmers can monitor crops remotely. Initial set up cost is required for layer 1 and 2 which is a burden for farmers. However, farmers can use services of cloud for layer 3 and 4. Day by day the number of mobile phone users is increasing and most of the subscribers use smart phones with numerous applications. By using this application few agricultural devices can be controlled remotely. Based on humidity and temperature water sprinklers can be instructed to spray water. There are agricultural experts in the cloud from whom farmers are benefited. Farmers can take suggestion from them regarding pest control, harvesting, and accessing global market. For example, irrigation can be delayed as there is chance of raining.

3.2.5 MESSAGE COMMUNICATION IN FRAMEWORK

In AgriTech, the following message communications happen:

- Human to object (things) communication,
- Object (things) to object (things) communication,
- Object to Internet communication, and
- Human to internet communication.

Crop field related data is sensed by deployed sensors. Sensed data are accessed by farmers via Internet in the first type of communication. There are few automated or semi-automated devices used in agriculture now-a-days. In the second type of communication, one device can share data to another device. For example, humidity sensors can send data to water sprinklers. Semi-automated sprinklers can now start irrigation based on humidity values. In the third type of communication, a device can directly upload data to cloud. In the fourth mode of communication, farmers can access data from cloud through internet. Cloud provides services to different stakeholder in the application on demand.

3.2.6 DESIGN OF FRAMEWORK

This section presents the detailed technical design of AgriTech. This section describes the design with the help of use case diagram and sequence diagram.

A. USE CASE DIAGRAM

This section designs AgriTech. There are many actors in the system like sensors, farmer, cloud, etc. having different roles. The roles of different actors are depicted in use case diagrams. Fig. 3.5 shows use case of layer 1 and layer 2 while Fig. 3.6 depicts use case of layer 3 and layer 4 of AgriTech. Fig. 3.5 reveals that sensor nodes have routing and sensing roles, base station has routing and aggregation, and local gateway has routing, data aggregation, and uploading data in cloud. Fig. 3.6 shows the roles of farmers, cloud, expert, and satellite.

Farmers can have suggestions from agricultural experts. The suggestion will be aimed towards controlling actuators/sensors in the field. Lastly a farmer can get this suggestion from cloud and take appropriate measures.

B. SEQUENCE DIAGRAM

The agricultural field where AgriTech will work is first deployed with sensor nodes attached with several different purpose sensors. For example, it may be supposed that a set of sensor nodes are deployed in field for the purpose of knowing soil moisture. This will be required for the purpose of

automating the water spraying mechanism. It assumes that ArgiTech devices are equipped with sensors and be either fully automated like an automated robot controlled tractor or can also be regulated manually like water sprinklers. The sensors sense the moisture contents at different locations in the field and send the field humidity values to the local gateway in the form of messages.

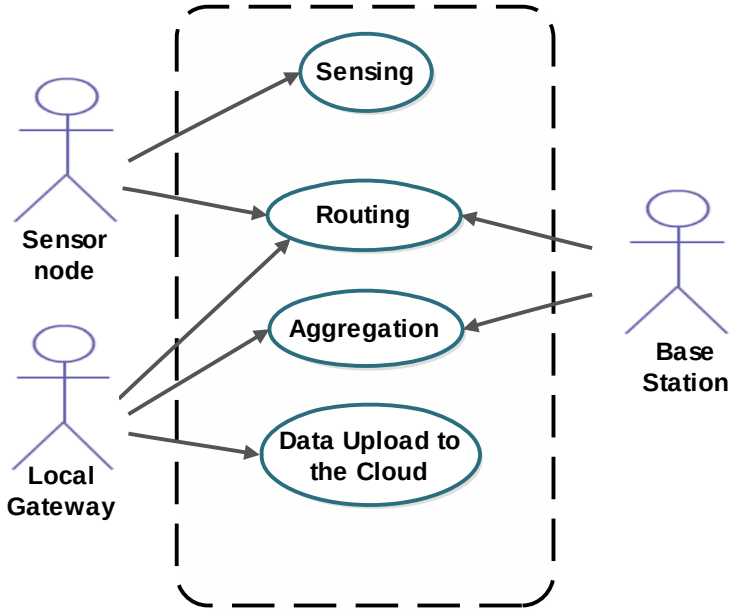


Fig. 3.5. Use case diagram for layer 1 and layer 2 of AgriTech

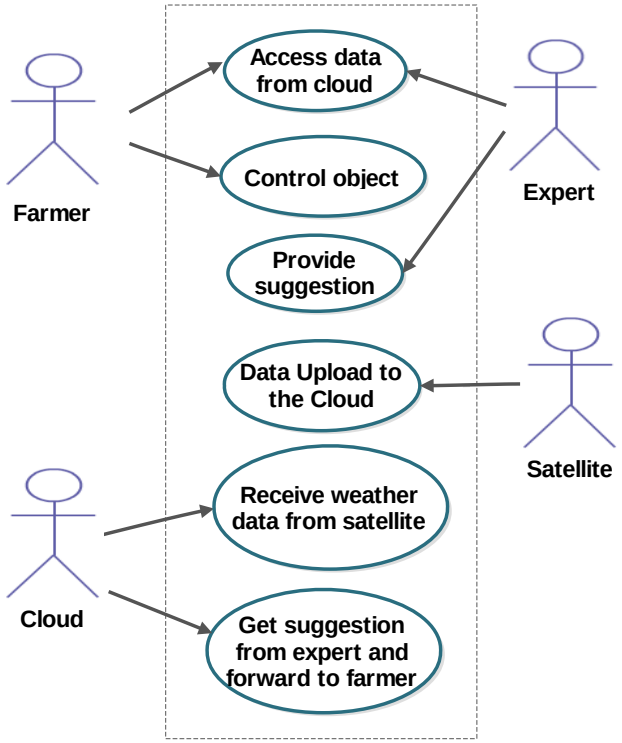


Fig. 3.6. Use case diagram for layer 3 and layer 4 of AgriTech

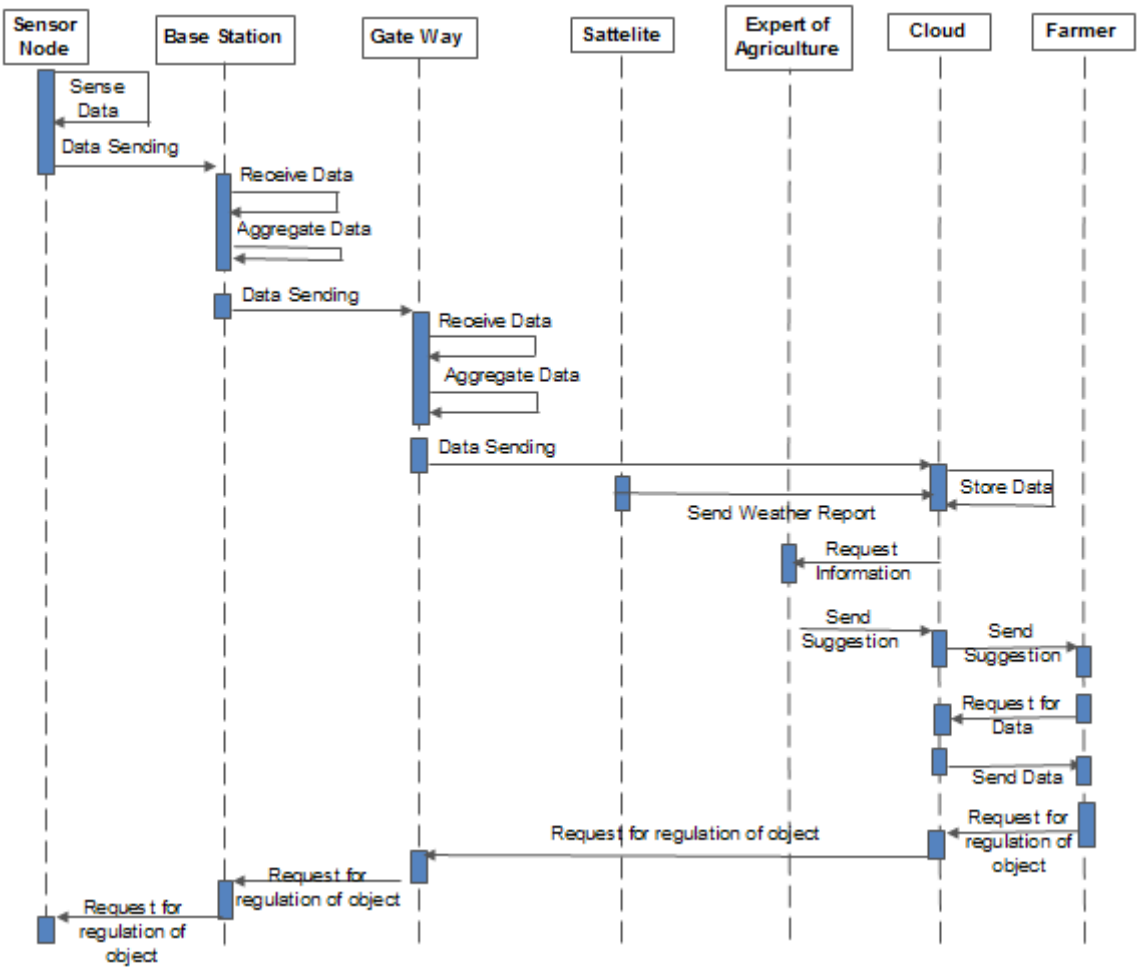


Fig. 3.7. Sequence diagram of AgriTech

The local gateway aggregates those data and uploads the same to cloud. Farmers can retrieve the uploaded data through Internet and get status of soil moisture content. As explained later, farmers are also able to take assisted-decision. Through AgriTech, farmers can now directly instruct the automated water sprayer to spray water in selected locations of the field. This instruction reaches the automated devices through local gateway. The sequence of actions taken by different actors is illustrated using a sequence diagram in Fig. 3.7. Sensor nodes deployed in field sense data such as soil moisture, temperature and send the same to nearest sink. On receiving data from different sensors, sink aggregates data before forwarding to local gateway. Gateway performs further aggregation on received data and sends it to IoT cloud. Here, cloud stores field data as well as weather data from satellite. Now, cloud takes help of expert in agriculture for suggestion in order to take decision. After getting the suggestion from the expert the cloud application also performs its own data analysis. After compilation of both analyses, cloud application sends the suggestion to the farmer. Thus the farmer gets assisted decision. AgriTech will be semi-automated system consisting of automated as well as manual devices. Therefore depending on the data collected by the sensor the cloud will instruct the

internet object to act accordingly. On the other hand the farmer can control that internet object of AgriTech through his mobile phone application.

3.2.7 PRACTICAL IMPLICATIONS AND LIMITATIONS OF FRAMEWORK

AgriTech is supposed to be used by farmers. This technology will increase crop yields and quality of crops. It is beneficial to countries dependant on agriculture. Farmers can save manual labour. So, they can be engaged in other profession in parallel with agriculture. This technology can save natural resources like water and minimizes the use of pesticides in field. Knowing the location of affected crop area is possible here as the sensors are location-aware. So, water, pesticides or other materials will be applied in specific area, not in entire crop field. This is how it minimizes use of water and pesticides. By observing humidity level of soil water sprinklers may be instructed to start spraying water. Economic growth is possible by adopting AgriTech.

But there are a number of limitations for implementing AgriTech. In third world countries, farmers may not afford the initial setup cost. Also, they have to pay the cloud service provider for using the AgriTech. To use the service they must have smart phone. These are all burden to the farmers. Sensors deployed in field are vulnerable to physical attack. For example, the farmers may get insufficient or wrong information if sensor nodes are compromised by adversaries. Anchor nodes in localization may also be forged so as to disrupt location estimation of unknown nodes. If improper deployment is done, sensors may sense the field not belonging to that corresponding farmer. Deployment must ensure the coverage and connectivity issues in WSN.

3.2.8 DATA ANALYSIS FOR SUITABILITY OF AGRITECH

Different set of data is collected and studied from the web site of World Bank (Year 2011-2014). Based on the collected data Fig. 3.8 and Fig. 3.9 are drawn. Fig. 3.8 describes comparison of percentage of employment in agricultural sector of different countries. According to Fig. 3.8, USA remains the least and Tanzania possesses the maximum position in employment. India holds the second highest position. Therefore from this graph it can be said that for some of the third world countries lots of population depends on agricultural profession. Fig. 3.9 compares the percentage of GDP earned in agriculture for different countries. From this graph it can be said that the developed countries like UK, Japan and USA etc has least dependency on agricultural sector over GDP (Gross Domestic Product) of those countries. From Fig. 3.8 and Fig. 3.9 it can be stated that countries which

depend on agriculture mostly have lower per capita income compared to the countries which do not depend on agricultural sector.

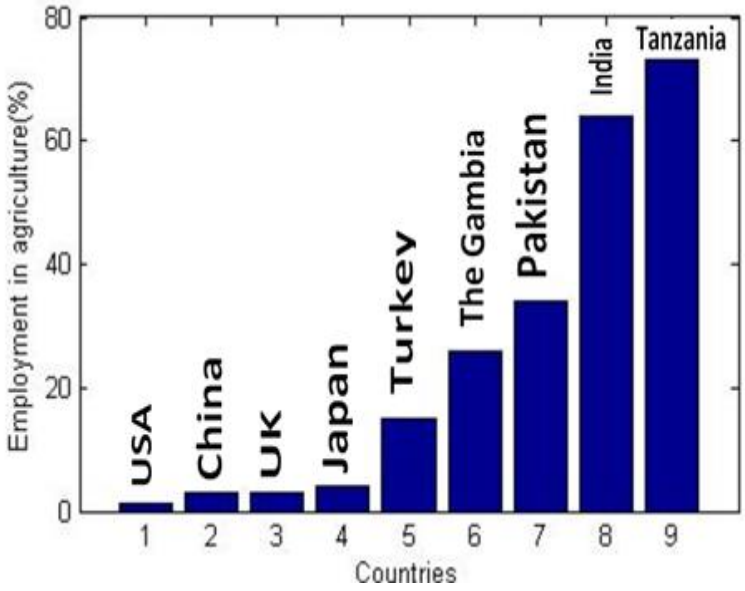


Fig. 3.8. Comparison of percentage of employment in agricultural sector of different countries [185]

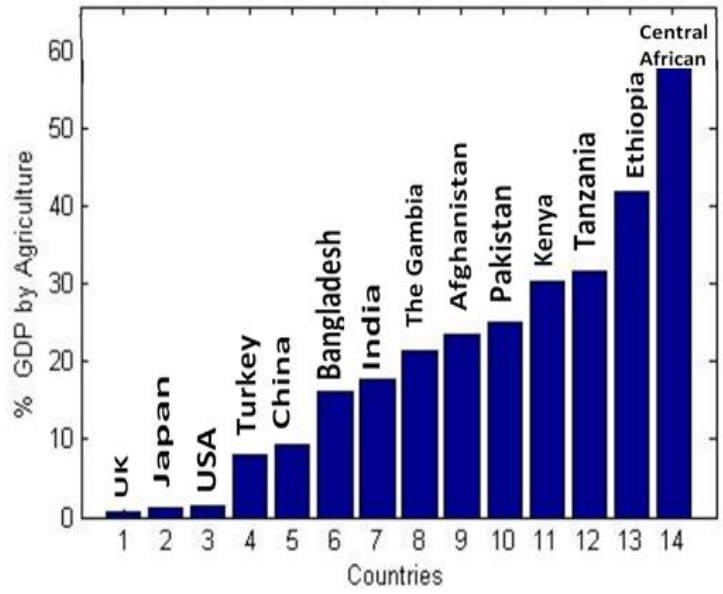


Fig. 3.9. Comparison of percentage of GDP earned by agriculture of different countries [185]

Again it can be said that the countries which are least dependent on agriculture have higher total GDP. One interesting fact is though India has higher total GDP but it has significantly lower per capita

income. The reason is that India is the second most populated country in the world. Therefore accumulated little amount of per capita income of huge number of population becomes significant amount of GDP. Still the total GDP of India is not as much as China with significant population. The reason behind this is that they are mostly dependent on production based industry and not on agriculture. But in India agriculture is the main backbone of economy and we cannot avoid these.

We need to increase per capita income of farmer keeping the agricultural output same. The only way is if we can apply AgriTech over agriculture. The AgriTech will reduce time and effort of a farmer on agricultural work. Therefore farmer can get involved in other profession like food industry or any other production based industry from which the country as well as those farmers can profit.

3.3 CHAPTER SUMMARY

This chapter initially presents a comprehensive survey on IoT. Then this chapter proposes a framework for precision agriculture based on the survey. The state-of-the-art of IoT architecture, enabling technologies, are mentioned in the survey. State-of-the-art of IoT initiatives and standards made by different countries has been summarized. Middleware solutions are also discussed in this chapter. Major challenges which need to be addressed in coming years are pointed out. Although, current enabling technologies make IoT feasible, they are not in a position to address scalability and performance requirements for future IoT. Uniform common architecture and related standards need to be developed to address scalability and heterogeneity. Due to inherent openness, security and privacy remain major challenge in IoT. Design of lightweight security methods can secure IoT. Research towards addressing the challenges can help achieving better future IoT. Massive scaling, inherent openness, security and privacy demand researchers to contribute in IoT. Coordinated effort is needed by industries, researchers, providers, and application developers to make IoT useful to all.

Finally, this chapter prescribes a framework for precision agriculture. Using an application implementing the proposed framework will help farmers to monitor crop area remotely. Agricultural data are collected at sink and may be uploaded into cloud. Farmers can access data from cloud and take necessary actions.

However, implementing AgriTech is challenging due to the limitations of underlying WSN. The underlying WSN must be energy efficient and location-aware for successful implementation of the framework. Energy efficiency in data collection is achieved by clustering and routing while security is

provided by a secure localization method. Hence, combining location-aware sensor nodes with energy-efficient clustering in WSN will be an effective IoT-based application in precision agriculture.

As sensors are limited to computational resources, we need to design an energy-efficient data gathering method for WSN. In the next chapter, an energy-efficient clustering and routing protocols are proposed for large scale application of WSN.

CHAPTER FOUR

ENERGY EFFICIENT WSN CLUSTERING AND ROUTING

A framework for precision based on IoT and WSN is proposed in the previous chapter. For the successful implementation of the proposed framework the underlying WSN must be energy-aware. This chapter addresses energy-awareness of underlying WSN in two ways: by proposing a fuzzy logic based clustering algorithm and an adaptive routing protocol with energy harvesting sensors. The rest of the chapter is organised as follows. Section 4.1 presents an optimum fuzzy clustering algorithm for energy efficient data collection. Section 4.2 proposes an adaptive routing protocol for WSN which restore energy sensors with energy harvesting. Finally, the conclusion is drawn in Section 4.3.

4.1 OPTIMUM FUZZY CLUSTERING APPROACH IN WSN

Wireless sensor networks are being used in wide range of applications including precision agriculture, health monitoring, human activity recognition, disaster monitoring, precision livestock farming etc. [1]. In spite of being battery operated with limited energy, sensors are also deployed in hostile environment (rough terrain) for military applications. Generally, the sensors remain unattended till death. Since replacing or recharging battery is not feasible, energy of a sensor node remains a constraint. The challenge of energy conservation [186] is faced by developers of large scale applications using WSN.

Wireless sensor networks can be integrated into IoT to meet the challenges of seamless communication between things [186]. A WSN is a network of small size low power sensors capable of detecting physical phenomenon. The potentiality of WSN may be flourished in precision agriculture. Extensive use of different sensors like temperature, humidity, salinity, pH, etc. in agricultural fields and networking among them help in taking timely decision which might improve agricultural yields. Effectiveness of such application can be improved by ensuring desired quality-of-service (QoS) of WSNs like energy efficiency, reliable and secure localization of sensors.

Clustering is one of the techniques towards extending network lifetime by conserving limited energy of sensor nodes [187]. Based on applications, lifetime of WSN is measured in terms of time to first node death (FND), half node death (HND), last node death (LND), ten percent node death (TND), etc.

One approach of sending data is when every node sends data directly to sink or via another node which is shown in Fig. 4.1(a). But the overhead increases if all nodes in a cluster communicate directly with the BS. Eventually, the nodes would end up using their limited energy quickly.

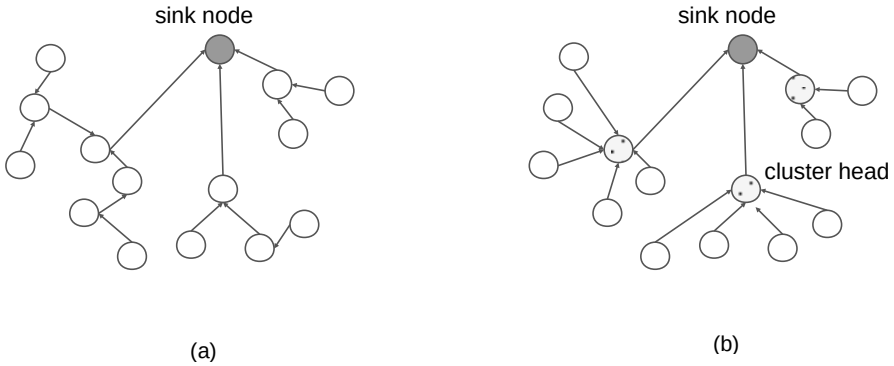


Fig. 4.1. WSN clustering: (a) flat topology and (b) hierarchical clustering

Instead, nodes in WSN may be divided into clusters each cluster having one Cluster Head (CH) [19], [18]. The CHs are in charge of collecting data from member sensor nodes in respective clusters and forwarding data packets to sink; after aggregation which is shown in Fig. 4.1(b). It is apparent that CHs will dissipate more energy soon. Hence, the CHs are periodically rotated to balance energy dissipation. A round is considered where round denotes the time between two consecutive election phases of CH [45], [188]. The CHs for rotation may follow single-hop or multi-hop routing while sending packets to BS. The CHs are computation intensive nodes dissipating more energy in collecting and aggregating other information. The novelty of clustering algorithm lies in choosing CHs efficiently so as to balance routing load among WSN nodes.

In equal clustering like HEED [32], each cluster has equal communication radius. But the nodes closer to BS use up their energy quickly for additional inter-cluster communication. This relay traffic affects network lifetime as well as it partitions the network near BS. This is known as hot spot problem, which is solved in unequal clustering [34], [35], [189], that guarantees balanced energy dissipation. Details of these techniques are discussed in Chapter 3.

The nodes in WSN are subject to environmental factors like interference, high temperature, fog, vibration, etc. They may have overlapping communication ranges too. Hence, nodes on the boundaries of clusters may belong to more than one cluster at the same time. This scenario poses uncertainties in clustering the nodes and electing CHs for each cluster. In this situation, fuzzy logic [190] may be used to handle uncertainties in clustering. The overhead of CH election in uncertain environment may be reduced by fuzzy logic. Many clustering protocols including LEACH-ERE [21], LEACH-FL [39], LEACH-SF [6], [22], [48] and [40] use fuzzy logic. Type-1 fuzzy logic is used in [21], [39] and [6] whereas T2FL is utilized in [22], [44]. A T2FL model is expected to handle uncertainty better than T1FL model. However, a few protocols utilize T2FL due to its computational complexities. Fuzzy-based algorithms [191] elect CHs among WSN nodes using Fuzzy Inference System (FIS) by applying fuzzy rules.

In this chapter, an unequal clustering protocol named Optimized Fuzzy Clustering Algorithm (OFCA) is proposed. This algorithm elects CHs along with estimation of communication radii using a T1FL model and finds routing path to relay traffic to sink in multi-hop using particle swarm optimization (PSO). The proposed algorithm can be used by an application of WSN as multi-hop data forwarding is followed. The algorithm achieves energy efficiency through unequal balanced clustering, efficient CH election, and forwarding aggregated data from CH to BS in an energy-efficient way. At first, CHs are elected based on residual energy, distance from sink, and concentration of nodes using T1FL. Then communication radii of CHs are fixed depending on distance to BS and unequal clusters are formed after associating nearby sensor nodes with CHs. Local data aggregation is performed at CHs to reduce overhead of data forwarding. Secondly, energy efficient multi-hop data forwarding path is calculated by PSO after deriving a fitness function in the form of solution to linear programming (LP) problem. Unlike [6], the proposed algorithm creates unequal clusters in order to cope with energy hole problem near BS. Clusters closer to BS have smaller size than that of the clusters away from BS. Unlike [22], T1FL is used to avoid computational complexity of T2FL system. The agricultural application of WSN in which sensor nodes are used for sensing soil moisture, air temperature, and soil nutrients is considered here. Fuzzy inference system is used to find confidence factor (CF) i.e., fuzzy chance of a sensor node to be elected as CH based on its residual energy, distance from BS, and concentration of nodes around it. A node with higher residual energy, nearer to BS, and more number of neighbor nodes has higher chance to be elected as CH in a cluster. The communication radii are calculated by the inference system based on distance to

BS. The closer the distance the smaller is the communication radii. The lifetime of WSN using OFCA is measured in terms of FND, TND, and HND.

The major contributions of this chapter are:

(a) Managing uncertainties in CH election through fuzzy logic.

(b) Unequal clustering by calculation of communication radii using fuzzy logic.

(c) Establishment of energy efficient routing path for multi-hop data forwarding through PSO using a novel fitness function.

The proposed algorithm not only extends lifetime of WSN, but it also works well in heterogeneous WSN with limited heterogeneity.

The rest of the chapter is organized as follows: Section 4.1.1 presents preliminaries of network model and energy model that form the basis of the proposed protocol while Section 4.1.2 provides an introduction to fuzzy logic. The overview of the proposed approach is provided in Section 4.1.3. The algorithm for cluster head election and calculation of communication radii using fuzzy logic is proposed in Section 4.1.4. Section 4.1.5 presents optimum routing path selection by PSO. Particle representation and derivation of fitness function are mentioned in Section 4.1.6 and Section 4.1.7 respectively. In Section 4.1.8, simulation results are analysed while the chapter summary is drawn in Section 4.1.9.

4.1.1 THE NETWORK AND ENERGY MODEL

The proposed algorithm OFCA is based on the following assumptions. The WSN is created with 100 nodes which are deployed randomly over a crop field of area $100\times100m^2$, following non-uniform distribution with the intention of monitoring the crop field. In multi-hop data forwarding, CHs closer to BS dissipate more energy than CHs away from BS due to inter-cluster traffic in addition to intra-cluster traffic. This creates energy hole near BS. To get rid of energy hole problem, unequal clusters with different competition radius is generated. Here, the WSN is considered to be divided into a number of levels as shown in Fig. 4.2. The algorithm, OFCA organizes the nodes into clusters and elects one CH for each cluster, based on residual energy of a node, distance of node from BS and concentration at each level. Clustering helps in minimizing energy dissipation by forwarding data from individual nodes to BS via respective CH. Each CH aggregates sensed data from its member nodes and forwards it towards BS via multi-hop path following a TDMA schedule. Inter-cluster messages (i.e., the traffic amongst CHs) are not aggregated. This means that a CH forwards messages sent by other CHs without aggregation. The BS is placed at the center of the field which collects data from CHs and aggregates them. The aggregated data is used to take decision regarding irrigation,

harvesting, using fertilizers in the selected area of crop field as mentioned in [92]. For example, water can be released from automated sprinklers when it is detected that the soil is "dry". All nodes including BS are stationary. The BS has no energy limitation and has enhanced computation capabilities. Each node can perform as a regular sensor node as well as a CH.

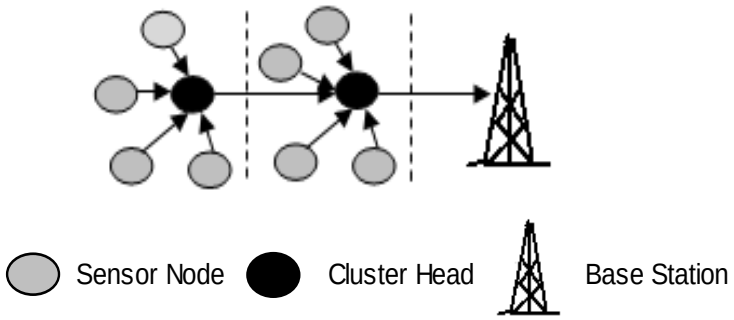


Fig. 4.2. Multi-hop clustering network

The first order energy model [19] for consumed energy (during communication) is as follows. The energy consumed by transmitter for transmitting k bits over a distance of d is given by eqn. (4.1). The transmitter dissipates energy to run the radio electronics (E_{Telec}) and the power amplifier (E_{Tamp}). If the distance is less than d_0, the algorithm adopts free space model (d^2 power loss) else adopts multi path fading channel model (d^4 power loss).

$$E_T(k,d) = E_{Telec}(k) + E_{Tamp}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, & d \le d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4, & d > d_0 \end{cases} \quad (4.1)$$

But the receiver consumes energy to run the radio electronics (E_{Relec}) only and is given in eqn. (4.2).

$$E_R(k) = E_{Relec}(k) = kE_{elec} \quad (4.2)$$

where E_{elec} represents electronics energy consumption for transmitting or receiving 1 bit. Also, ε_{fs}, and ε_{amp} are the coefficients of energy consumption of transmitter amplifier for different channel propagation models, namely, free space and multi-path. While d_0 is the threshold distance between transmitter and receiver calculated by eqn. (4.3).

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{amp}} \quad (4.3)$$

4.1.2 INTRODUCTION TO FUZZY LOGIC

In classical set theory, an element is allowed to be entirely included in the underlying set or not at all. That means an element if included has a membership value of 100% or 0%, if not included in the set. However, it is human to express uncertainty or vagueness in reasoning. That is why the linguistic terms *hot*, *many*, *tall* etc. are used. Fuzzy sets allow an element to have partial membership as shown in Fig. 4.3.There are four sets of temperature: Freezing, Cool, Warm, Hot. The temperature 40^0F may belong to freezing as well as cool. It apparent from Fig. 4.3 that today is warm with temperature 72^0F. Though 72^0F belongs to warm and hot both sets, it has higher membership value in warm set. In the next day we say it is a hotter day with temperature 85^0F, again in another day with 93^0F temperature we say it is too hot day. In fact, all these three days are hot with some degrees of membership values. In particular, we may consider the membership values: 0.6, 0.7, and 0.9 in the fuzzy set *hot* (say) corresponding to 35^0F, 37^oF, and 39^0F temperature respectively. So, fuzzy sets define multiple membership levels for elements within [0, 1].

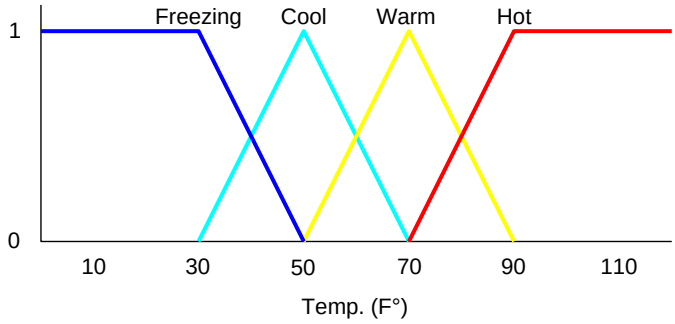


Fig. 4.3. Example of fuzzy membership functions of temperature

With fuzzy logic invented by Zadeh real world approximate reasoning is possible. A fuzzy system consists of fuzzy sets and fuzzy rules. The behaviour of a fuzzy system is prescribed by a set of fuzzy rules. The fuzzy rules appear in the form: *if* antecedents *then* consequents. Antecedents and consequents are propositions associated with linguistic input and output variables respectively. Antecedents are expressed as the logical operations of linguistic variables. For example, if temperature is hot and humidity is high, then cooler is turned ON. It suggests that to turn on cooler in a room whenever there is high temperature and high humidity. In a rule-based inference system, fuzzy sets and fuzzy rules act as knowledge base. A fuzzy inference system showing different components is depicted in Fig. 4.4. It consists of three components: fuzzifier, inference engine, and defuzzifier. The fuzzifier maps non-fuzzy i.e., crisp inputs to equivalent fuzzy inputs using membership functions

like triangular, trapezoidal etc. Fuzzy reasoning is performed by inference engine which makes use of fuzzy knowledge base. The fuzzy output is determined from the consequent of the rule whose antecedent closely matches with fuzzy inputs. Then the fuzzy output is transformed into crisp output by the defuzzifier.

Fuzzy logic [190] was introduced by Zadeh to deal with uncertainty in data. Fuzzy logic is used in situation consisting of entities with imprecise data. Fuzziness in data is represented by fuzzy set along with membership in the set. Unlike classical sets, elements in fuzzy sets may have partial membership values. Membership values are calculated by membership functions like trapezoidal function. Mapping of fuzzy inputs to outputs is executed by fuzzy inference system (FIS) as given in Fig. 4.4. The FIS first converts crisp inputs to fuzzy values by fuzzifier. The outputs are calculated by an inference engine. The decision making is performed inside inference engine. Generally, it uses IF-ELSE rules to map inputs to outputs.

Fuzzy logic has been successfully applied in image processing, control systems, and pattern recognition. It is being used in WSN also.

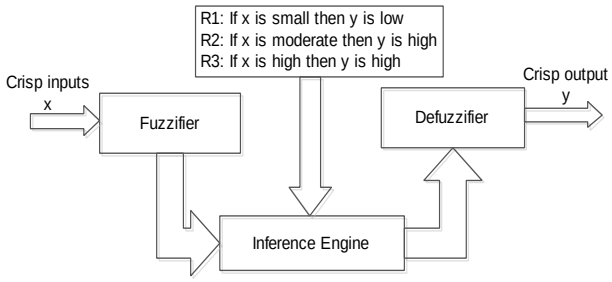


Fig. 4.4. A fuzzy inference system showing three components.

4.1.3 OVERVIEW OF PROPOSED APPROACH

Every round of the proposed clustering algorithm consists of two phases, namely, setup phase and steady state phase as given in Algorithm 1. Setup phase consists of CH election centrally at BS by FIS, estimating competition radius of CHs, and formation of unequal clusters by associating nearby nodes. In steady state phase, a CH collects data from member nodes, aggregates it, and forwards it to BS following optimum routing path as established by PSO. The proposed OFCA is a centralized clustering and routing approach implying that computations for choosing CHs are performed in BS. Balanced energy dissipation among CHs due to intra-cluster communication is assured by unequal clusters. Again, energy dissipation due to inter-cluster communication is minimized by optimum routing path selection by PSO. The process of CH election and communication radii calculation in

OFCA is depicted in Fig. 4.5. Due to the two-fold energy balancing, lifetime of network increases. Based on three fuzzy inputs, namely, residual energy, distance to BS, and concentration, the FIS finds confidence factor (CF) for a node. The CF of a node represents the degree of fitness to be elected as a CH. The fuzzy output CF represents the goodness of a node to become a CH. After calculating CF for all nodes, the node with maximum CF is elected as CH. Once the CHs are elected, the BS advertises CH-message to elected CHs. For unequal clustering the communication radius of CHs are elected by fuzzy logic based on distance to BS.

Each CH in turn informs the same to its nearby nodes by broadcasting CH-message. After receiving JOIN-REQ message from nearby nodes within communication radii, CH sends DATA-REQ message to members. The member nodes send data to respective CHs following a TDMA schedule defined by corresponding CH. In a TDMA, each CH collects and aggregates the traffic of its member nodes into a single message and transmits to BS following a multi-hop routing. In OFCA, 10 such TDMAs are considered to constitute a round. CHs are re-elected after 1 round.

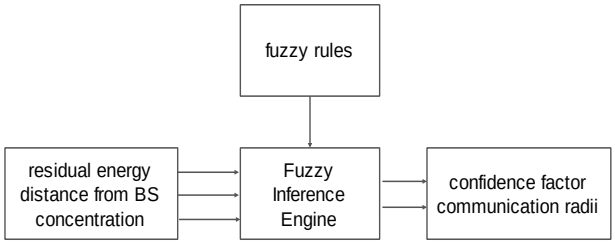


Fig. 4.5. Cluster head election and radii calculation by fuzzy system

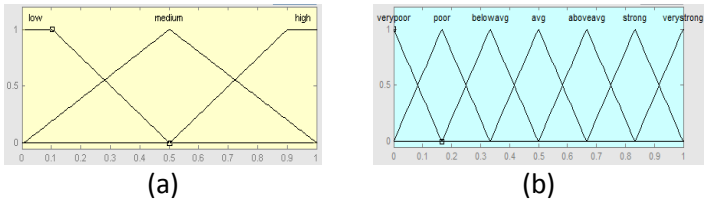


Fig. 4.6. Membership function for (a) inputs (b) output

4.1.4 CLUSTER HEAD ELECTION AND CALCULATION OF COMMUNICATION RADII USING FUZZY LOGIC

Fuzzy logic has established its superiority in decision making under uncertain and chaotic environment. A WSN exhibits uncertainties in many respects. Uncertainties in electing CHs over the network can be better dealt with FIS. FIS evaluates fuzzy inputs and maps to fuzzy outputs using

fuzzy rules. Fuzzy rule base is the set of rules defined in FIS to infer fuzzy chance or probability of a node to become CH. The Mamdani and Sugeno fuzzy inference models [192], [193] are applied by researchers in this area. Each of the models is based on rules like "if antecedence then consequence".

In this work, type-1 Sugeno FIS is used to elect good CHs and calculate communication radii in Fig. 4.5. The proposed FIS works with three fuzzy inputs: residual energy, distance from sink, and concentration of nodes around the particular node and two outputs: CF and communication radii. Residual energy represents the energy available in a sensor node. The second input measures the distance of a node from BS while concentration of a node denotes number of nodes existing within its communication range. The higher the value of CF for a sensor node, the higher is its chance to become a CH. Enhanced lifetime can be achieved by ensuring energy efficiency in electing CHs. A CH is responsible for aggregating data collected from its member sensor nodes and relaying to the sink. So, CHs demand more energy than other normal (non CH) nodes. The higher the residual energy of a node, the greater is the chance to become a CH. The more the BS distance, less is the chance to be elected as CH. The number of nodes around a node is represented by the third fuzzy input, concentration. The chance will be more if concentration is higher. All three fuzzy inputs vary dynamically from node to node over the network. The Sugeno FIS based on these fuzzy inputs and following fuzzy rules determines CF of a node to be elected as a CH. The rule base used to calculate CF in FIS of proposed algorithm utilizes the rule base in [22]. For example, whenever residual energy is less, distance is near, and concentration is low, the CF is defined as very poor. Similarly, whenever residual energy is less, distance is farthest, and concentration is medium, the CF is defined as very average. In the same way, whenever residual energy is high, distance is farthest, and concentration is high, the CF is defined as very strong.

Though initially elected CHs belong to nearby area of BS, later on (say, in rounds after first node death) CHs away from BS will be elected as these nodes now get higher preference over nodes closer to BS due to their higher residual energy. In this way CHs are rotated and distributed over time and over the network with increasing number of rounds, thereby avoiding energy hole near BS.

The communication radii of CHs are calculated based on distance to BS. In order to save energy of CHs closer to BS their communication radii are set smaller than that of the farther ones. This setting is made as the CHs closer to BS are overloaded with inter-cluster traffic in addition to intra-cluster traffic.

The fuzzy sets that represent input and output variables are depicted in Fig. 4.6. Each fuzzy input variable is associated with three linguistic variables low, medium, and high. There are 7 membership functions of CF corresponding to 7 linguistic variables i.e., very poor, poor, below average, average, above average, strong, and very strong. The FIS calculates the value of CF based on residual energy, distance from BS, and concentration.

Algorithm 1: Proposed OFCA Clustering Algorithm

Input:

W: network, r: round number, *a*: node in W, *c*: cluster
CF(a): fuzzy chance to become a CH
L: number of clusters, max_round: maximum round number
b: fuzzy inference system

Output:

CH(j): cluster head of the j-th cluster

Function:

eval_fiscf(residual_energy, distance_from_BS, concentration, fis): calculates fuzzy confidence factor
eval_fiscr(distance_from_BS, fis): calculates communication radius
find_maxCF(cluster): returns node with maximum CF value
broadcast(information, destination): advertises message

Initialization:

1: Define fuzzy rule base
2:$b \leftarrow read\_fiscf(\,)$ and $d \leftarrow read\_fiscr(\,)$//read fuzzy system into *a* and *b*
3: $r \leftarrow 0$ // initialization of round

Main:

4: For each *r* until *max_round*
*/*setup phase*/*
5: For each node $a \in W$
6: $\mathrm{CF}(a) \leftarrow$eval_fiscf(residual_energy(a), distance_from_BS (a),concentration(a), b);
[End for]
7: For $j=1$ to L //form L clusters
8. $\mathrm{CH}(j) \leftarrow$find_maxCF ($c_j$) //elect node with max. CF as CH
9. //calculate competition radius of CH(j)
$R(j) \leftarrow$eval_fiscr(distance_from_BS(j),d);
10: Broadcast(CH-message, CH) //BS informs all elected CHs
[End for]
/ steady state phase*/*
11: For each cluster $c_j \in \{c_1, c_2, \ldots\ldots, c_j, \ldots, c_L\}$
12: Find an optimal routing path applying PSO.
13: Collect data and aggregate.
14: Forward data to BS using optimal path.
[End for]
15: $r \leftarrow r + 1$
[End for]
16: Exit.

Once a CH is elected for a cluster, communication radius of the CH is adjusted based on distance from BS. This consideration guarantees the unequal clustering in WSN. Each CH in turn informs the same to its nearby nodes by broadcasting CH-message. After receiving JOIN-REQ message from nearby nodes within communication radii, CH sends DATA-REQ message to members. In steady state, member nodes send data to respective CHs following a TDMA schedule defined by corresponding CH.

4.1.5 OPTIMUM ROUTING PATH SELECTION BY PSO

Aggregated data at CHs are forwarded to BS following multi-hop communication to support large application area. Energy consumption due to inter-cluster traffic can be reduced by choosing an optimal routing path from a CH to BS using other CHs. Finding energy efficient route is an optimization problem in which choice of CHs as relay node in a multi-hop network depends on factors like residual energy, distance from BS, and concentration of CH. In this section, optimum path using PSO is obtained after formulating a novel fitness function. PSO is used due to its simplicity and quick convergence ability in global search.

The relay CHs in a multi-hop routing path will be elected in such a way that total residual energy and total concentration of all CHs along the path must be maximized while average distance to BS is to be minimized. Election of CHs will be done so as to minimize energy dissipation of CHs involved in inter-cluster communication. This is how the lifetime of WSN can be enhanced.

4.1.6 PARTICLE REPRESENTATION AND INITIALIZATION IN PSO

Particle swarm optimization (PSO) is a population based stochastic optimization method which exhibits the behavior of bird flocking [194]. A flock of birds is in search of food at unknown location. Here, each bird, known as particle, represents a complete solution in search space and the food denotes the optimum solution. The best strategy to find food is to follow the bird closest to the food. PSO consists of evolutionary steps: initialization of population by generating random solutions, searching for optima after evaluating fitness value, and updating the generation.

In view of choosing optimum routing path we need to elect relay CHs with higher residual energy and more concentration but closer to BS. A particle represents optimum CH positions of L number of routing paths. The objective of PSO is to find a particle that result in best evaluation of the given objective function in eqn. (4.7). The fitness function helps to evaluate each particle for quality of the solution.

Let a swarm in PSO be constituted of N_p number of particles and the i-th particle, P_i be represented as $P_i = [X_{i,1}(t), X_{i,2}(t), \dots, X_{i,D}(t)]$ where each component $X_{i,d}(t)$ reprsents one CH; $1 \leq i \leq N_p$, $1 \leq d \leq D$. With respect to the problem, we set $D = C$ as there are C number of relay CHs along a path in WSN. Again, $X_{i,d}(t)$ denotes feasible values of CH location for the i-th routing path.

Besides $X_{i,d}(t)$, a particle P_i, $1 \leq i \leq N_p$ possesses velocity $V_{i,d}$, $1 \leq d \leq D$ in the d-th dimension of search space. With PSO a global best solution is reached at a particle that yields best result for the given fitness function.

4.1.7 DERIVATION OF FITNESS FUNCTION

The fitness function of PSO as given in eqn. (4.7) is chosen. A CH node with higher residual energy and more concentration but closer to BS has strong chance to be elected as a relay CH. Here the aim is to minimize the fitness value. A lower fitness value represents better position of particle. Alternatively, the better the particle position, better is the relay CH election.

Here, optimization problem is formulated as a linear programming problem of three objectives to achieve energy efficiency in multi-hop routing. Objective 1 denotes the total residual energy of all relay CHs along a routing path which must be maximized. A node with higher residual energy has greater probability to be elected as a relay CH. Average distance between BS and CHs represented by Objective 2 should be minimized. The greater the average distance between relay CH to BS the more is the energy dissipation. Hence that is to be avoided. Objective 3 conveys total concentration of all relay CHs, which should be maximized. A node with higher concentration has higher chance to be elected as a relay CH. In this work, the optimization problem using PSO is addressed after formulating a multi-objective linear programming as follows:

Objective 1: Maximize the total residual energy of L elected cluster heads. As the problem is of minimization type, maximizing the energy $f_1$is as good as minimizing the reciprocal of total residual energy (say, f_1) of all cluster heads.

$$\text{Minimize } f_1 = \frac{1}{\sum_{j=1}^{L} E_{CH_j}} \tag{4.4}$$

Objective 2: Minimize average BS distance (say, f_2) from CH to BS for C cluster heads as a node closer to BS has more chance over others to be CH.

$$\text{Minimize } f_2 = \frac{1}{L}\sum_{j=1}^{L} dis(CH_j, BS) \tag{4.5}$$

Objective 3: Maximize the total concentration of the set C of elected CHs over the network, which is similar to minimization of reciprocal of total concentration (say, f_3) as the problem is of minimization type. So, it is expressed as follows:

$$\text{Minimize } f_3 = \frac{1}{\sum_{j=1}^{L} n_j} \tag{4.6}$$

where n_j denotes the number of nodes within communication range of j-th cluster. In this work, we normalize $f_p, p = 1, 2, 3$ between 0 and 1 as the ratio the of difference between f_p and min (f_p) to the difference between $\max(f_p)$ and $\min(f_p)$. The objective is to minimize the linear combination of f_p , $p = 1, 2, 3$ as:

$$\text{Minimize: } F = \sum_{p=1}^{3} w_p \times f_p \tag{4.7}$$

Subject to the following constraints,

$$dis(CH_j, BS) \leq R_{max} \tag{4.8}$$

$$0 \leq w_p \leq 1, \ \sum_{p=1}^{3} w_p = 1, \quad p = 1, 2, 3 \tag{4.9}$$

$$0 < f_p < 1, \quad p = 1, 2, 3 \tag{4.10}$$

where $w_1, w_2, \text{and } w_3$ are weights used to impose the relative importance of three parameters $f_1, f_2, \text{and } f_3$. R_{max} represents the maximum communication radius of cluster heads. The values of $w_1, w_2, \text{and } w_3$ are set so as to achieve maximum lifetime of WSN.

Considering agricultural application of WSN, f_1 in eqn. (4.4) will be the most influential factor in the election of a relay CH because lifetime of a node is directly controlled by its residual energy. Besides aggregation, CHs dissipate energy in forwarding data to BS. CHs away from BS dissipate more energy than closer ones. So, lifetime of WSN is affected by f_2, corresponding to average BS distance. Thus, f_2 may be given preference over f_3, a function of node concentration. In the experiment, $w_1, w_2, \text{and } w_3$ are varied to get maximum lifetime and the respective values 0.5, 0.3, and 0.2 are found to be the optimum ones. Owing to simplicity and efficient global search ability, PSO is used to resolve the optimization problem.

4.1.8 RESULTS AND DISCUSSION

The proposed algorithm is simulated in Matlab R2013a with 100 randomly deployed sensor nodes non-uniformly spread over a network area of $100m \times 100m$. The BS is placed at centre position with no energy constraint. All sensor nodes are assumed to have same initial energy of 1J. All simulation parameters are given in Table 4.1. Weights of the fitness function in eqn. (4.7) are set as $w_1 = 0.5$, $w_2 = 0.3$, and $w_3 = 0.2$ as they provide optimum lifetime of WSN for application like agriculture. The PSO is run for 100 iterations with a swarm size of 30 and other parameters as given

in Table 4.2. In each round, CHs are elected and unequal balanced clusters are formed by adjusting the communication radii of CHs through FIS. The CHs are elected by Type-1 Sugeno FIS in Matlab R2013a based on three fuzzy inputs, namely, residual energy, distance from BS, and concentration. But, the competition radii of CHs are set based on distance to BS. The simulation is conducted over 10 different topographical areas of $100m \times 100m$ with 100 sensor nodes. In a round, 10 TDMAs have been considered. The max_round is set as 5000 in the simulation within which all nodes are expected to die.

Simulation of iCSHS, ER-HEED, PSO-UFC and LEACH-SF are performed in the same platform with parameters as in OFCA. The simulation results for these algorithms in Matlab R2013a environment are validated using the results available in the existing literature. Then simulation results of OFCA are compared with the above mentioned algorithms in terms of first node death, ten percent node death, half node death, alive and dead nodes versus round, and number of packets received in the BS. The average value of each metric in 40 runs is used to compare with other approaches. The simulation results of OFCA used to plot different observations are shown in Fig. 4.7 through Fig. 4.11 for homogeneous sensor network. This work has been validated in heterogeneous sensor network as shown in Fig. 4.12.

OFCA extends lifetime of WSN in terms of improved FND, TND, and HND because of unequal balanced clustering, efficient CHs election through FIS and multi-hop data forwarding from CHs to BS. In the proposed algorithm, efficient CHs are dynamically elected for each cluster using optimized fuzzy rule base. Unlike existing fuzzy based approaches, the fuzzy rule base is tuned for large application of WSN like agricultural monitoring to elect the best CHs. Multi-hop data forwarding from CH to BS via other CHs avoids the chance of creating energy holes as well as loss of packets at BS. Again, hot spot problem is ignored through introduction of unequal clustering.

The effectiveness of proposed algorithm is shown in Fig. 4.7 in terms of number of alive nodes versus number of rounds. From Fig. 4.7 it is clear that OFCA outperforms others due to balanced clustering. Network lifetime is assessed in terms of FND, TND, and HND in Fig. 4.8 and Fig. 4.9. In simulation, FND, TND and HND are measured through number of rounds. Fig. 4.8 shows lifetime of WSN in terms of FND and TND. It reveals that PSO-UFC outperforms iCSHS due to unequal and fault tolerant clustering. Although LEACH-SF is superior to ER-HEED when FND is considered, but ER-HEED provides 18% betterment than them when TND is considered. OFCA improves FND by 27% than LEACH-FL, 58% than ER-HEED, and 11% than LEACH-SF due to its unequal balanced clustering. In application like agricultural monitoring, HND is more significant than FND because death of first or a few nodes does not affect agricultural data collection. So, improvement in TND and HND is desirable than FND in such type of WSN application. Fig. 4.9 conveys that the proposed algorithm attains a considerable improvement in terms of HND. The reason for such fact is that

proposed approach follows unequal clustering and multi-hop routing in contrast to single-hop routing as in LEACH-SF.

Performances of OFCA are evaluated in a heterogeneous network with varying heterogeneity levels in terms of FND. Simulation settings are same as in Table 4.1 except nodes with random initial energy between 0.2 and 0.8J.

Table 4.1. Details of simulation parameters

Parameter	Value
Network size	100x100m^2
No. of nodes	100
Initial energy	1J
E_{elec}	50 nJ/bit
ε_{fs}	100 pJ/bit/m^2
ε_{amp}	0.013pJ/bit/m^4

Table 4.2. Parameters for PSO

Parameters	Value
Number of particles	30
Iterations	100
w_1	0.5
w_2	0.3
w_3	0.2

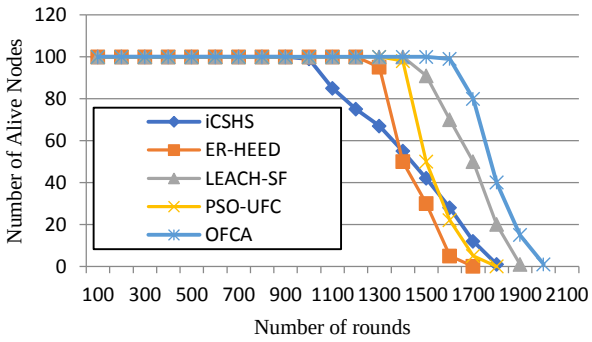


Fig. 4.7. Number of alive nodes versus rounds with 100 sensor nodes

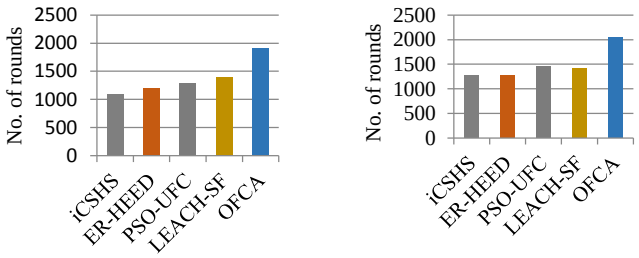


Fig. 4.8. Lifetime (a) First Node Death (FND)[rounds] (b) Ten percent Node Death (TND), with 100 nodes.

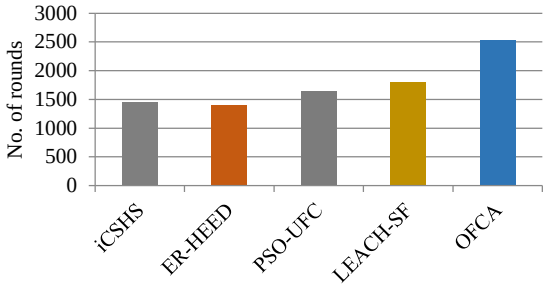


Fig. 4.9. Time to Half of Nodes Die (HND)[rounds], with 100 nodes

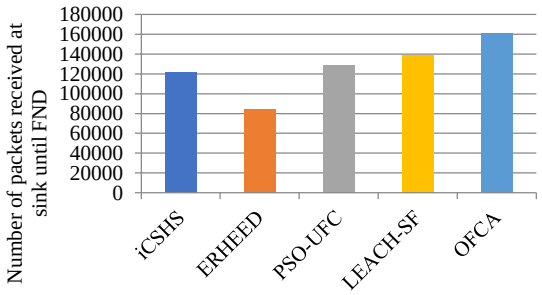


Fig. 4.10. Number of packets received at sink until FND

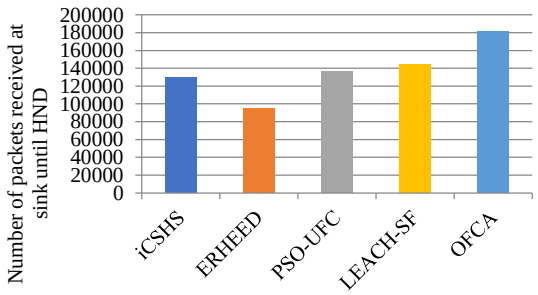


Fig. 4.11. Number of packets received at sink until HND

Fig. 4.10 and Fig. 4.11 depict the number of packets received in BS until FND and HND respectively. Number of packets received at BS is measured so as to indicate that the WSN remain operative even after FND and HND. It is shown that the proposed algorithm outperforms others due to its multi-hop data forwarding from CHs to BS.

With 10% heterogeneous nodes (Fig. 4.12(a)), it is found that OFCA is more energy efficient than not only UHEED and REECHD protocols which are commonly used in homogeneous WSN but also FMUC and DEBUC which are adopted in heterogeneous WSN. This is because OFCA reduces intra-cluster traffic near sink and handles uncertainties in CH election in a better way.

In Fig. 4.12(b) with increased heterogeneity level (40%), proposed protocol OFCA falls behind REECHD. The probable reason behind this is that, although the WSN is heterogeneous (40%), OFCA experiments did not consider node heterogeneity in particular, and all types of nodes, irrespective of their capability or capacity, were considered as prospective candidates for CH. It also appeared that other parameters that are not required to be considered in homogeneous WSN are required to be considered for heterogeneous WSN. Hence network lifetime for OFCA decreases with respect to REECHD in this case.

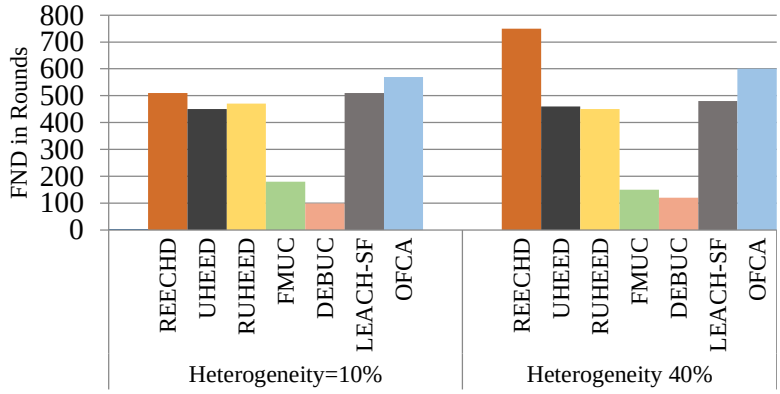


Fig. 4.12. Network lifetime (FND) comparison of protocols in heterogeneous network with (a) 10% and (b) 40% heterogeneity levels, intra-traffic rate limit=50%

4.2 AN ADAPTIVE ROUTING PROTOCOL FOR OPTIMIZING ENERGY HARVESTING TIME IN WSN

Once sensors are deployed in field, generally they remain unattended. They use up battery power in sensing and forwarding data. Consideration of proper routing protocols has become essential in WSN for energy efficient operation. Routing algorithms try to find optimum path to send data to sink node in order to minimize usage of battery energy [195], [196]. It is seen that most routing protocols use similar strategy for the entire network at any instant of time. However, adopting suitable strategy based on local network parameters for the application area seems to be a better approach with respect to efficiency. This chapter proposes technique where message sending strategy will be tuned by local level trade-off. The proposed technique has also considered that instead of switching to sleep mode, the sensor node will harvest energy if its energy falls below a certain threshold. Energy can be harvested from various ambient sources like solar, thermal, vibration and wireless radio frequency energy [197], [198], [199], in clustered WSN.

This chapter proposes an adaptive cross layer protocol with self-sufficient energy harvesting technique. As this protocol is capable to adapt to network parameters based on lower level parameters, it achieves energy efficiency. Table 4.3 describes different symbols used in this chapter.

The remainder of the section is organized as follows. Hierarchical nature of network parameters is illustrated in Section 4.2.1. Parameters for optimizing MAC layer protocol are considered in Section 4.2.2. Section 4.2.3 gives the algorithmic outline of adaptive routing protocol while Section 4.2.4 provides calculation of different parameters. Energy harvesting schedule is mentioned in Section 4.2.5 and the algorithm is given in Section 4.2.6. Performance evaluation is done in Section 4.2.7.

4.2.1 HIERARCHICAL NATURE OF NETWORK PARAMETERS

There are different parameters that characterize the cross layer protocol at local level based on which decisions of routing are made. The network will adapt itself locally that will lead it to the global optimization of parameters like life time of the network, energy harvesting time and network coverage. Different intermediate parameters will be derived from lower level parameters. It is assumed that there will be m level of parameters. Intermediate level parameters that depend on other parameters are denoted by I_{ij} (j^{th} parameter at i^{th} level). Independent parameters for different levels are denoted by L_{ij} . The solution approach can be represented as a bottom up structure in Fig. 4.13.

Table 4.3. Description of symbols

Parameters	Description
δ	Percentage of time a node will remain active for message transmission/reception
e_{rem}^{i}	Remaining energy of i^{th} node.
$e_{\max}$	Maximum energy storing capacity of battery
ξ	Percentage of communication synchronicity
m_i^d	Message density at the i^{th} node
n_i^d	Node density of a local region centering the i^{th} node
$n_{\max}$	Maximum possible node density(hypothetically assumed)
η_i	Regular occurrence of data in the surrounding region of i^{th} node
ρ	Reactiveness/Proactiveness of the network
τ_i	Parameter determining cluster head for i^{th} cluster
k_i	Different constants where i is natural number
RT_j	Routing table for j^{th} node
d_{avg}^{k}	Average distance of neighbor nodes from node k

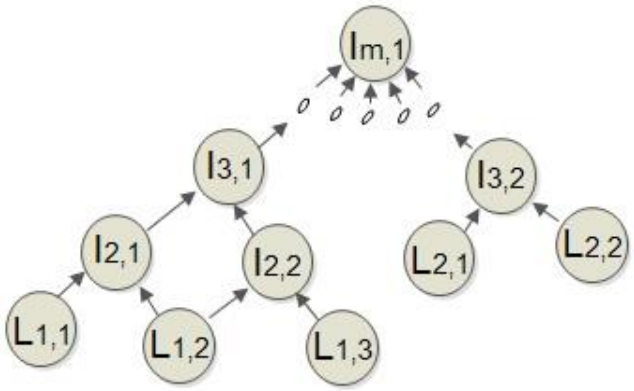


Fig. 4.13. Bottom up approach for finding network parameters

Fig. 4.13 shows the example of how to get upper level parameters by using lower level parameters. For eample, $I_{3,1}$ and $I_{2,1}$ are derived according to eqn. (4.11) and eqn. (4.12) as:

$$I_{3,1} = I_{2,1} \otimes I_{2,2} \tag{4.11}$$

$$I_{2,1} = L_{1,1} \otimes L_{1,2} \tag{4.12}$$

In this way, we can get the expression for $I_{m,1}$

$$I_{m,1} = I_{m-1,1} \otimes I_{m-1,2} \ldots\ldots \otimes I_{m-1,n} \otimes L_{m-1,1} \otimes L_{m-1,2} \ldots\ldots \otimes L_{m-1,k} \tag{4.13}$$

The eqn. (4.11), eqn. (4.12) and eqn. (4.13) are sample equations for finding the final parameters $I_{m,1}$. Thus the intermediate parameters can be found based on local independent parameters, where $\otimes$ represents an operator.

4.2.2 PARAMETERS FOR OPTIMIZING MAC LAYER PROTOCOL

Design of the MAC layer protocol considers contention in the network, frequency of event occurrence, and remaining energy of sensor node among others [17], [200]. Based on these parameters the protocol can be designed to be either synchronous or asynchronous for message transmission. Also, these parameters will determine the time a node will spend on energy harvesting and the duration for which the node will remain active within certain period of time. To do so, estimation of few intermediate parameters like δ (percentage of time a node will remain active for message transmission/reception), ξ (percentage of communication synchronicity) and ρ (reactiveness/proactiveness of the network) will be necessary. This is required in order to tune various network parameters for obtaining an optimum protocol for MAC layer.

A. PERCENTAGE OF TIME A NODE TO REMAIN ACTIVE (δ)

When remaining energy is low, energy harvesting time will be increased in comparison with the active time period. On the contrary, when remaining energy of a node becomes high, the node involves itself more in active mode. Therefore, we can say

$$\delta \alpha \left(e_{rem}^{j} / e_{\max} \right) \tag{4.14}$$

Again, when node density increases then per node message sending responsibility will decrease since there will be alternate nodes available for forwarding. Thus, nodes get involved in energy harvesting. Therefore, we can say

$$\delta\alpha\left(n_i^d \Big/ n_{\max}\right)^{-1} \tag{4.15}$$

Combining eqn. (4.14) and eqn. (4.15), we get the following:

$$\delta = k_1\left(e_{rem}^i / e_{\max}\right)\left(n_i^d / n_{\max}\right)^{-1} \tag{4.16}$$

where k_1 is a constant and n_{max} is the maximum node density which may be equal to total number of deployed nodes.

B. THE PERCENTAGE OF SYNCHRONOUS COMMUNICATION (ξ)

With high node density, the network will be relatively with lower contention, because per node message transmission will be less. Message density decreases with increase in node density. Therefore, the percentage of synchronous communication will decrease with increase in the value of node density n_i^d in the local area centring i-th node. Thus, the relation between percentage of synchronous communication (ξ) parameter and node density n_i^d is:

$$\xi\alpha\left(n_i^d \Big/ n_{\max}\right)^{-1} \tag{4.17}$$

Intuitively, it can be said that if the message density (m_i) becomes higher, then the value of synchronous communication parameter (ξ) will be higher. Therefore, the relation between ξ and m_i is as follows:

$$\xi\alpha\left(m_i \Big/ m_{\max}\right) \tag{4.18}$$

Higher value of the parameter representing the regular occurrence of data (η) means that message is coming in regular intervals. Thus, an increase in the value of η means percentage of synchronous communication will increase and therefore the value of ξ will increase. Therefore, the relation between ξ and η can be expressed as directly proportional to each other:

$$\xi\alpha\left(\eta_i \Big/ \eta_{\max}\right) \tag{4.19}$$

Combining eqn. (4.17), eqn. (4.18) and eqn. (4.19), we get eqn. (4.20) as given below:

$$\xi = k_2\left(\frac{n_i^d}{n_{\max}}\right)^{-1}\left(\frac{m_i}{m_{\max}}\right)\left(\frac{\eta_i}{\eta_{\max}}\right) \tag{4.20}$$

where k_2 is a constant.

C. PROACTIVENESS OF THE NETWORK

Generally, in case of higher contention in message transmission, proactiveness of network proves to be beneficial. Conversely, in case of lower contention based application, reactiveness of the network is required. The value of ρ determines how the network will function: proactive or reactive. If the value of ρ is high, then it signifies that the network is more proactive and less reactive. Thus, it can be said that if regular occurrence of data increases, then proactiveness of the network should increase, conversely, the reactiveness of the network will decrease. From the above discussion it can be said that the percentage of synchronous communication is related to parameters: n_i^d, m_i and η_i. Thus, percentage of synchronous communication (ξ) is a function of n_i^d, m_i, and η_i. Therefore, the relation between reactiveness of the network (ρ) and (ξ) is:

$$\rho \propto \left(\frac{\xi}{\xi_{max}} \right) \tag{4.21}$$

When energy is low, the nodes will be involved more in energy harvesting mode. Therefore, the network has less number of messages. In this circumstance, reactiveness of the network will increase. Therefore, the parameter 'percentage of time a node remains active' (δ) will be directly proportional to the parameter ρ.

$$\rho \propto \left(\frac{\delta}{\delta_{max}} \right) \tag{4.22}$$

Combining eqn. (4.21) and eqn. (4.22), we get,

$$\rho = k_3 \left(\frac{\xi}{\xi_{\max}} \right) \left(\frac{\delta}{\delta_{\max}} \right) \tag{4.23}$$

From eqn. (4.16) and eqn. (4.20), eqn. (4.23) can be written as:

$$\rho = k_4 \left(\frac{e_{rem}^i m_i \eta_i}{\left(n_i^d \right)^2} \right) \tag{4.24}$$

where,

$k_4 = k_1 k_2 k_3 \left(\frac{1}{\delta_{\max} \xi_{\max}} \right) \left(\frac{\left(n_{\max}^2 \right)^2}{e_{\max} m_{\max} \eta_{\max}} \right)$ is a constant.

4.2.3 ALGORITHMIC STRUCTURE OF THE ADAPTIVE ROUTING PROTOCOL

The proposed cross-layer protocol works in the following two phases.

A. SETUP PHASE

The network is logically divided into several smaller regions, called clusters using LEACH protocol [19]. Excepting election of cluster head, the current protocol follows LEACH protocol in set up phase. Priority based cluster head election approach is adopted in this protocol. Each cluster will have one cluster head node. Other nodes take part in decision to elect a cluster head and join a cluster according to the signal strength of the cluster head node. During message transmission, every node will send priority value for election of cluster head node along with the sensed data. Priority value signifies the measurement of relative preference for cluster head node among all neighboring nodes. The preference of a node as a cluster head depends on remaining energy of that node and distance from the neighbor nodes. Priority is assigned by individual node for each other node. Total priority assigned by different nodes will evaluate the final priority of a node. The priority of node j to become a cluster head as assigned by node i is denoted as $p_{j,i}$ .Here, higher priority value indicates that the network is proactive rather than reactive. Therefore, $p_{j,i}$ is directly proportional to ρ_j^{α} (where ρ_j denotes the reactiveness of the network in the surrounding area of node j and α is the priority constant with respect to proactiveness). Since priority of a node to become cluster head will be higher if the node resides at a shorter geographical distance, we can say $p_{j,i}$ is inversely proportional to d_{ji}^{β}, where β is priority constant with respect to distance. Here, relatively greater value of α with respect to β determines the network to be more proactive. Therefore, we can say α enforces priority over proactiveness of the network, and β enforces priority over the reactiveness of the protocol. Let, e_j be remaining energy of node j and d_{ji} the distance between node j and node i. Eqn. (4.25) represents the relative priority of node j with respect to the neighbor node i.

$$p_{i,j} = \frac{\left(\rho_j\right)^{\alpha}}{\left(d_{j,i}\right)^{\beta}}$$

or,

$$p_{i,j} = k_4^{\alpha} \frac{\left(e_{rem}^{j}\right)^{\alpha} m_j^{\alpha} \eta_j^{\alpha}}{\left(n_j^{d}\right)^{2\alpha} \left(d_{j,i}\right)^{\beta}} \tag{4.25}$$

At the end of a steady state, every node j will calculate the *overall priority* τ_j which will determine the cluster head. For a particular node j the parameter τ_j is calculated as

$$\tau_j = \sum_{i=1}^{N} p_{i,j} \tag{4.26}$$

If other parameters are kept constant and e_{rem}^{j} is varied, then eqn. (4.26) can be rewritten as:

$$\tau_j = k_5 \left(e_{rem}^{j}\right)^{\alpha} \tag{4.27}$$

where,

$$k_5 = k_4^{\alpha} \frac{m_j^{\alpha} \eta_j^{\alpha}}{\left(n_j^{d}\right)^{2\alpha}} \sum_{i=1}^{N} \frac{1}{\left(d_{j,i}\right)^{\beta}}$$

If the value of τ_j is greater than threshold value (τ_{th}), then that node will declare itself as a cluster head node.

Theorem I: If the value of τ_j is greater than the value of τ_k while other parameters remain same then the remaining energy of node j is greater than that of node k.

Proof: After simplifying the expression, $\tau_j - \tau_k$ becomes

$$\tau_j - \tau_k = k_5 \left\{ \left(e_{rem}^{j}\right)^{\alpha} - \left(e_{rem}^{k}\right)^{\alpha} \right\} \tag{4.28}$$

From eqn. (4.28), it can be said that there is greater chance of the node possessing more remaining energy than others to become CH. Now, if $\tau_j - \tau_k > 0$, three cases may arise with respect to threshold value (τ_{th}):

Case 1: $\tau_j > \tau_k > \tau_{th}$

According to Case 1, the τ value of node j and node k are greater than the threshold value τ_{th}. The algorithm can, therefore choose any node as the cluster head. If node k is chosen, then unequal energy dissipation may occur. The previous assumption is true until a certain limit which will be discussed under Case 2.

Case 2: $\tau_j > \tau_{th} > \tau_k$

In case 2, the value of τ for node j is greater than threshold value τ_{th} whereas the value of τ for node k is less than τ_{th}. In this circumstance, the algorithm will choose node j as the cluster head. Following case 1, choosing node k rather than node j increases energy difference between two nodes. Once the τ value falls under the threshold value then algorithm will not prefer node k any more over node j. Therefore, we can say that energy difference is generated in case 1 and that is overcome if case 2 arises. Therefore, a uniform energy distribution criterion has been satisfied.

Case 3: $\tau_{th} > \tau_j > \tau_k$

According to case 3, the threshold τ_{th} is greater than the values of τ for both nodes (τ_j and τ_k), and thus, no node will be elected as the cluster head node. Node j and node k will act as multi-hop relay nodes only. The nodes will remain reactive in nature. The node whose priority value is less than τ_{th} signifies that its remaining energy is reduced to threshold level and will be involved in energy harvesting. During the period messages coming from neighbour nodes will be forwarded in reactive mode. The node having more remaining energy will be chosen for sending a message to the next hop. Therefore, from above discussion it can be said that the proposed routing protocol ensures uniform energy dissipation.

Theorem II: The value of τ_j is greater than the value of τ_k when the number of neighbour nodes of node j is greater than that of the node k while other parameters remain unchanged.

Proof: While other parameters remain constant and number of neighbour nodes varies for node j and node k then the expression for $\tau_j - \tau_k$ will be

$$\tau_j - \tau_k = \frac{k_4^{\alpha} \left(e_{rem}^{j}\right)^{\alpha} m_j^{\alpha} \eta_j^{\alpha}}{\left(n_j^{d}\right)^{2\alpha} d_j^{\beta}} \left\{N_j - N_k\right\} \tag{4.29}$$

Here, N_j and N_k are number of neighbour node of node j and node k respectively. From the previous discussion and from eqn. (4.27), it can be said that if $\tau_j > \tau_k$,then $N_j > N_k$. In other words, it can be said that a node with more number of neighbour nodes, with other parameters remaining same, gets more priority to become the cluster head node.

Theorem III: The value of τ_j is greater than τ_k when average distance of node j from its neighbour nodes is less than that of node k assuming other parameters are the same for both node.

Proof: From eqn. (4.25), it is seen that β mean square value of distance is inversely proportional to the value of τ. Let us assume d_j^{avg} is the β mean square value for node j. Thus, τ_j will be

$$\tau_j = \frac{k_4^{\alpha}\left(e_{rem}^{j}\right)^{\alpha} m_j^{\alpha}\eta_j^{\alpha}N_j}{\left(n_j^{d}\right)^{2\alpha}\left(d_j^{avg}\right)^{\beta}} \tag{4.30}$$

Therefore, expression for $\tau_j - \tau_k$ will be

$$\tau_j - \tau_k = \frac{k_4^{\alpha}\left(e_{rem}^{j}\right)^{\alpha} m_j^{\alpha}\eta_j^{\alpha}N_j}{\left(n_j^{d}\right)^{2\alpha}\left(d_k^{avg}d_j^{avg}\right)^{\beta}}\left\{\left(d_k^{avg}\right)^{\beta} - \left(d_j^{avg}\right)^{\beta}\right\} \tag{4.31}$$

From (4.31), it can be said that a node obtains higher priority for becoming a cluster head node if follower nodes reside relatively closer to it. This result signifies the positional importance of cluster head node.

B. STEADY STATE PHASE

In the steady state phase, sensor nodes are mainly involved in communication, energy harvesting and sleep schedule. Thecluster headnode gets network information from the member nodes. Using this information, the cluster head node calculates the network parameters ξ, δ and ρ. Thereafter, the cluster head sends the values of these parameters to the member nodes of that cluster along with the time schedule for each node. After getting the parameters, individual member node decides the mode of message transmission like synchronous transmission (TDMA), asynchronous transmission (CSMA) or combination of synchronous and asynchronous type of message transmission to be followed. The duration of the steady state is also variable and it depends on different parameters.

4.2.4 CALCULATION OF DIFFERENT PARAMETERS

If the parameters ($e_{rem}^{j}, m_j, n_j^{d}, \eta_j$ and $d_{j,i}$) and constant k_4 are calculated, then we are able to calculate the parameter $p_{i,j}$ can also be calculated, from which τ_j can be calculated. Knowing the value of τ_j, a node j can decide whether it will become a cluster head node or not.

A. CALCULATION OF CONSTANT k_4

Let us assume the values of k_1, k_2 and k_3 to be each 1 then the value of k_4 becomes $\left(\frac{1}{\delta_{\max}\xi_{\max}}\right)\left(\frac{\left(n_{\max}^{d}\right)^2}{e_{\max}m_{\max}\eta_{\max}}\right)$, where every parameter is in absolute form and that can be assumed as the known parameters. Therefore, from the above the value of constant k_4 can be found out. The modified expression for $p_{i,j}$ will be

$$p_{i,j}=\left(\frac{1}{\delta_{\max}\xi_{\max}}\right)^{\alpha}\left(\frac{\left(n_{\max}^{d}\right)^2}{e_{\max}m_{\max}\eta_{\max}}\right)^{\alpha}\frac{\left(e_{rem}^{j}\right)^{\alpha}m_j^{\alpha}\eta_j^{\alpha}}{\left(n_j^{d}\right)^{2\alpha}\left(d_{j,i}\right)^{\beta}} \tag{4.32}$$

B. CALCULATION OF NODE DENSITY IN THE REGION SURROUNDING NODE *j*

Here, n_j is the node density with respect to the j^{th} node. At the time of communication, j^{th} node receives message from its neighbour nodes. Suppose, total number of neighbour node for node j is a_j and the communication range of node j is r. Therefore, within area of πr^2 total number of nodes present including j^{th} node is a_j. So, the node density is $a_j/\pi r^2$. Thus, the value of n_j^d is equal to $a_j/\pi r^2$. The modified expression for $p_{i,j}$ will be

$$p_{i,j}=\left(\frac{1}{\delta_{\max}\xi_{\max}}\right)^{\alpha}\left(\frac{\left(n_{\max}^{d}\right)^2}{e_{\max}m_{\max}\eta_{\max}}\right)^{\alpha}\frac{\left(e_{rem}^{j}\right)^{\alpha}\pi^{2\alpha}r^{4}m_j^{\alpha}\eta_j^{\alpha}}{\left(a_j\right)^{2\alpha}\left(d_{j,i}\right)^{\beta}} \tag{4.33}$$

C. CALCULATION OF MESSAGE DENSITY IN THE REGION SURROUNDING NODE J

Here, m_j is the message density in the region surrounding by node j. Node j will calculate the number of messages that came to it per unit time and let that be b_j. Since the number of nodes number in the surrounding region of node j is a_j, then message density (message sending per node) is b_j / a_j. Therefore the value of m_j is b_j / a_j. Thus, the modified expression for $p_{i,j}$ will be

$$p_{i,j} = \left(\frac{1}{\delta_{\max} \xi_{\max}} \right)^{\alpha} \left(\frac{\left(n_{\max}^{d} \right)^2}{e_{\max} m_{\max} \eta_{\max}} \right)^{\alpha} \frac{\left(e_{rem}^{j} \right)^{\alpha} \pi^{2\alpha} r^4 b_j^{\alpha} \eta_j^{\alpha}}{\left(a_j \right)^{3\alpha} \left(d_{j,i} \right)^{\beta}} \tag{4.34}$$

D. CALCULATION OF DISTANCE BETWEEN NODE i AND j

The distance between node i and node j can be estimated by the signal strength indicators of receiver and sender using the equation below.

$$\frac{P_r}{P_t} = G_t . G_r \left(\frac{\lambda}{4\pi d} \right)^2 \tag{4.35}$$

where, P_r is received power, P_t is transmitted power, G_t and G_r are transmitter and receiver antenna gains respectively, and d denotes the distance between receiver and sender.

E. CALCULATION OF REGULAR OCCURRENCES OF DATA IN THE REGION SURROUNDING NODE J

Here, η_j denotes the regular occurrences of data at time instants: t_1, $t_2, t_3 \ldots t_n$. Let us assume the mean value of t_1, $t_2, t_3 \ldots t_n$ be t_{mean}.

Theorem IV: When events occur at regular interval then the standard deviation of time difference of data occurrence will be lower.

Proof: Let us assume, D is the difference matrix as below:

$$D = \{t_2 - t_1, t_3 - t_2, ..., t_n - t_{n-1}\}$$

or, $D = \{\Delta t_{2,1}, \Delta t_{3,2}, ..., \Delta t_{n,n-1}\}$

Let us assume, Δt_{mean} be the mean of set D

$$\Delta t_{mean} = \sum_{i=2,\, j=1}^{n,n-1} t_{i,j} / (n-1) \tag{4.36}$$

Assuming s_j to be the standard deviation of set D

$$s_j = \sqrt{\sum_{i=1}^{n} \left(\Delta t_{i,i-1} - \Delta t_{mean} \right)^2 / n}$$

$$s_j^2 = \sum_{i=1}^{n} \left(\Delta t_{i,i-1} - \Delta t_{mean} \right)^2 / n$$

$$s_j^2 = \frac{\left(\Delta t_{2,1} - \Delta t_{mean} \right)^2}{n} + \frac{\left(\Delta t_{3,2} - \Delta t_{mean} \right)^2}{n} + ... + \frac{\left(\Delta t_{n,n-1} - \Delta t_{mean} \right)^2}{n} \tag{4.37}$$

The minimum value of $\left(\Delta t_{2,1} - \Delta t_{mean} \right)^2$ is zero when $\Delta t_{2,1} = \Delta t_{mean}$. Therefore, the value of s^2 will be minimum when

$$\Delta t_{2,1} = \Delta t_{3,2} = .. = \Delta t_{n,n-1} = \Delta t_{mean} \tag{4.38}$$

Hence, it can be said that eqn. (4.38) is the condition when s_j will be minimum. Alternatively, we can also write eqn. (4.38) for any i, $1 < i < n$

$$\Delta t_{i,i-1} = \Delta t_{i+1,i}$$

$$t_i - t_{i-1} = t_{i+1} - t_i$$

$$t_i = \frac{\left(t_{i+1} + t_{i-1} \right)}{2} \tag{4.39}$$

Eqn. (4.39) expresses the condition that s_j be minimum. As eqn. (4.39) is true for all i, we can say the message arriving times are sequential in nature. Therefore, from the above discussion it is obvious that if message comes in regular interval then the standard deviation of time difference of data

occurrence will be low and in ideal case it will be zero. Now, η_j can be represented by s_j. Therefore, the modified equation of $p_{i,j}$ will be

$$p_{i,j} = \left(\frac{1}{\delta_{\max}\xi_{\max}}\right)^{\alpha}\left(\frac{\left(n_{\max}^{d}\right)^{2}}{e_{\max}m_{\max}\eta_{\max}}\right)^{\alpha} \frac{\left(e_{rem}^{j}\right)^{\alpha}\pi^{2\alpha}r^{4}b_j^{\alpha}s_j^{\alpha}}{\left(a_j\right)^{3\alpha}\left(d_{j,i}\right)^{\beta}} \tag{4.40}$$

In eqn. (4.40), the parameters $\delta_{\max}, \xi_{\max}, e_{\max}, m_{\max}, n_{\max}, \eta_{\max}, \alpha, \beta, r$ will be predefined and the parameters $a_j, b_j, s_j, d_{i,j}$ can be measured as discussed above. Therefore, the proposed algorithm can find out $p_{i,j}$ without any ambiguity. From $p_{i,j}$, the value of τ_j can be calculated. Knowing the value of τ_j the node can decide whether the current node will be the cluster head or not.

4.2.5 ENERGY HARVESTING SCHEDULE

Energy harvesting scheduling is made during the steady state phase. The scheduled time for energy harvesting of a particular node depends on the remaining energy of the node. As the remaining energy decreases the scheduled time of energy harvesting of a node increases which is depicted in Fig. 4.14. Initially in phase 1, there is no need of energy harvesting as nodes are fully charged. In steady state phase 2, nodes loose energy a bit. So, they need to harvest energy by decreasing active state. While in steady state phase 3, as nodes lose more energy, more time is scheduled for energy harvesting compared to active time. We can express scheduled time for energy harvesting of node j as:

$$T_H^j = T_H^{\max}\left(1 - \frac{e_{rem}^{j}}{e_{\max}}\right) \tag{4.41}$$

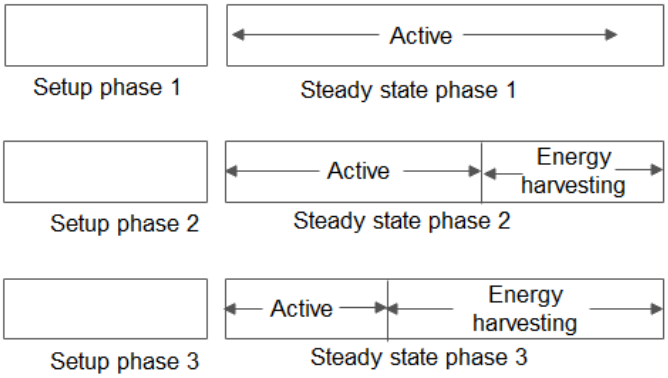


Fig. 4.14. Time schedule of active phase and energy harvesting phase

4.2.6 PROPOSED ALGORITHM

Setup phase

1. Deploy sensor nodes in application area.
2. Set the initial values of parameters:

   $\delta_{\max}, \xi_{\max}, n_{\max}, e_{\max}, m_{\max}, \eta_{\max}, \alpha, \beta, r$.
3. Initially, every node will send message to its neighbor node.
4. Each node i calculates the distance ($d_{i,j}$) from any arbitrary node j using eqn. (4.35).
5. After receiving initial message, node j measures parameters a_j, b_j, s_j and $d_{i,j}$.
6. Each node j calculates its priority $P_{i,j}$ with respect to any node i using eqn. (4.33).

$$p_{i,j} = \left(\frac{1}{\delta_{\max} \xi_{\max}} \right)^{\alpha} \left(\frac{\left(n_{\max}^{d} \right)^2}{e_{\max} m_{\max} \eta_{\max}} \right)^{\alpha} \frac{\left(e_{rem}^{j} \right)^{\alpha} \pi^{2\alpha} r^4 m_j^{\alpha} \eta_j^{\alpha}}{\left(a_j \right)^{2\alpha} \left(d_{j,i} \right)^{\beta}}$$

7. Each node j calculates over all priority (τ_j) with respect to its neighbor nodes as:

$$\tau_j = \sum_{i=1}^{N} p_{i,j}$$

8. If τ_j is greater than τ_{th}, then node j declares itself as cluster head and sends message to its neighbor nodes.

Steady state phase

1. Non cluster head nodes sense data and send it to cluster head.

2. Cluster head node collects data from different source nodes or higher gradient cluster head node (s).
3. Data are aggregated by cluster head node and sent either to the next cluster head node with lower gradient or to sink.
4. Nodes follow energy harvesting and wakeup schedule (Fig. 4.14 explains the scenario).

4.2.7 PERFORMANCE EVALUATION

For evaluating the performance of the proposed protocol, a WSN with 400 nodes capable of harvesting environmental energy is simulated. Nodes are randomly deployed over an area of 100 m × 100 m. size of each data packet is considered to be 200 bytes in this experiment. The detail of simulation parameters is listed in Table 4.4. The calculation of energy consumed by transmitter and receiver is done as per the energy model in [19]. We compared the proposed adaptive routing with low energy adaptive clustering hierarchy (LEACH), hybrid energy efficient distributed (HEED) cluster-based routing protocol, and secure routing protocol with energy harvesting by Alrajeh et al. [33]. Fig. 4.15 depicts the network lifetime of three protocols in terms of number of rounds. The ability of the proposed cross layer protocol to adapt network parameters hierarchically increases network lifetime with respect to the others.

In Fig. 4.16, the remaining network energy is shown in terms of number of rounds. Due to efficient balance between energy harvesting and active time, the proposed approach outperforms others. In LEACH, network energy reduces faster with increasing no. of rounds. As there is no concept of energy harvesting in HEED, network energy decreases gradually after 40 rounds. A comparison of routing overhead (in terms of bit/sec) of algorithms is shown in Fig. 4.17. It reveals that proposed algorithm has higher overhead than LEACH but fewer than others. Fig. 4.18 depicts number of live nodes with respect to number of rounds in increased traffic scenario towards destination. The proposed protocol can support the WSN with more than 350 nodes even after 2000 rounds due to efficient cluster head election and energy harvesting.

Table 4.4. Details of simulation parameters

Parameter	**Value**
Network size	100x100m^2
No. of nodes	400
Initial energy	1J
Packet size	200 bytes
E_{elec}	50 nJ/bit
ε_{fs}	100 pJ/bit/m^2
ε_{amp}	0.013pJ/bit/m^4

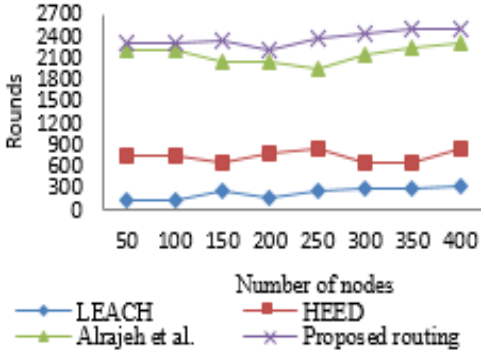


Fig. 4.15. Network lifetime in number of rounds

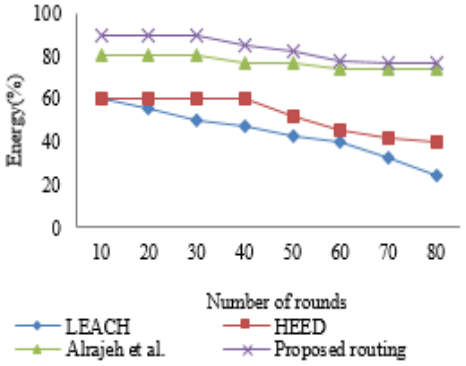


Fig. 4.16. Remaining network energy of a WSN with 400 nodes

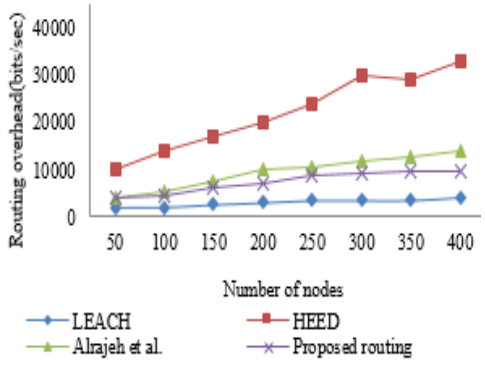


Fig. 4.17. Routing overhead comparison in bits/sec

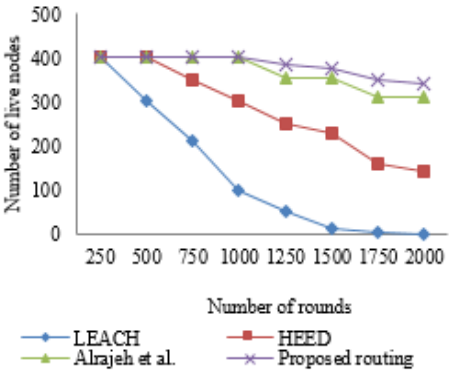


Fig. 4.18. Number of live nodes in increased traffic scenario

In a nutshell, a comparison of the proposed algorithm with LEACH, HEED, and work of Alrajeh et al. [33] on the basis of balanced clustering, clustering stability, sleep-awake aware, and cross-layer design is provided in Table 4.5.

Table 4.5. Comparison of proposed algorithm with other algorithms

Clustering approach	**Balanced clustering**	**Clustering stability**	**Sleep-awake aware**	**Cross-layer design**
LEACH	Not good	Moderate	No	No
HEED	Good	High	No	No
Alrajeh et al.	Good	Moderate	Yes	Yes
Proposed routing	Good	High	Yes	Yes

4.3 CHAPTER SUMMARY

This chapter deals with energy efficiency of WSN. It consists of two sections. Section 4.1 presents an optimal fuzzy clustering algorithm for achieving energy efficiency of underlying WSN while Section 4.2 includes an adaptive routing protocol with energy harvesting sensors. In Section 4.1, an energy efficient clustering algorithm elects cluster heads using type-1 fuzzy logic based on remaining energy, distance from sink, and concentration of nodes. The communication radii of cluster heads are calculated based on distance from BS using fuzzy logic. In proposed work, unequal balanced clusters are formed by setting different communication radii of cluster heads. An effort has been made to find optimum routing path to sink station via cluster heads. The optimization problem is solved by particle swarm optimization with a fitness function so as to choose relay cluster heads. Multi-hop routing is followed to transmit packets to sink in order to avoid early death of cluster heads in larger applications. Simulation results reveal that the proposed clustering algorithm outperforms other clustering algorithms in terms of lifetime and throughput. This work is validated on heterogeneous network and seems better than other related algorithms with limited heterogeneity. This clustering algorithm is limited to stationary sensor nodes only. In future, the work can be extended by including mobile sensor nodes and/or sink nodes.

Now-a-days, sensor nodes are also capable of harvesting energy from ambient energy sources like sunlight, vibration. Section 4.2 presents an adaptive routing protocol for optimizing energy harvesting time in WSN. Based on various network parameters, energy harvesting schedule is fixed. A routing protocol is also suggested for energy harvesting WSN. A run time optimization of various network parameters based on cross layer protocol for energy harvesting in WSN is also proposed in this section. Depending on some parameters like node density, remaining energy and message density, the network adjusts its cross-layer protocol policies for certain duration of time. Every node sends the relative preference value for electing a cluster head node. The proposed scheme minimizes the active periods of sensor nodes by maintaining efficiency and reliability of the network and application. In terms of number of rounds and remaining energy, this algorithm performs better than other algorithm as it is able to balance clustering and sleep awake scheduling.

As location awareness is one of the characteristics of a wide range of WSN based applications, accurate and secure localization techniques are developed in the next chapter. The next chapter deals with localization of WSN nodes.

CHAPTER FIVE

FUZZY LOGIC BASED LOCALIZATION TECHNIQUES

The design and production of low cost sensors have enabled successful application in areas like healthcare, agriculture, livestock, smart city, etc. After deployment of sensors in an application area, sensed data are aggregated and collected and decision making is done at sink. Irrespective of applications, the collected data has a limited or no use without knowing the locations from where the data is collected. In this context, location awareness becomes an essential task in every application of WSN. Localization is the process by which the location of an unknown node is estimated in terms of the locations of few known nodes called anchors or beacon nodes. As attaching Global Positioning System (GPS) to every sensor node is not feasible with respect to cost, only the anchors have GPS and all other unknown nodes estimate their locations with the help of those anchors.

Knowing the precise location of sensor nodes in agricultural field of interest is sometimes needed to take timely decision about farming. Localization without GPS is made possible by estimating the distance between two nodes from the received signal strength indicator [13], time-of-arrival, angle-of-arrival. This process involves uncertainty and approximation error. Soft computing techniques like genetic algorithms, fuzzy logic, neural network, and ant colony optimization can solve the problems with uncertainty. Performance of localization algorithms depends on factors like number of anchor nodes, node density, computation overhead, accuracy of localization, etc. Each algorithm has its own merits and demerits, making them suitable for different applications. Localization algorithms in WSN are either centralized or distributed. Centralized algorithms are suitable for applications requiring accuracy as they provide more accurate locations. On contrary, distributed algorithms do not rely on large centralized system and potentially support better scalability, making them suitable for agricultural application. As they have low communication cost, sensors life can be extended also.

Typical research challenges in localization include localization in ambient and noisy condition (e.g., humidity, interference), providing security during localization, localization in mobile wireless sensor network (MWSN) [14], and localization in three dimensional space.

Successful application of WSN in large area depends on QoS of underlying WSN. Improving QoS of the underlying network is possible in terms of security and accuracy of localization. The proposed QoS-aware localization methods are based on fuzzy logic and information theory.

This chapter consists of three sections. Section 5.1 presents a localization method using fuzzy logic to cope up with uncertainty. In order to address the limitations of single parameter fuzzy logic, a multi-parameter fuzzy logic-based localization is proposed in Section 5.2. The chapter is summarized in Section 5.3.

5.1 FUZZY LOGIC-BASED RANGE-FREE LOCALIZATION FOR WSN IN AGRICULTURE

Rapid technological advances in low-cost, low-power and multifunctional sensor devices makes them useful in every area of life. Generally, deployed WSN are used to gather spatio-temporal characteristics of the physical world. They are being successfully used in environment monitoring, precision agriculture, patient monitoring, habitat monitoring, object tracking [1]. For instance, WSN used in agriculture [186] can monitor field characteristics like temperature, moisture, nutrients, etc. Location-dependent applications like object tracking needs to know the physical location of sensors. Determining the physical position of sensors in WSN is localization. Localization plays a major role in such WSN applications. Researchers have contributed much in the field of localization [201]. However, it remains a challenging task due to the limited capacity of tiny sensors like energy, computing power.

Although global positioning system (GPS) provides position information to sensors, but it is not feasible to be incorporated in every sensors in terms of cost, hardware and computational capacity requirements of GPS devices. Again, GPSs are not particularly suitable in hazardous environment like industrial plant monitoring and in indoor applications. Generally, in localization algorithms only a few nodes are enabled with GPS to assess the positions. These nodes are called anchor nodes. The problem of localization is to estimate locations of unknown nodes in WSN with the help of anchor nodes.

DV-Hop [57] is a popular range-free localization algorithm. It assumes that anchors closer to an unknown node can provide more accurate hop-count than a farther one. However, two anchors closely placed in a randomly distributed WSN consider other in calculating hop-count between them. So, a closest anchor not always offers better hop-count estimation than far away anchors with accurate hop-

count. Efforts have been made to modify DV-Hop algorithm to enhance accuracy of localization. In weighted DV-Hop [58], weights of anchors are used to enhance localization accuracy without additional hardware device. The weight of an anchor node is calculated based on minimal hop-count between an unknown node and an anchor node. In all DV-Hop variants [58], [59], weights are assigned to anchors such that more the hop-count the less is the weight of an anchor. However, this fact is not always correct. An anchor farther from an unknown node may give better estimation of hop-count possessing more weights than a closely placed anchor. Inaccurate hop-count results in inaccurate anchor weights. Hence, deciding weights of anchors with erroneous hop-count is a challenge in range-free localization. Uncertainty in deciding weights of anchors can introduce error in localization.

There are many localization algorithms in WSN. The existing localization algorithms can be classified as range-based and range-free. Range-based algorithms estimate locations of sensors based on range measurements like distance [202] or angle [54]. Although range-based localization technique provides accurate location information, they require additional costly hardware for range measurements. Range-free algorithms do not rely on absolute range information, hence do not require additional hardware [203], [64]. Range-free localization algorithms are widely used in large-scale WSN applications like precision agriculture to avail economic benefit over the others.

In this section, a fuzzy-based weighted DV-Hop (called, FWDV-Hop) algorithm is proposed. In this algorithm, location accuracy is enhanced dealing with uncertainty in anchor weights. Here, weights are estimated based on hop-count through fuzzy logic [190].

The remainder of this section is organized as follows. In section 5.1.1, an overview of DV-Hop algorithm is presented. The proposed FWDV-Hop algorithm is presented in Section 5.1.2 followed by simulation result and analysis are presented in Section 5.1.3.

5.1.1 PRINCIPLE OF DV-HOP ALGORTHM

The DV-Hop algorithm works in two phases. In the first phase, each anchor node broadcasts a beacon message providing its position information along with an initial hop count of one. Each receiving node maintains a minimum hop-count per anchor for all beacons. Beacons with higher hop-count values (called, stale information) from anchors are simply discarded. Non-stale beacons are flooded outward after incrementing hop-count at every intermediate hop until all the shortest paths are found. This is how all nodes including the anchors know the shortest path distance to all anchor nodes in terms of minimum hop-count information.

In the second phase, each anchor node calculates its average hop-size (in terms of one hop distance) using the minimum hop-count to other anchors. The average hop-size of *i*-th anchor is calculated as:

$$Hopsize_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{j \neq i} h_{ij}} \tag{5.1}$$

where $(x_i, y_i), (x_j, y_j)$ are the co-ordinates of anchors i and j and h_{ij} denotes the minimum hop-count between them. After calculating average hop-size, an anchor node broadcasts that value throughout the network. Once an unknown node receives hop-size, it finds the distance to the beacon node using hop-count and hop-size using eqn. (5.2).

$$d_{ij} = Hopsize_i * h_{ij}. \tag{5.2}$$

where d_{ij} is the distance between nodes *i* and *j*.

In the last step, an unknown node, P estimates its position, $X = (x, y)$ using position of n number of anchor nodes and the distance, $d_i, i = 1,2,..n,$ to P as follows:

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = {d_1}^2 \\ (x - x_2)^2 + (y - y_2)^2 = {d_2}^2 \\ \quad\quad\quad . \quad\quad\quad . \\ \quad\quad\quad . \\ (x - x_n)^2 + (y - y_n)^2 = {d_n}^2 \end{cases} \tag{5.3}$$

Now, eqn. (5.3) can be expanded as:

$$\begin{cases} 2(x_1 - x_n)x + 2(y_1 - y_n)y = {x_1}^2 - {x_n}^2 + {y_1}^2 - {y_n}^2 - {d_1}^2 + {d_n}^2 \\ 2(x_2 - x_n)x + 2(y_2 - y_n)y = {x_2}^2 - {x_n}^2 + {y_2}^2 - {y_n}^2 - {d_2}^2 + {d_n}^2 \\ \quad\quad\quad\quad\quad\quad\quad . \quad\quad\quad\quad\quad\quad\quad . \\ \quad\quad\quad\quad\quad\quad\quad . \\ 2(x_{n-1} - x_n)x + 2(y_{n-1} - y_n)y = {x_{n-1}}^2 - {x_n}^2 + {y_{n-1}}^2 - {y_n}^2 - {d_{n-1}}^2 + {d_n}^2 \end{cases} \tag{5.4}$$

Now, eqn. (5.4) can be represented by linear system as $AX = B$, where,

$$A = -2 \times \begin{bmatrix} x_1 - x_n & y_1 - y_n \\ x_2 - x_n & y_2 - y_n \\ \quad\quad . & \quad\quad . \\ \quad\quad . & \quad\quad . \\ x_{n-1} - x_n & y_{n-1} - y_n \end{bmatrix},$$

$$B = \begin{bmatrix} {d_1}^2 - {d_n}^2 - {x_1}^2 + {x_n}^2 - {y_1}^2 + {y_n}^2 \\ {d_2}^2 - {d_n}^2 - {x_2}^2 + {x_n}^2 - {y_2}^2 + {y_n}^2 \\ \quad\quad\quad . \\ \quad\quad\quad . \\ {d_{n-1}}^2 - {d_n}^2 - {x_{n-1}}^2 + {x_n}^2 - {y_{n-1}}^2 + {y_n}^2 \end{bmatrix}, \text{ and}$$

$$X = \begin{bmatrix} x \\ y \end{bmatrix}$$

Hence, X can be calculated as:

$$X = (A^T A)^{-1} A^T B \,. \tag{5.5}$$

Evaluation of localization method is done through root mean square error (RMSE). The RMS error is calculated as in eqn. (5.6),

$$e = \frac{1}{n-1} \sum_{i=1}^{n} \sqrt{(x - x_i)^2 + (y - y_i)^2} \,. \tag{5.6}$$

where $(x, y)$and (x_i, y_i) are the actual and estimated co-ordinates of node i respectively.

5.1.2 PROPOSED FUZZY-BASED WEIGHTED DV-HOP (FWDV-HOP) ALGORTIHM

This section gives an overview of fuzzy-based weighted DV-Hop (FWDV-Hop) algorithm. In DV-Hop, an unknown node estimates its location using least square method as in eqn. (5.3). Weights are assigned to anchors to impose the relative importance over other anchors. Weights calculated directly based on inaccurate/noisy hop-count provides inaccurate average hop-size which decreases accuracy of localization. In proposed FWDV-Hop, we assign weights of anchors using fuzzy logic. This approach can provide appropriate weight assignment so as to localize nodes dealing with uncertainty in hop-count. This algorithm follows DV-Hop except the weight calculation for anchors through fuzzy inference system (FIS). The fuzzy input hop-count is fed to FIS as shown in Fig. 5.1 and mapped to weight via inference engine using fuzzy rules. The membership function of fuzzy variables hop-count and weight is divided into five triangular membership functions such as very low (VL), low (L), moderate (M), high (H), and very high (VH) as shown in Fig. 5.2. The fuzzy rule base of FIS consists of five fuzzy rules corresponding to five membership functions. A fuzzy rule is defined with hop-count as antecedent while weight as consequent. For example, whenever hop-count is very low, weight of node is very high. On contrary, whenever hop-count is very high, weight is very low.

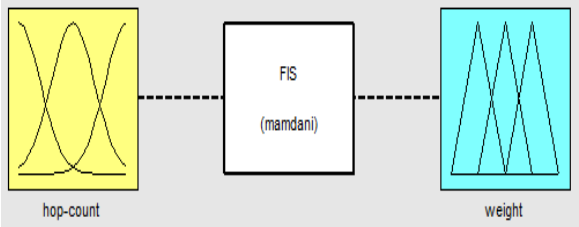


Fig. 5.1. Fuzzy model for proposed algorithm with hop-count as input and weight as output

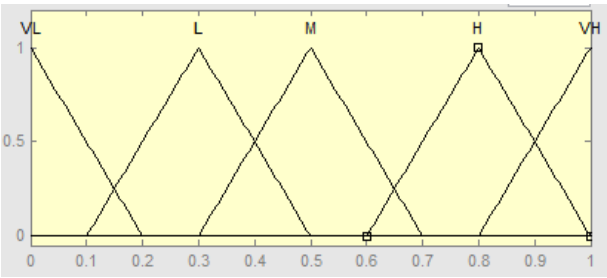


Fig. 5.2. Membership functions for input/output variable

5.1.3 SIMULATION RESULTS AND ANALYSIS

Matlab R2013a is used for simulation. A WSN is created with randomly deployed sensors and anchors over an area of 50x50 m^2. All nodes are assumed to have 2J initial energy and 15m of communication radius. Number of nodes is varied from 100 to 500 while radio communication radius of each sensor is changed from 10m to 20m. We plot the localization error with varying anchor nodes to sensor node ratio from 5% to 40% is plotted. In the same Matlab R2013a environment other algorithms like DV-Hop, HWDV-Hop, IWDV-Hop are also evaluated. Performance of proposed algorithm is measured through normalized localization error (RMSE) using eqn. (5.6) as the average deviation of estimated location to actual location of all unknown nodes. The simulation results are used to plot localization error by varying number of nodes, communication radius, and ratio of anchor nodes to unknown nodes. Proposed algorithm is compared with other algorithms in Fig. 5.3 through Fig. 5.5.

Fig. 5.3 depicts localization error with respect to total number of sensor nodes, with 10% of anchor nodes. It is observed that localization error decreases as number of increases. The error become steady when number of sensors increases to 300 and more. With same number of nodes and 10% of anchors, proposed algorithm outperforms others as the weights are fixed with fuzzy logic.

In Fig. 5.4, localization error is plotted with varying anchor nodes from 5% to 40% of total nodes in the network. The more the anchor ratio the less is the localization error. By dealing uncertainties through fuzzy logic, the proposed algorithm gives better localization accuracy than others.

In Fig. 5.5, localization error is depicted with respect to communication radius of sensors varying from 10m to 20m. Here, 100 nodes are randomly deployed with 20% of anchor nodes in order to evaluate the algorithms. With increasing radius of sensors, localization accuracy improves. Again, proposed algorithm outperforms others in terms of localization accuracy due to appropriate fixing of anchor weights in location estimation.

In this section, fuzzy logic is used to find weights of anchors based on a single parameter: hop-count. However, weights of anchors depend on other factors like residual energy and node density. So, a multi-parameter localization method using fuzzy logic is introduced in the next section.

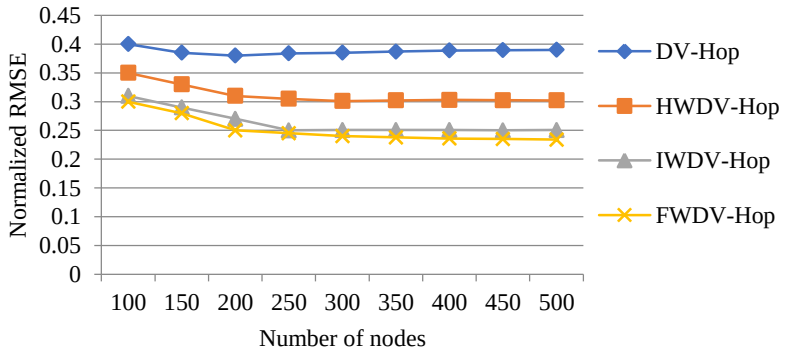


Fig. 5.3. Normalized localization error vs. number of sensor nodes, with 10% of anchor nodes

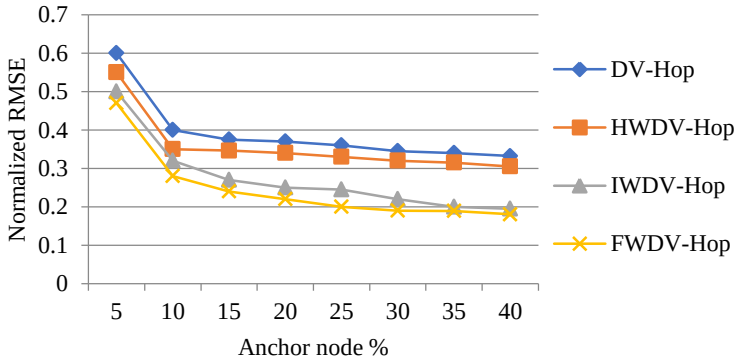


Fig. 5.4. Normalized localization error vs. anchor nodes ratio (in percentage of anchor nodes) with 100 sensor nodes

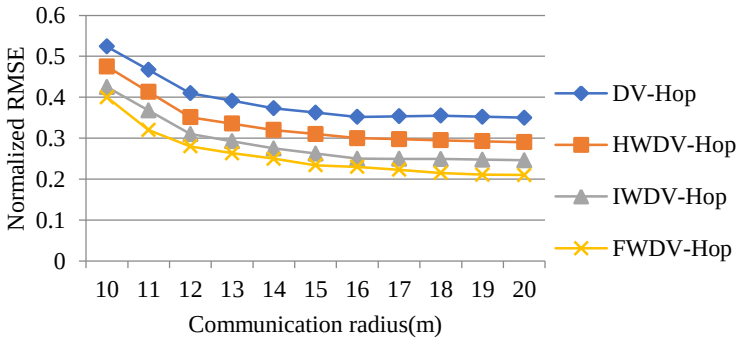


Fig. 5.5. Normalized localization error vs. radio range of sensors, with 100 sensors and 10% of anchor nodes

5.2 MULTI-PARAMETER RANGE-FREE LOCALIZATION FOR WSN USING FUZZY LOGIC

Due to the availability of low cost tiny sensors, they are being used in every sector of society. Generally, sensors are used to collect information parameters like sound from an unattended environment like military surveillance area. In order to gather information over a wide area, large numbers of sensors have to be deployed over the application area. Allowing them to communicate each other so as to forward sensed data via other sensors to a central location, forms a WSN. The authors in [186] have proposed a smart agricultural model using WSN to collect soil parameters like moisture so as to assist farmers in taking timely decision. Location-dependant application like smart precision agriculture initiates irrigation to the dried up crop area once the location is known. Without knowing locations of sensors, water may be wasted or the soil may become more moist, thereby increasing cost of cultivation. Such an application saves natural resources like water. The method of estimating locations of sensors in WSN is called localization [201]. Location-aware applications come to know locations of data with the help of localization. WSN used in military surveillance must have accurate localization capability to monitor enemy movement. Localization methods must be efficient in terms of computational complexity as sensors have limited energy.

Attaching global positioning system (GPS) for the purpose of locating sensors is not possible as they incur cost. Generally, a few sensors are attached with GPS making them location-aware, called anchors. Rest of the sensors in WSN adopts techniques to find their locations using locations of anchors.

In a densely deployed WSN, hop-count values are not always accurate as one anchor may count another nearby anchor. Fuzzy logic has been used to resolve ambiguity in hop-count values. As the nodes in WSN are randomly deployed, hop-count does not always reflect the actual physical distance. Inaccurate hop-count may result in inaccurate weight of anchor. In this circumstance, fuzzy logic may be used to calculate anchor weights dealing with uncertainties in hop-count. In FWDV-Hop [204], as described in Section 5.1, erroneous hop-count has been mapped to anchor weights using fuzzy logic. This algorithm only considers hop-count in weight calculation. However, selecting an anchor in localization not only depends on hop-count but also on other factors like residual energy and node density surrounding the anchor. An anchor with more residual energy and node density surrounding the anchor may provide accurate location information to an unknown node. In other words, two anchors with same hop-count to an unknown node with different residual energy and node density may have different weights. The anchor with more residual energy and node density may be preferred over the other in unknown location estimation. Motivated by the discussion, a fuzzy model named, NFWDV-Hop is developed for selecting weights based on the above mentioned three factors.

The remainder of this section is organized as follows. Section 5.2.1 presents existing literature related to modifications to DV-Hop algorithm. The proposed fuzzy model for calculating anchor weights is given in Section 5.2.2. Simulation results along with analysis can be found in Section 5.2.3.

5.2.1 ADDITIONS TO DV-HOP ALGORITHM

Guadane et al. [58] suggest weight of an anchor to be calculated as :

$$w_i = \frac{1}{h_{ij}}. \tag{5.7}$$

Here, h_{ij} is the hop-count between node i and j. w_i's are inaccurate if hop-counts are inaccurate. Weighted DV-Hop algorithm follows least square method using calculated weights in eqn. (5.8):

$$f(x,y) = min \sum_{i=1}^{n} {w_i}^2 (\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} - d_i)^2 . \tag{5.8}$$

where *n* is number of nodes.

Eqn. (5.8) may be formed as $\boldsymbol{A'X = B'}$, where

$$A' = -2 \times \begin{bmatrix} {w_1}^2{w_n}^2(x_1 - x_n) & {w_1}^2{w_n}^2(y_1 - y_n)_1 \\ {w_2}^2{w_n}^2(x_2 - x_n) & {w_2}^2{w_n}^2(y_2 - y_n) \\ . & . \\ . & . \\ {w_{n-1}}^2{w_n}^2(x_{n-1} - x_n) & {w_{n-1}}^2{w_n}^2(y_{n-1} - y_n) \end{bmatrix}, \text{ and}$$

$$B' = \begin{bmatrix} {w_1}^2{w_n}^2({d_1}^2 - {d_n}^2 - {x_1}^2 + {x_n}^2 - {y_1}^2 + {y_n}^2) \\ {w_2}^2{w_n}^2({d_2}^2 - {d_n}^2 - {x_2}^2 + {x_n}^2 - {y_2}^2 + {y_n}^2) \\ . \\ . \\ {w_{n-1}}^2{w_n}^2({d_{n-1}}^2 - {d_n}^2 - {x_{n-1}}^2 + {x_n}^2 - {y_{n-1}}^2 + {y_n}^2) \end{bmatrix}$$

So, location of P is calculated as below:

$$X = (A'^T A')^{-1} A'^T B' . \tag{5.9}$$

In [58], weights are estimated using eqn. (5.10). This algorithm not only prefers a closer anchor but also an anchor with correct hop-count.

$$w_i = \frac{\frac{1}{h_{ij}}}{\sum_{k=1}^{n} \frac{1}{h_{kj}}} \quad , k \neq j \, . \tag{5.10}$$

Localization error for the position of node i is calculated by eqn. (5.6).

In HWDV-hop [59], a node finds hop-size using one-hop distances to all anchors. This algorithm minimizes localization error.

In FWDV-Hop [204], weights are allocated based on hop-count. Uncertainty in hop-count is managed by fuzzy logic. The fuzzy logic model takes a single input hop-count and generates weight as output. Triangular memberships are used to map inputs to outputs. Although the algorithm provides near-accurate localization, however, it ignores other influencing parameters like residual energy and node density of anchor node, in assigning weight.

5.2.2 OVERVIEW OF THE PROPOSED ALGORITHM

In this section, we outline the overview of the fuzzy model. The fuzzy inputs hop-count, residual energy, and node density are applied to FIS and the system returns weight as output as shown in Fig. 5.6. Here, hop-count represents the number of hops in the shortest path from unknown node to anchor, residual energy is the energy of a sensor node at that time instant, and the node density signifies the number of nodes surrounding an anchor. For simplicity, all fuzzy input and output variables are represented by the same triangular membership function given in Fig. 5.7. The fuzzy variables possess five membership values: very low (VL), low (L), moderate (M), high (H), and very high (VH). Anchors with lower hop-count, higher residual energy as well as higher node density provide more accurate location information to an unknown node. Accordingly, input and output variables are related as follows. An anchor with higher hop-count is assigned lower weight. The higher the residual energy the more is weight. Similarly, the more the node density around an anchor the more is its weight. The rule base of FIS consists of 27 fuzzy rules corresponding to the 27 combinations of three inputs. Each rule is defined as if antecedent then consequent. For example, whenever hop-count is low, residual energy is high, and node density is medium, then the weight of an anchor node is high.

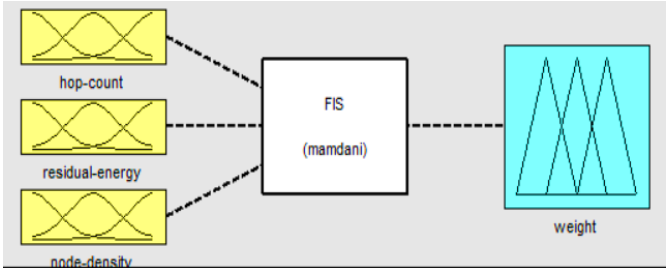


Fig. 5.6. Fuzzy logic model built with inputs to calculate weight

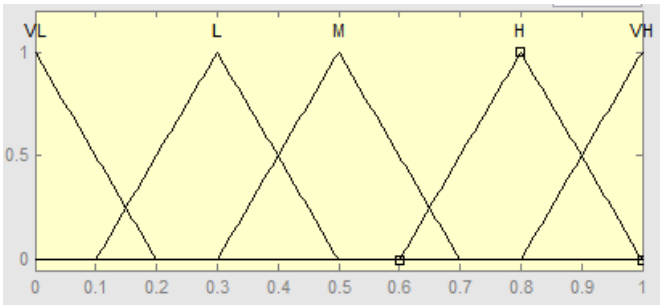


Fig. 5.7. Membership functions for input/output variable

5.2.3 SIMULATION RESULTS AND ANALYSIS

Matlab R2013a is used for simulation of the proposed algorithm, NFWDV-Hop. We consider a WSN with randomly deployed sensors in an area of 50x50 m^2. All nodes are set with an initial energy of 2J and communication radius of 15m. Localization error in terms of RMSE is estimated with nodes in the range 100 to 500 and communication radius of nodes within 10m to 20m. Localization error is plotted after changing anchor to sensor node ratio from 5% to 40%. Other algorithms are also executed in the same simulation platform and parameters. The proposed algorithm is compared with other algorithms, HWDV-Hop, IWDV-Hop, FWDV-Hop, in Fig. 5.8 through Fig. 5.10.

In Fig. 5.8, localization error is shown with varying number of sensor nodes of which 10% nodes are anchors. The more the nodes the less is the localization error. There is no significant change in error as soon as number of nodes reaches to 250. With 10% of anchors, proposed algorithm provides more accurate localization than other algorithms because of ability to deal with hop-count ambiguity in randomly deployed WSN. The error of NFWDV-Hop reaches to 20% with 500 nodes as weights are calculated using fuzzy logic, whereas the error of FWDV-Hop is 24%. More precisely, NFWDV-Hop has normalized error of 0.20, FWDV-Hop has normalized error of 0.24, IWDV-Hop has normalized error of 0.26, and HWDV-Hop has normalized error 0.29.

Number of anchors deployed in WSN influences localization error. Localization error is illustrated in Fig. 5.9 with varying anchor nodes from 5% to 40%. Localization error decreases with increase of anchor ratio. Fuzzy logic can represent imprecise hop-count and estimates weight. That is why the proposed approach provides more localization accuracy compared to others.

With increased communication radius, sensors can communicate with more neighbors. The effect of communication radius on localization error is given in Fig. 5.10. It reveals that error decreases with increased radius. In simulation, 100 nodes of which 20% are anchor nodes are considered for experiment. Simulation with a communication radius of 12m, the RMSE value of proposed algorithm remains at around 0.24 but the RMSE value of FWDV-Hop is 0.28, the RMSE value of IWDV-Hop is 0.31, the RMSE value of HWDV-Hop is 0.35. Again, simulation with a communication radius of 16m, the RMSE value of proposed algorithm remains at around 0.21 but the RMSE value of FWDV-

Hop is 0.23, the RMSE value of IWDV-Hop is 0.25, the RMSE value of HWDV-Hop is 0.3. The RMSE value approaches to nearly 20% with a communication radius of 20m. As anchor weights are calculated using fuzzy logic, the present approach outperforms others in terms of RMSE.

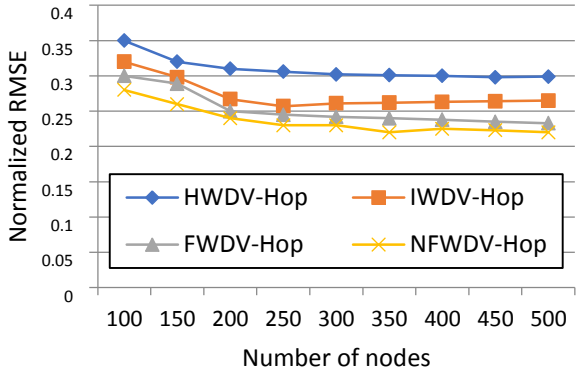


Fig. 5.8. Normalized localization error vs. number of sensor nodes, with 10% of anchor nodes

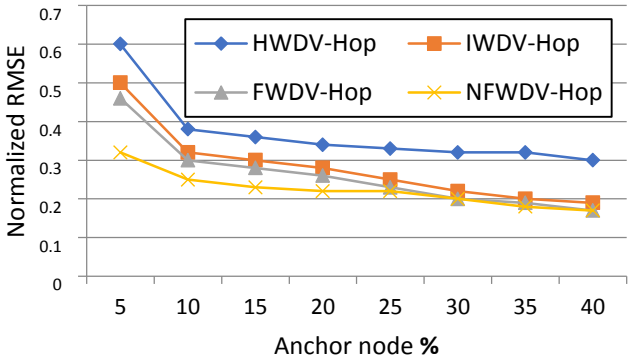


Fig. 5.9. Normalized localization error vs. anchor nodes ratio (in percentage of anchor nodes) with 100 sensor nodes

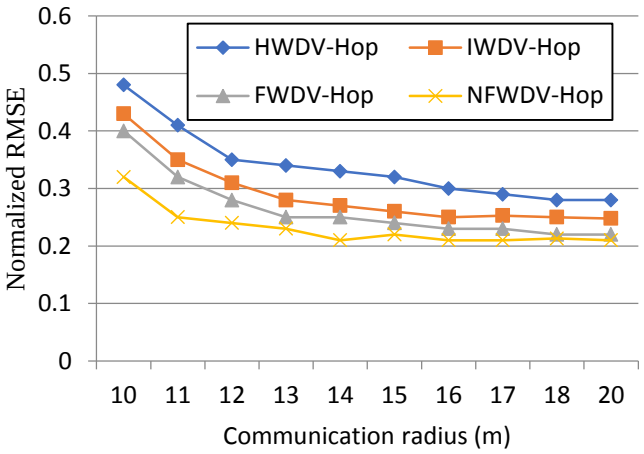


Fig. 5.10. Normalized localization error vs. radio range of sensors, with 100 sensors and 10% of anchor nodes

In this section, a multi-parameter localization method using fuzzy logic is proposed for WSN. However, underlying WSN may face attacks like sybil attack. Anchor nodes once compromised, might give inaccurate location information. So, a secure localization method using information entropy is presented in the next section.

5.3 CHAPTER SUMMARY

Localization is essential for location-dependent application of WSN like smart precision agricultural. Range-free localization becomes popular because of its lack of additional hardware requirements. In this chapter, a range-free localization method is presented using fuzzy logic. In weighted DV-Hop algorithm, weights are calculated as the inverse of hop-count. With closely placed anchor nodes in randomly distributed sensor network, hop-count estimation is not correct, so weights are affected. In this chapter, fuzzy logic is utilized to find weights of anchors based on erroneous hop-count. Again, a multi-parameter localization is proposed to improve accuracy of location estimation using fuzzy logic. Localization error is calculated for algorithms with varying number of sensors, anchors, and communication radius of sensors. Simulation results reveal that proposed algorithm improves others in terms of localization accuracy.

Nodes in WSN are vulnerable to different attacks as they are not generally reachable after deployment. If sensors are not protected against attacks, localization may be hampered. For example, localization with the fake beacon information communicated by compromised anchor nodes may result in erroneous location estimation. In the next chapter, an effort is made towards securing localization even in adversary attack.

CHAPTER SIX

AN INFORMATION THEORETIC APPROACH TO SECURE LOCALIZATION

Sensors are distributed in nature and mostly used in unknown and probably hostile environment which makes sensors vulnerable to attacks by adversaries. An adversary may affect localization process by impersonating the identities of sensor nodes. As a result, location-aware applications may no longer be useful to the beneficiaries. Lack of security in location-aware applications like forest fire detection may result in estimating incorrect locations which may incur immense losses. Such a security breach may degrade the Quality-of-Service (QoS) of underlying WSN too. Though there are plenty of localization methods available in literature, little research has been done on securing localization against attacks. In a hostile WSN environment, an adversary may compromise one node to forge one or multiple fake identities of it or other nodes at a given time; we say all identities of the compromised node are sybil nodes [205]. *Sybil attack* is a severe attack in WSN since it can be easily deployed in the WSN and diminishes localization accuracy or even collapse the localization system. Moreover, compromising anchor nodes have fatal influence on localization as localization accuracy mostly relies on anchor positions.

The objective in this work is to consider the detection of sybil attack. The first and foremost thing in securing localization is to ensure that the anchor nodes are reliable. In WSN localization, an anchor is treated unreliable (i.e., sybil anchor) if it is compromised by an adversary to forge sybil nodes. Hence, sybil attack detection attracts significant research in WSN localization. As sybil identities are generated from a single geographical position, the beacon packets travel the same distance to reach an unknown node. Consequently, all sybil attacked anchor nodes have the same Received Signal

Strength Indicator (RSSI) values measured at that unknown node. RSSI-based scheme like SF-APIT [89] detects sybil attack relying on RSSI values. However, RSSI values fluctuate in a hostile environment owing to various factors like physical obstacles, radio propagation problems like multi-path fading, shadowing [206]. As a result, sybil nodes may remain concealed.

Motivated by the limitation of RSSI-based schemes, a sybil anchor detection scheme utilizing information theory is proposed here. Due to problems like fading and shadowing RSSI values are considered as random variables. In this section, information theory concept is utilized in order to cope with randomness of RSSIs and identify sybil anchors in the network [207]. The scheme is applied on a well-known localization algorithm: APIT [64]. Simulation results reveal that localization using the proposed approach outperforms others in terms of location estimation error.

The rest of the chapter is organized as follows. Section 6.1 presents system model including network and attack model. In Section 6.2, sybil detection scheme using information theory is proposed while simulation results and analysis are given in Section 6.3. Finally, the chapter summary is given in Section 6.4

6.1 SYSTEM MODEL

This section describes the underlying network model and attack model that is considered in this work.

6.1.1 NETWORK MODEL

N number of sensor nodes with unknown locations and Q number of anchors with known locations are randomly deployed over an area A. Only the anchors are equipped with GPS and have larger communication ranges as well as higher energy. All other sensor nodes are unaware of their locations.

6.1.2 ATTACK MODEL

In a hostile WSN environment, an adversary may compromise one node to forge one or multiple fake identities of it or other nodes at a given time. All identities of the compromised node are called sybil nodes. Since anchor nodes play the most important role in localization, attack on anchor node is only looked into. In this chapter, sybil attacks on sensor nodes other than anchor nodes are ignored since localization accuracy depends heavily on positions of anchors. A sybil attack scenario is depicted in Fig. 6.1. A malicious anchor s_k forges three sybils pretending to be three separate nodes with different location information to an unknown node M. The three sybils s_m, s_n, and s_p with different virtual identities id_m, id_n and id_p have three different beacon packets (id_m, x_m, y_m), (id_n, x_n, y_n), and (id_p, x_p, y_p) respectively. Considering sybil information in localization, M calculates own location incorrectly.

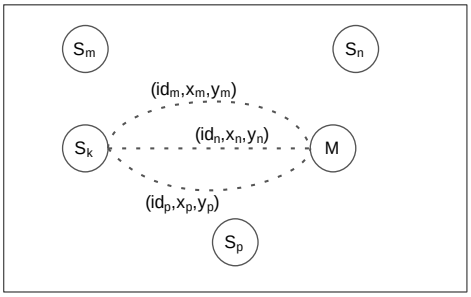


Fig. 6.1. A sybil attack scenario with three virtual identities of a malicious node

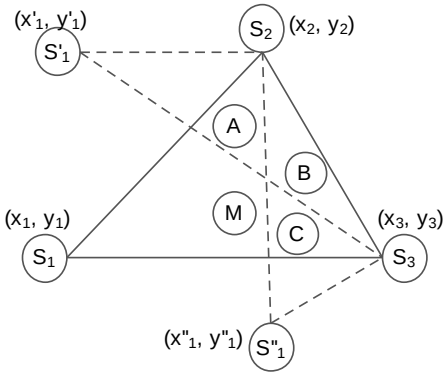


Fig. 6.2. Impact of sybil attack on localization

Fig. 6.2 illustrates impact of sybil attack on localization methods. $S_1, S_1,$ and S_3 denote three anchor nodes with locations $(x_1, y_1), (x_2, y_2),$ and (x_3, y_3) respectively. S_1 is compromised to generate two sybil nodes S'_1 and S''_1. $A, B, C,$ and M are sensor nodes of which M is an unknown node. Although M lies inside the triangle $\Delta S_1 S_2 S_3$, it neither lies inside the triangle $\Delta S'_1 S_2 S_3$ nor inside triangle $\Delta S''_1 S_2 S_3$ after sybil attack. Hence, localization using S'_1 and S''_1 gives erroneous location estimation of M by approximate point in triangulation (APIT) algorithm [64].

In APIT [64], location of an unknown node is calculated as the centre of gravity of overlapping triangles covering the unknown node. After receiving beacon messages, an unknown node selects three anchors so as to form a triangle covering itself. Presence of unknown node inside the triangle is ensured by point in triangle (PIT) test. Location is estimated as the intersection point of all triangles satisfying PIT test. However, APIT is simple to implement, it ignores sybil attack.

One sybil-free localization scheme based on APIT is proposed in SF-APIT [89]. SF-APIT algorithm uses RSSI values to perform detect sybil anchor nodes in localization. Like APIT algorithm, SF-APIT algorithm forms triangles with three anchor nodes and applies PIT test. Then, this algorithm checks if a pair of anchor nodes of a triangle is sybil attacked. An unknown node M detects

a pair of anchor nodes as sybil nodes if the difference between RSSI values measured at M lies above a predefined threshold error of RSSI readings. The threshold error of RSSI readings is calculated as the sum of mean RSSI error to an error tolerance value. Anchors detected as sybil are kept aside from participating in location estimation.

6.2 SECURE LOCALIZATION BASED ON INFORMATION THEORY

In this section, the characteristics of sybil attack are mentioned and an approach to detect sybil anchors using entropy correlation coefficient is described.

6.2.1 CHARACTER OF SYBIL ATTACKS

In sybil attacks, an anchor node is compromised (called malicious anchor)to generate multiple virtual identities as shown in Fig. 6.1. All virtual anchors pretend to be the same malicious anchor. As all virtual anchors are generated from the same physical place, they have equal distance to M but with different locations. Consequently, all sybil anchors have almost the same RSSI values as received at an unknown node M. In other words, we can say sybil anchors lie on the same circle centered at M. In Fig. 6.3, sybil attack character is illustrated with an example. The malicious anchor$s_k$generates three sybil anchors $s_m, s_n,$ and $s_p$and sends three different beacon packets to M. We assume that unknown node M lies in communication range of s_k.With equal RSS values received at M, all virtual anchors $s_m, s_n,$ and s_p lie on the same circle with M as centroid.

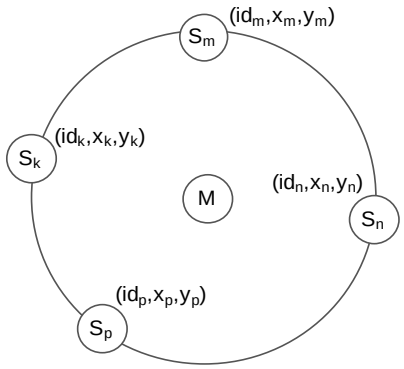


Fig. 6.3. Sybil attack character illustrating all sybil anchors lie on the same circle with M as centroid

6.2.2 INFORMATION-THEORETIC APPROACH

Let, an unknown node, Mwants to find its own position. On receiving beacon packets it estimates the corresponding RSSI values. As most of the sensors are capable of calculating RSSI without extra hardware, the technique does not incur extra cost. Direct use of RSSI in distance estimation is error prone due to multi-path fading of radio signal. Then it chooses three anchors having minimum RSSI values in order to form a minimum-area triangle enclosing M. But due to sybil attack, anchor nodes forming the triangle may not be reliable for localization. In this chapter, an information-theoretic approach is adopted to detect if a pair of anchors is sybil attacked. Once detected sybil anchors, they are discarded from forming a triangle. Triangle formation is continued with other anchors.

By the characteristics of sybil attack, all sybil nodes as well as the compromised anchor node lie in the same circle with the unknown node as the centre. As the beacon packets are generated from the same compromised anchor, they all travel the same distance to reach M. Hence, the RSSI values of all sybil nodes calculated by M are not different. As RSSI measurements are random owing to fading and shadowing [206], we can consider the RSSIs of anchors A and B measured at M as two random variables, X and Y (say) with the probability distributions $P(x)$ and $P(y)$ respectively.

In information theory, entropy of a random variable is the amount of uncertainty present in itself. The entropy $H(X)$ of the random variable X is given as:

$$H(X) = -\sum_{x \in X} P(x) \log P(x) \tag{6.1}$$

where x is the value of X and $P(x)$ is the probability that X be x.

Similarly, the entropy $H(Y)$ of the random variable Y is given as:

$$H(Y) = -\sum_{y \in Y} P(y) \log P(y) \tag{6.2}$$

where y is the value of Y and $P(y)$ is the probability that Y be y. For multi-random variables X and Y, the uncertainty is measured by their joint entropy $H(X,Y)$ and defined as:

$$H(X,Y) = -\sum_{x \in X} \sum_{y \in Y} P(x,y) \log P(x,y) \tag{6.3}$$

where $P(x,y)$ is the probability that x and y appear together.

Now, the individual entropy and joint entropy of two random variables X and Y follow the inequality:

$$H(X,Y) \leq H(X) + H(Y) \tag{6.4}$$

If X and $Y$are independent, their joint entropy is equal to the sum of the individual entropies. In such case, the RSSI values of anchors A and B measured at M are different. It signifies that X and Y are not sybil nodes. With dependency between X and Y, their joint entropy will be smaller than their total entropies. In this case, the RSSI values of anchor A and anchor B measured at M are equal. It signifies that anchor nodes A and B and are two sybil nodes, generated by the same compromised node. If two anchors A and B are sybil nodes and are forged by a single compromised anchor, they will have same RSSI values. We say two anchors are dependent if and only if they are sybil nodes and possess same RSSI values. The more likely that two RSSIs are equal, greater is their dependency. Again, the higher the dependency the more likely that they are sybil nodes.

Relationship between two random variables is also measured by the information metric: mutual information. It measures how much information is borne by one random variable about another. As stated earlier, two anchors A and B which are sybil attacked have the same RSSI values. The more similarity between the RSSI values of A and B, the more is their mutual information. The mutual information of X and Y is expressed as below:

$$I(X,Y) = -\sum_{x\in X}\sum_{y\in Y} P(x,y)\log\frac{P(x,y)}{P(x)P(y)} \tag{6.5}$$

where $P(x,y)$ is the joint distribution of $X$and Y. Again, in terms of entropy, $I(X,Y)$ can be defined as:

$$I(X,Y) = H(X) + H(Y) - H(X,Y) \tag{6.6}$$

In order to measure the strength of association between X and Y, normalized correlation coefficient, called entropy correlation coefficient defined as below is used:

$$\begin{aligned}\rho(X,Y) &= 2\frac{I(X,Y)}{H(X)+H(Y)} \\ &= 2 - 2\frac{H(X,Y)}{H(X)+H(y)}\end{aligned} \tag{6.7}$$

From eqn. (6.4), it is obvious that correlation coefficient ρ lies between 0 and 1. The correlation increases with increase in ρ. If X and Y are fully dependent on each other (in case of sybil attack), i.e., $H(X) = H(Y) = H(X,Y)$, then $\rho = 1$. In other words, $\rho = 1$ detects anchors A and B to be sybil nodes. On the other hand, if X and Y are independent (not sybil attacked), i.e., $H(X,Y) = H(X) + H(Y)$, then $\rho = 0$. It signifies that A and B are not sybil attacked as the corresponding RSSI values of X and Y have no correlation. In this chapter, we use ρ to decide if two anchors X and $Y$are sybil nodes.

Following this technique, there is a chance that a pair of reliable anchors may be treated as sybil nodes by two trustable nodes. This situation is illustrated in Fig. 6.4. Two anchors S_1 and S_2 are situated on the points where two circles centered at two nodes M and Q intersect each other. Here, Q is a trustable neighbour of unknown node M. The radius of one circle is the distance between M and S_1, while the radius of the other circle is the distance between Q and S_2 . Let, RSSI readings of S_1 and S_2 measured by any trustable node are X and Y respectively. In this situation, both M and Q calculate $\rho(X,Y) = 1$ by using eqn. (6.7) and treat S_1 and S_2 as sybil anchors, although they are not compromised. So, there is a misjudgement if two trustable nodes are used to verify sybil attack. Like the work in [89], to avoid misjudgement of anchor nodes as sybil nodes, the value of ρ is required to be verified by at least three trustable nodes as shown in Fig. 6.5. In Fig. 6.5, only S_2 lies on the intersection of three circles centered at sensor nodes M, Q, and R, but not S_1 . In this circumstances, the value of $\rho(X,Y)$ calculated by R is different from the values of $\rho(X,Y)$ calculated by M and Q. So, S_1 and S_2 are not considered as sybil anchor nodes after verification of $\rho(X,Y)$ by third node R. If a pair of anchors is detected sybil by at least three trustable nodes, then the pair is discarded by the unknown node M for location calculation.

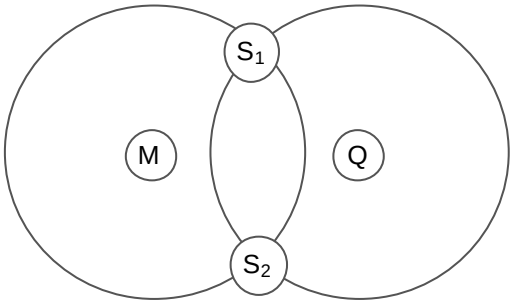


Fig. 6.4. An example showing incorrect judgment of anchors S_1 and S_1 as sybil nodes by two trustable nodes *M* and *Q*

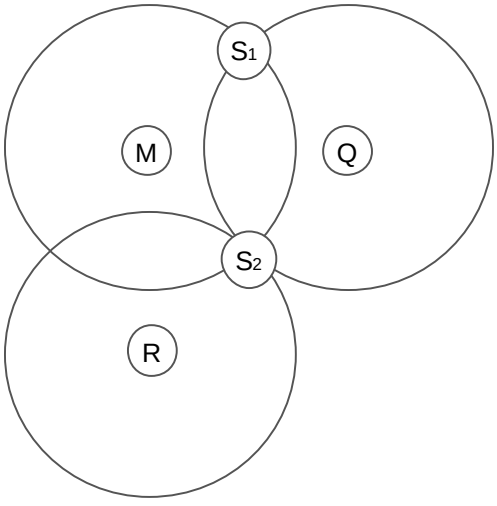


Fig. 6.5. Sybil detection with the help of three trustable nodes to defend incorrect judgment

6.3 SIMULATION AND RESULT ANALYSIS

For the simulation of the proposed scheme, the same parameter setting as used in the work [89] is considered with a network of size $300\text{m} \times 300\text{m}$. Here, sensors and anchors are randomly deployed over the network with communication range 60m and 120m, respectively. The ratio of sensor to anchor node is varied from 1 to 10. The simulation is run for 40 times in Matlab R2013a. Performance of the proposed approach is evaluated in terms of two metrics: sybil detection rate and localization estimation error.

Fig. 6.6 depicts sybil detection rate for different number of legitimate nodes following the present approach. This figure reveals that detection rate of sybil attack increases with increasing number of legitimate nodes. The reason is that, the higher the number of trustable nodes around an unknown node, the lesser is the chance of misjudgement, as illustrated in Fig. 6.5. The detection accuracy increases if it is verified by more number of neighbor nodes around an unknown node. This approach provides higher sybil detection rate of more than 95% with 30 legitimate nodes since it can manage uncertainties in RSSI values in hostile environment using the concept of entropy.

In order to evaluate performance of this approach, localization using both SF-APIT and the current approach under the same simulation environment as mentioned in this section is simulated. After calculating localization errors, they are normalized to radio range (R) of sensors. A comparison of two approaches in terms of normalized location estimation error is depicted in Fig. 6.7. It is obvious that localization is affected by sybil attack and significant error is introduced in localization with sybil attack in both approaches. In a hostile environment, sybil attack sneak through the detection process of SF-APIT scheme as RSSI measurements tend to be error prone. Localization error in a hostile WSN environment with sybil attack is further minimized in the current approach as it provides higher sybil detection rate. We can achieve normalized localization error of 0.35R as compared to an error of 0.48R of SF-APIT. Hence, it is evident that the present approach is capable of estimating node positions with minimum localization error in a hostile environment.

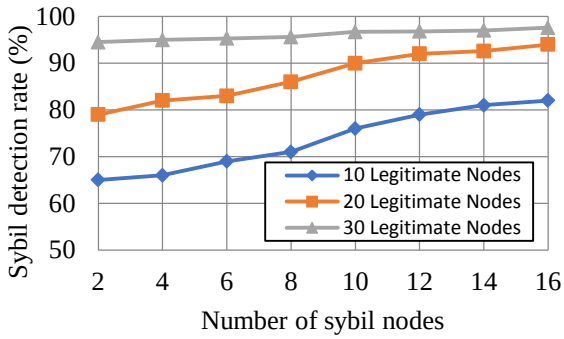


Fig. 6.6. Sybil detection rate with different number of sybil nodes following proposed approach

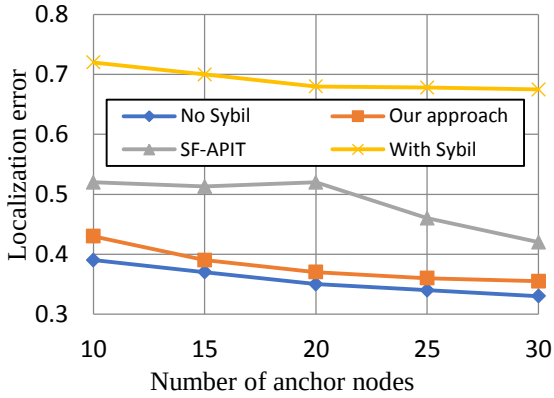


Fig. 6.7. Normalized localization error with different number of anchor nodes

6.4 CHAPTER SUMMARY

Sybil attack in a WSN can hamper localization accuracy or even damage the localization system. A location-aware application without security against sybil attack can cause devastation too. Though RSSI-based approach like SF-APIT algorithm tries to defend against sybil attack, it relies directly on RSSI values which are influenced by factors like radio communication errors. As a result, sybil attack may sneak through the sybil detection process. In this chapter, an effort is made to fight against sybil attack based on the concept of information entropy after dealing with uncertainties in RSSI values. The simulation results claim that the present approach can successfully detect sybil attack and increase localization accuracy in spite of sybil attack.

CHAPTER SEVEN

CONCLUSION AND FUTURE PROSPECTS

Now-a-days, IoT has become an indispensible part of our life. Novel applications like smart precision agriculture, livestock management, ambient assisted living, etc. are developed using IoT. Wireless sensor network can be incorporated with IoT to meet the seamless communication among sensors and things. In such IoT-based applications, WSN acts as backbone. However, WSN possesses few limitations like energy and computational power. Sensors are generally battery powered and the batteries are not replaced once deployed. So, operations in WSN like clustering, localization must be energy-aware. Again, due to inherent openness of IoT, nodes are vulnerable to many network attacks. Location-based WSN applications must be secured against such attacks. Inaccurate location estimation resulting from network attack may cause devastation too.

This thesis proposes energy efficient and localization-aware approaches for IoT and WSN based framework for precision agriculture. The proposed framework aims at optimizing various resources (water, fertilizers, insecticides and manual labour) for precision agriculture through the use of IoT and WSN. Literature survey reveals limitations and challenges while implementing the proposed framework. For successful implementation of the framework, underlying WSN must be energy efficient and location-aware. Energy efficient WSN clustering approaches can extend network lifetime by balancing energy dissipation among nodes. On the other hand, localization methods provide precise and accurate location estimation of sensors even in network attack. Thus, combining location-aware sensor nodes with energy efficient clustering in WSN will contribute to an effective IoT-based application in precision agriculture.

This work has two primary objectives, i.e., developing energy efficient balanced clustering to extend lifetime of WSN and devising secure localization schemes to deal with attacks in sensor

networks which are mentioned in Chapter 1. This chapter also presents an overview WSN including its applications and limitations, followed by motivation and contributions of the work.

Chapter 2 includes literature survey related to clustering and localization in WSN. Security related WSN works are also investigated in this chapter. Based on the survey, this work proposes energy efficient clustering and routing protocols, followed by secure localization for precision agriculture.

Chapter 3 proposes a framework, AgriTech for IoT and WSN based application in precision agriculture monitoring. As the proposed framework is IoT-enabled, an exhaustive survey on IoT is carried out initially. The survey includes layered architecture, underlying technologies including sensing, identification, and communication are presented in this chapter. State-of-the-art of middleware technology, standardization activities and related projects in IoT are also summarized here. Due to inherent openness, security and privacy remain challenge in IoT. Design of lightweight security methods can secure IoT. Research towards addressing the challenges can help achieving better future IoT.

Finally, this chapter presents a framework based on IoT and WSN for precision agriculture. The framework consists of four layers: the objects, the local gateway, the Internet, and the data cloud. The AgriTech is beneficial to countries dependant primarily on agriculture. The farmers can monitor crop field without physically reaching there. This framework not only minimizes wastage of natural resource like water, but also finds the global market to trade crops. The suitability of the framework is validated with data.

Chapter 4 presents an optimized fuzzy clustering algorithm to forward data to sink in energy efficient way. In optimized fuzzy clustering algorithm, cluster heads are elected based on residual energy, distance from sink, and concentration of nodes using fuzzy logic. At the same time, communication radii of cluster heads are calculated based on distance from sink so as to promote unequal clustering. In order to route data to sink an energy efficient routing path via other cluster heads is determined by particle swarm optimization. The fitness function is defined so as to prolong the network lifetime keeping in mind wide application of WSN. Simulation results reveal that proposed algorithm attains longer lifetime and is able to forward more messages to sink in energy efficient route.

This chapter also proposes an adaptive cross layer protocol with energy harvesting sensors. Recently, sensors are capable of charging their batteries from many ambient sources like vibration. An effort is made to trade off between energy harvesting time and active time for message transmission. During charging sensors are not involved in sensing or communicating, resulting diminishing of sensor efficiency. Trade-off between energy conservation and efficiency is one of the most important issues in designing WSN based applications. Network lifetime is primarily determined by the lifetime of battery. Depending on the value of various network parameters like, remaining

energy of node, node density, message density in a particular region of the network, the cross-layer protocol changes its policy. The chapter also proposes a cluster head election method that ensures maximum network life time and higher quality of service. The result shows an overall increase in network lifetime as compared to other protocols.

Chapter 5 provides range-free localization methods along with a secure localization. Especially in agricultural monitoring, precise location of the affected crop is required for effective use of fertilizers or pesticides. Low-cost and accurate localization algorithms are proposed for such applications with WSN. Localization techniques based on distance vector calculate hop distance based on hop count. However, hop counts are not always accurate in densely deployed network and do not always reflect relative influence of beacons in location estimation. Fuzzy logic is used to calculate weight of anchors based on hop count. Furthermore, many factors like residual energy have influence on anchor selection. So, a multi-parameter localization using fuzzy logic is also presented which assigns weights of anchors depending on hop count, remaining energy, and node density. Uncertainty in anchor selection is better handled by fuzzy logic which is proved by simulation results.

As sensor nodes are incorporated in IoT, they are vulnerable to many network attacks. In sybil attack, an anchor generates many virtual identities with different locations. As a result, location estimation by an unknown node with location information from compromised anchors is erroneous. In order to secure localization in sensor network against sybil attack, information entropy concept is utilized to identify compromised anchors in Chapter 6. As all virtual identities are generated by the same sybil anchor, RSSI values of all virtual nodes are same. By applying information entropy, sybil anchors are identified. Once anchors are detected compromised, they are kept away from participating in location estimation. So, this approach can provide accurate location estimation even in sybil attack.

As mentioned in Chapter 3, this thesis proposes a framework for smart precision agriculture using IoT and WSN. The work includes an exhaustive survey on IoT including architecture, enabling technologies, applications, challenges, and middleware technology. This survey is beneficial to all the layers of the proposed framework. The focus of the work in the present thesis is primarily on *Layer 1* (things layer) forming wireless sensor network. Hence, energy efficient and location-aware approaches are developed for wireless sensor network. The energy efficient clustering and adaptive cross-layer routing with energy harvesting concept can be applied in *Layer 1* (things layer) of the framework. This will help in extending lifetime of sensors deployed in agricultural field. Knowing the precise location of affected crop area is possible by employing proposed range-free localization methods. Also, this thesis defends attacks in localization by developing a secure localization technique using information theory. The location-aware approaches can be adopted in *Layer 1* of the framework.

Future Prospects: This thesis presents a novel framework of IoT-based application of WSN. The underlying network is energy efficient and location-aware for successful implementation the framework. However, many further research works may be carried on it. A few are as follows:

i. Addressing other QoS parameters of WSNs such as reliability, packet delivery ratio, and end to end delay in application.
ii. Providing lightweight security to sensed data communicated within the framework.
iii. Studying effect of mobility of cluster heads and beacon nodes in clustering and localization, respectively.
iv. Developing an application for real time monitoring and automation of agricultural processes in precision agriculture using the proposed framework.

Bibliography

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] S. R. J. Ramson and D. J. Moni, "Applications of wireless sensor networks—A survey," in 2017 international conference on innovations in electrical, electronics, instrumentation and media technology (ICEEIMT), 2017, pp. 325–329.

[3] Z. Ullah, L. Mostarda, R. Gagliardi, D. Cacciagrano, and F. Corradini, "A Comparison of HEED Based Clustering Algorithms--Introducing ER-HEED," in 2016 IEEE 30th international conference on advanced information networking and applications (AINA), 2016, pp. 339–345.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4. pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[5] H. Knoche and H. De Meer, "QoS parameters: A comparative study," Univ. Hamburg, Hamburg, Ger. Tech. Rep, 1997.

[6] M. Shokouhifar and A. Jalali, "Optimized sugeno fuzzy clustering algorithm for wireless sensor networks," Eng. Appl. Artif. Intell., vol. 60, pp. 16–25, 2017, doi: 10.1016/j.engappai.2017.01.007.

[7] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 2. pp. 551–591, 2013, doi: 10.1109/SURV.2012.062612.00084.

[8] H. Yoo, M. Shim, and D. Kim, "Dynamic duty-cycle scheduling schemes for energy-harvesting wireless sensor networks," IEEE Commun. Lett., vol. 16, no. 2, pp. 202–204, 2012.

[9] G. M. Shafiullah, S. A. Azad, and A. B. M. S. Ali, "Energy-efficient wireless MAC protocols for railway monitoring applications," IEEE Trans. Intell. Transp. Syst., vol. 14, no. 2, pp. 649–659, 2013.

[10] S. Sudevalayam and P. Kulkarni, "Energy harvesting sensor nodes: Survey and implications," IEEE Commun. Surv. Tutorials, vol. 13, no. 3, pp. 443–461, 2011.

[11] J. Yan, M. Zhou, and Z. Ding, "Recent advances in energy-efficient routing protocols for wireless sensor networks: A review," IEEE Access, vol. 4, pp. 5673–5686, 2016.

[12] K. Akkaya and M. Younis, "An energy-aware QoS routing protocol for wireless sensor networks," in Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on, 2003, pp. 710–715.

[13] J. Kuriakose, S. Joshi, R. V. Raju, and A. Kilaru, "A Review on Localization in Wireless Sensor Networks.," in SIRS, 2014, pp. 599–610.

[14] G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani, and G. K. Karagiannidis, "A survey on mobile anchor node assisted localization in wireless sensor networks," IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2220–2243, 2016.

[15] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, Disruptive technologies: Advances that will transform life, business, and the global economy, vol. 180. McKinsey Global Institute San Francisco, CA, 2013.

[16] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for IOT," in Multimedia Technology (ICMT), 2011 International Conference on, 2011, pp. 747–751.

[17] P. Sengottuvelan and N. Prasath, "BAFSA: Breeding artificial fish swarm algorithm for optimal cluster head selection in wireless sensor networks," Wirel. Pers. Commun., vol. 94, no. 4, pp. 1979–1991, 2017.

[18] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. p. 10 pp. vol.2, 2000, doi: 10.1109/HICSS.2000.926982.

[19] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wirel. Commun., vol. 1,

no. 4, pp. 660–670, 2002.
[20] J. Jia, Z. He, J. Kuang, and Y. Mu, “An energy consumption balanced clustering algorithm for wireless sensor network,” in Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference On, 2010, pp. 1–4.
[21] J.-S. Lee and W.-L. Cheng, “Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Predication,” IEEE Sens. J., vol. 12, no. 9, pp. 2891–2897, 2012, doi: 10.1109/JSEN.2012.2204737.
[22] P. Nayak and B. Vathasavai, “Energy Efficient Clustering Algorithm for Multi-Hop Wireless Sensor Network Using Type-2 Fuzzy Logic,” IEEE Sens. J., vol. 17, no. 14, pp. 4492–4499, 2017.
[23] J. Wang, Y. Cao, B. Li, H. Kim, and S. Lee, “Particle swarm optimization based clustering algorithm with mobile sink for WSNs,” Futur. Gener. Comput. Syst., vol. 76, pp. 452–457, 2017.
[24] G. Ahmed, J. Zou, M. M. S. Fareed, and M. Zeeshan, “Sleep-awake energy efficient distributed clustering algorithm for wireless sensor networks,” Comput. Electr. Eng., vol. 56, pp. 385–398, 2016.
[25] L. Qing, Q. Zhu, and M. Wang, “Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks,” Comput. Commun., vol. 29, no. 12, pp. 2230–2237, 2006.
[26] B. Xie and C. Wang, “An improved distributed energy efficient clustering algorithm for heterogeneous WSNs,” in 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017, pp. 1–6.
[27] M. Selvi, C. Nandhini, K. Thangaramya, K. Kulothungan, and A. Kannan, “HBO based clustering and energy optimized routing algorithm for WSN,” in 2016 Eighth International Conference on Advanced Computing (ICoAC), 2017, pp. 89–92.
[28] Z. Wang, X. Qin, and B. Liu, “An energy-efficient clustering routing algorithm for WSN-assisted IoT,” in 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6.
[29] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, “Residual energy-based cluster-head selection in WSNs for IoT application,” IEEE Internet Things J., vol. 6, no. 3, pp. 5132–5139, 2019.
[30] S. Li, H. Fang, and J. Chen, “Energy efficient multi-target clustering algorithm for WSN-based distributed consensus filter,” in 2017 36th Chinese Control Conference (CCC), 2017, pp. 8201–8206.
[31] D. Lin and Q. Wang, “An energy-efficient clustering algorithm combined game theory and dual-cluster-head mechanism for WSNs,” IEEE Access, vol. 7, pp. 49894–49905, 2019.
[32] O. Younis and S. Fahmy, “HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,” IEEE Trans. Mob. Comput., vol. 3, no. 4, pp. 366–379, 2004, doi: 10.1109/TMC.2004.41.
[33] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, “Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks,” Int. J. Distrib. Sens. Networks, vol. 9, no. 1, p. 374796, 2013.
[34] E. Ever, R. Luchmun, L. Mostarda, A. Navarra, and P. Shah, “UHEED-an unequal clustering algorithm for wireless sensor networks,” 2012.
[35] N. Aierken, R. Gagliardi, L. Mostarda, and Z. Ullah, “RUHEED-rotated unequal clustering algorithm for wireless sensor networks,” in 2015 IEEE 29th international conference on advanced information networking and applications workshops (WAINA), 2015, pp. 170–174.
[36] N. Nokhanji, Z. M. Hanapi, S. Subramaniam, and M. A. Mohamed, “An energy aware distributed clustering algorithm using fuzzy logic for wireless sensor networks with non-uniform node distribution,” Wirel. Pers. Commun., vol. 84, no. 1, pp. 395–419, 2015.
[37] T. Liu, J. Peng, J. Yang, G. Chen, and W. Xu, “Avoidance of energy hole problem based on feedback mechanism for heterogeneous sensor networks,” Int. J. Distrib. Sens. Networks, vol. 13, no. 6, p. 1550147717713625, 2017.
[38] M. Micheletti, L. Mostarda, and A. Piermarteri, “Rotating energy efficient clustering for heterogeneous devices (REECHD),” in 2018 IEEE 32nd International Conference on Advanced

Information Networking and Applications (AINA), 2018, pp. 213–220.
[39] G. Ran, H. Zhang, and G. Shulan, “Improving on LEACH Protocol of Wireless Sensor using Fuzzy Logic,” Inf. Comput. Sci., vol. 3, no. March, pp. 767–775, 2010, doi: 10.1109/SENSORCOMM.2007.21.
[40] T. C. Kim, J, S. Park, Y. Han, “CHEF: Cluster Head Election mechanism using Fuzzy logic in Wireless Sensor Networks,” ”, Adv. Commun. Technol. ICACT, pp. pp. 654–659, 17–20, 2008.
[41] T. Sharma and B. Kumar, “F-MCHEL: Fuzzy based master cluster head election leach protocol in wireless sensor network,” Int. J. Comput. Sci. Telecommun., vol. 3, no. 10, pp. 8–13, 2012.
[42] G. P. Gupta and S. Jha, “Integrated clustering and routing protocol for wireless sensor networks using Cuckoo and Harmony Search based metaheuristic techniques,” Eng. Appl. Artif. Intell., vol. 68, pp. 101–109, 2018.
[43] T. Kaur and D. Kumar, “Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks,” IEEE Sens. J., vol. 18, no. 11, pp. 4614–4622, 2018.
[44] Q.-Y. Zhang, Z.-M. Sun, and F. Zhang, “A clustering routing protocol for wireless sensor networks based on type-2 fuzzy logic and ACO,” in Fuzzy Systems (FUZZ-IEEE), 2014 IEEE International Conference on, 2014, pp. 1060–1067.
[45] H. Bagci and A. Yazici, “An energy aware fuzzy approach to unequal clustering in wireless sensor networks,” Appl. Soft Comput. J., vol. 13, no. 4, pp. 1741–1749, 2013, doi: 10.1016/j.asoc.2012.12.029.
[46] S. A. Sert, H. Bagci, and A. Yazici, “MOFCA: Multi-objective fuzzy clustering algorithm for wireless sensor networks,” Appl. Soft Comput., vol. 30, pp. 151–165, 2015.
[47] M. Khabiri and A. Ghaffari, “Energy-aware clustering-based routing in wireless sensor networks using cuckoo optimization algorithm,” Wirel. Pers. Commun., vol. 98, no. 3, pp. 2473–2495, 2018.
[48] A. Jain and A. K. Goel, “Energy efficient fuzzy routing protocol for wireless sensor networks,” Wirel. Pers. Commun., vol. 110, no. 3, pp. 1459–1474, 2020.
[49] R. Yarinezhad and S. N. Hashemi, “Solving the load balanced clustering and routing problems in WSNs with an fpt-approximation algorithm and a grid structure,” Pervasive Mob. Comput., vol. 58, p. 101033, 2019.
[50] N. Sabor, S. M. Ahmed, M. Abo-Zahhad, and S. Sasaki, “ARBIC: an adjustable range based immune hierarchy clustering protocol supporting mobility of wireless sensor networks,” Pervasive Mob. Comput., vol. 43, pp. 27–48, 2018.
[51] L. Doherty and L. El Ghaoui, “Convex position estimation in wireless sensor networks,” in Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213), 2001, vol. 3, pp. 1655–1663.
[52] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. O’dea, “Relative location estimation in wireless sensor networks,” IEEE Trans. signal Process., vol. 51, no. 8, pp. 2137–2148, 2003.
[53] W. Cheng, J. Li, and H. Li, “An improved APIT location algorithm for wireless sensor networks,” in Advances in electrical engineering and automation, Springer, 2012, pp. 113–119.
[54] D. Niculescu and B. Nath, “Ad hoc positioning system (APS) using AOA,” in IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003, vol. 3, pp. 1734–1743.
[55] Y. Zhu, D. Huang, and A. Jiang, “Network localization using angle of arrival,” in 2008 IEEE International Conference on Electro/Information Technology, 2008, pp. 205–210.
[56] A. Nasipuri and K. Li, “A directionality based location discovery scheme for wireless sensor networks,” in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, 2002, pp. 105–111.
[57] D. Niculescu and B. Nath, “Ad hoc positioning system (APS),” in IEEE Global Telecommunications Conference, GLOBECOM’01., 2001, vol. 5, pp. 2926–2931.
[58] M. Guadane, W. Bchimi, A. Samet, and S. Affes, “Enhanced range-free localization in wireless sensor networks using a new weighted hop-size estimation technique,” in Personal, Indoor, and

Mobile Radio Communications (PIMRC), IEEE 28th Annual International Symposium on, 2017, pp. 1–5.
[59] A. Hadir, K. Zine-Dine, M. Bakhouya, and J. El Kafi, "An optimized DV-hop localization algorithm using average hop weighted mean in WSNs," in Codes, Cryptography and Communication Systems (WCCCS), 2014, pp. 25–29.
[60] Z. Zhong and T. He, "RSD: A metric for achieving range-free localization beyond connectivity," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 11, pp. 1943–1951, 2011.
[61] J. Mei, D. Chen, J. Gao, Y. Gao, and L. Yang, "Range-free Monte Carlo localization for mobile wireless sensor networks," in 2012 International Conference on Computer Science and Service System, 2012, pp. 1066–1069.
[62] S. Zaidi, A. El Assaf, S. Affes, and N. Kandil, "Range-free node localization in multi-hop wireless sensor networks," in 2016 IEEE Wireless Communications and Networking Conference, 2016, pp. 1–7.
[63] M. Singh and P. M. Khilar, "An analytical geometric range free localization scheme based on mobile beacon points in wireless sensor network," Wirel. Networks, vol. 22, no. 8, pp. 2537–2550, 2016.
[64] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in Proceedings of the 9th annual international conference on Mobile computing and networking, 2003, pp. 81–95.
[65] S. M. Hosseinirad, M. Niazi, J. Pourdeilami, S. K. Basu, and A. A. Pouyan, "On improving APIT algorithm for better localization in WSN," J. AI Data Min., vol. 2, no. 2, pp. 97–104, 2014.
[66] L. He and Z. Kang, "A weighted APIT localization algorithm based on vector similarity," in 2015 International Conference on Computer Science and Intelligent Communication, 2015, pp. 8–11.
[67] X. Wan, L. Shen, Z. Chen, and H. Xu, "An efficient virtual nodes-based APIT localization algorithm with low computational cost," in 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), 2018, pp. 1–4.
[68] S. Jain, A. Singh, A. Kaur, and S. Jain, "Improved APIT localization algorithm in wireless sensor networks," in 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, pp. 77–81.
[69] N. Chuku and A. Nasipuri, "RSSI-Based localization schemes for wireless sensor networks using outlier detection," J. Sens. Actuator Networks, vol. 10, no. 1, p. 10, 2021.
[70] S. Arora and S. Singh, "Node localization in wireless sensor networks using butterfly optimization algorithm," Arab. J. Sci. Eng., vol. 42, no. 8, pp. 3325–3335, 2017.
[71] S. P. Singh and S. C. Sharma, "A PSO based improved localization algorithm for wireless sensor network," Wirel. Pers. Commun., vol. 98, no. 1, pp. 487–503, 2018.
[72] Q. Ren, Y. Zhang, I. Nikolaidis, J. Li, and Y. Pan, "RSSI quantization and genetic algorithm based localization in wireless sensor networks," Ad Hoc Networks, vol. 107, p. 102255, 2020.
[73] E. Tuba, M. Tuba, and M. Beko, "Two stage wireless sensor node localization using firefly algorithm," in Smart trends in systems, security and sustainability, Springer, 2018, pp. 113–120.
[74] P. SrideviPonmalar, V. J. S. Kumar, and R. Harikrishnan, "Hybrid firefly variants algorithm for localization optimization in WSN," Int. J. Comput. Intell. Syst., vol. 10, no. 1, pp. 1263–1271, 2017.
[75] S. Pandey and S. Varma, "A range based localization system in multihop wireless sensor networks: a distributed cooperative approach," Wirel. Pers. Commun., vol. 86, no. 2, pp. 615–634, 2016.
[76] S. K. Rout, A. K. Rath, P. K. Mohapatra, P. K. Jena, and A. Swain, "A fuzzy optimization technique for energy efficient node localization in wireless sensor network using dynamic trilateration method," in Progress in Computing, Analytics and Networking, Springer, 2018, pp. 325–338.
[77] L. Lazos, R. Poovendran, and S. Čapkun, "ROPE: robust position estimation in wireless sensor networks," in Proceedings of the 4th international symposium on Information processing in sensor networks, 2005, p. 43.

[78] T. Park and K. G. Shin, “Attack-tolerant localization via iterative verification of locations in sensor networks,” ACM Trans. Embed. Comput. Syst., vol. 8, no. 1, p. 2, 2008.
[79] S. Li, X. Wang, S. Zhao, J. Wang, and L. Li, “Local semidefinite programming-based node localization system for wireless sensor network applications,” IEEE Syst. J., vol. 8, no. 3, pp. 879–888, 2013.
[80] P. Perazzo, L. Taponecco, A. A. D’amico, and G. Dini, “Secure positioning in wireless sensor networks through enlargement miscontrol detection,” ACM Trans. Sens. Networks, vol. 12, no. 4, p. 27, 2016.
[81] P. Perazzo, F. B. Sorbelli, M. Conti, G. Dini, and C. M. Pinotti, “Drone path planning for secure positioning and secure position verification,” IEEE Trans. Mob. Comput., vol. 16, no. 9, pp. 2478–2493, 2016.
[82] L. Lazos and R. Poovendran, “SeRLoc: Secure range-independent localization for wireless sensor networks,” in Proceedings of the 3rd ACM workshop on Wireless security, 2004, pp. 21–30.
[83] L. Lazos and R. Poovendran, “HiRLoc: high-resolution robust localization for wireless sensor networks,” IEEE J. Sel. areas Commun., vol. 24, no. 2, pp. 233–246, 2006.
[84] M. Demirbas and Y. Song, “An RSSI-based scheme for sybil attack detection in wireless sensor networks,” in 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM’06), 2006, p. 5–pp.
[85] M. Wen, H. Li, Y.-F. Zheng, and K.-F. Chen, “TDOA-based Sybil attack detection scheme for wireless sensor networks,” J. Shanghai Univ. (English Ed., vol. 12, no. 1, pp. 66–70, 2008.
[86] Y. Zhang, K. Fan, S.-B. Zhang, and W. Mo, “AOA based trust evaluation scheme for Sybil attack detection in WSN,” Appl. Res. Comput, vol. 27, no. 2, pp. 1847–1849, 2010.
[87] X. Wang, L. Qian, and H. Jiang, “Tolerant majority-colluding attacks for secure localization in wireless sensor networks,” in 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, pp. 1–5.
[88] Y. Liu and Y. Wu, “An Enhanced RSSI-Based Detection Scheme for Sybil Attack in Wireless Sensor Networks,” in Future of Information and Communication Conference, 2019, pp. 87–102.
[89] Y. Yuan, L. Huo, Z. Wang, and D. Hogrefe, “Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks,” IEEE Access, vol. 6, pp. 27629–27636, 2018.
[90] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010, doi: http://dx.doi.org/10.1016/j.comnet.2010.05.010.
[91] X. Jia, Q. Feng, T. Fan, and Q. Lei, “RFID technology and its applications in Internet of Things (IoT),” Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. pp. 1282–1285, 2012, doi: 10.1109/CECNet.2012.6201508.
[92] A. Giri, S. Dutta, and S. Neogy, “Enabling agricultural automation to optimize utilization of water, fertilizer and insecticides by implementing Internet of Things (IoT),” International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds. pp. 125–131, 2016, doi: 10.1109/INCITE.2016.7857603.
[93] J. Gantz and D. Reinsel, “The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east,” IDC iView IDC Anal. Futur., vol. 2007, no. 2012, pp. 1–16, 2012.
[94] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of Internet of things,” in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, vol. 5, pp. V5–484.
[95] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, “A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment,” in Science Engineering and Management Research (ICSEMR), 2014 International Conference on, 2014, pp. 1–8.
[96] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, “A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities,” IEEE Wirel. Commun., vol. 20, no. 6, pp. 91–98, 2013.
[97] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for internet of things: a survey,” IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, 2016.

[98] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: A study," Int. J. Comput. Sci. Eng. Surv., vol. 2, no. 3, pp. 94–105, 2011.
[99] S. N. Han, I. Khan, G. M. Lee, N. Crespi, and R. H. Glitho, "Service composition for IP smart object using realtime Web protocols: Concept and research challenges," Comput. Stand. Interfaces, vol. 43, pp. 79–90, 2016.
[100] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a Social Structure to the Internet of Things," IEEE Communications Letters, vol. 15, no. 11. pp. 1193–1195, 2011, doi: 10.1109/LCOMM.2011.090911.111340.
[101] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on, 2012, pp. 257–260.
[102] G. M. Lee, N. Crespi, J. K. Choi, and M. Boussard, "Internet of things," in Evolution of Telecommunication Services, Springer, 2013, pp. 257–282.
[103] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Trans. Ind. informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
[104] N. Koshizuka and K. Sakamura, "Ubiquitous ID: standards for ubiquitous computing and the Internet of Things," IEEE Pervasive Comput., vol. 4, no. 9, pp. 98–101, 2010.
[105] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals," RFC 4919 (Informational), Internet Engineering Task Force, 2007.
[106] G. Roussos and V. Kostakos, "rfid in pervasive computing: State-of-the-art and outlook," Pervasive Mob. Comput., vol. 5, no. 1, pp. 110–131, Feb. 2009, doi: http://dx.doi.org/10.1016/j.pmcj.2008.11.004.
[107] A. Juels, "RFID security and privacy: A research survey," Sel. Areas Commun. IEEE J., vol. 24, no. 2, pp. 381–394, 2006.
[108] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: a survey and a comparison," IEEE Wirel. Commun., vol. 12, no. 1, pp. 12–26, 2005.
[109] R. Want, "Near field communication," IEEE Pervasive Comput., vol. 10, no. 3, pp. 4–7, 2011.
[110] P. McDermott-Wells, "What is bluetooth?," IEEE potentials, vol. 23, no. 5, pp. 33–35, 2004.
[111] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," 2014.
[112] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," IEEE Internet Comput., vol. 16, no. 2, pp. 62–67, 2012.
[113] D. Locke, "Mq telemetry transport (mqtt) v3. 1 protocol specification," IBM Dev. Tech. Libr., 2010.
[114] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," Internet Eng. Task Force (IETF), Fremont, CA, USA, Req. Comments 6120, 2011.
[115] A. J. Jara, P. Martinez-Julia, and A. Skarmeta, "Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for the Web of Things," in innovative mobile and internet services in ubiquitous computing (IMIS), 2012 sixth international conference on, 2012, pp. 731–738.
[116] I. 802 W. Group, "IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Std, vol. 802, pp. 4–2011, 2011.
[117] M. Durvy et al., "Making sensor networks IPv6 ready," in Proceedings of the 6th ACM conference on Embedded network sensor systems, 2008, pp. 421–422.
[118] V. Raghunathan, S. Ganeriwal, and M. Srivastava, "Emerging techniques for long lived wireless sensor networks," IEEE Commun. Mag., vol. 44, no. 4, pp. 108–114, 2006.
[119] D. Niyato, E. Hossain, M. M. Rashid, and V. K. Bhargava, "Wireless sensor networks with energy harvesting technologies: A game-theoretic approach to optimal energy management," IEEE Wirel. Commun., vol. 14, no. 4, 2007.
[120] M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey," Ad Hoc Networks, vol. 6, no. 4, pp. 621–655, 2008.
[121] X. Wu, G. Chen, and S. K. Das, "Avoiding energy holes in wireless sensor networks with nonuniform node distribution," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 5, pp. 710–720, 2008.

[122] I. F. Akyildiz, F. Brunetti, and C. Blázquez, "Nanonetworks: A new communication paradigm," Comput. Networks, vol. 52, no. 12, pp. 2260–2279, 2008.
[123] H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?," IEEE Communications Letters, vol. 15, no. 4. pp. 461–463, 2011, doi: 10.1109/LCOMM.2011.022411.110120.
[124] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," Int. J. Sustain. Dev. World Ecol., vol. 20, no. 3, pp. 216–222, 2013.
[125] O. Vermesan et al., "Internet of things strategic research roadmap," Internet Things-Global Technol. Soc. Trends, vol. 1, pp. 9–52, 2011.
[126] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TinyDB: an acquisitional query processing system for sensor networks," ACM Trans. database Syst., vol. 30, no. 1, pp. 122–173, 2005.
[127] K. E. Kjær, "A survey of context-aware middleware," in Proceedings of the 25th conference on IASTED International Multi-Conference: Software Engineering, 2007, pp. 148–155.
[128] P. Costa, G. Coulson, C. Mascolo, G. P. Picco, and S. Zachariadis, "The RUNES middleware: a reconfigurable component-based approach to networked embedded systems," 2005 IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 2. pp. 806–810 Vol. 2, 2005, doi: 10.1109/PIMRC.2005.1651554.
[129] P. R. Pietzuch, "Hermes: A scalable event-based middleware," University of Cambridge, Computer Laboratory, 2004.
[130] M. Eisenhauer, P. Rosengren, and P. Antolin, "Hydra: A development platform for integrating wireless devices and sensors into ambient intelligence systems," in The Internet of Things, Springer, 2010, pp. 367–373.
[131] E. Avilés-López and J. A. García-Macías, "TinySOA: a service-oriented architecture for wireless sensor networks," Serv. Oriented Comput. Appl., vol. 3, no. 2, pp. 99–108, 2009.
[132] V. Tsiatsis, "The SENSEI real world internet architecture," 2010.
[133] C. M. Kirsch, M. A. A. Sanvido, and T. A. Henzinger, "A programmable microkernel for real-time systems," in Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments, 2005, pp. 35–45.
[134] A. Boulis, C.-C. Han, R. Shea, and M. B. Srivastava, "SensorWare: Programming sensor networks beyond code update and querying," Pervasive Mob. Comput., vol. 3, no. 4, pp. 386–412, 2007.
[135] C.-L. Fok, G.-C. Roman, and C. Lu, "Agilla: A mobile agent middleware for self-adaptive wireless sensor networks," ACM Trans. Auton. Adapt. Syst., vol. 4, no. 3, p. 16, 2009.
[136] V. Terziyan, O. Kaykova, and D. Zhovtobryukh, "Ubiroad: Semantic middleware for context-aware smart road environments," in Internet and web applications and services (iciw), 2010 fifth international conference on, 2010, pp. 295–302.
[137] A. L. Murphy, G. Pietro Picco, and G.-C. Roman, "Lime: A middleware for physical and logical mobility," in Distributed Computing Systems, 2001. 21st International Conference on., 2001, pp. 524–533.
[138] R. de C. A. Lima, N. S. Rosa, and I. R. L. Marques, "TS-Mid: Middleware for wireless sensor networks based on tuple space," in Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on, 2008, pp. 886–891.
[139] P. Andreou, D. Zeinalipour-Yazti, M. Vassiliadou, P. K. Chrysanthis, and G. Samaras, "Kspot: Effectively monitoring the k most important events in a wireless sensor network," in Data Engineering, 2009. ICDE'09. IEEE 25th International Conference on, 2009, pp. 1503–1506.
[140] P. B. Gibbons, B. Karp, Y. Ke, S. Nath, and S. Seshan, "Irisnet: An architecture for a worldwide sensor web," IEEE pervasive Comput., vol. 2, no. 4, pp. 22–33, 2003.
[141] W. B. Heinzelman, A. L. Murphy, H. S. Carvalho, and M. A. Perillo, "Middleware to support sensor network applications," IEEE Netw., vol. 18, no. 1, pp. 6–14, 2004.
[142] Q. Han and N. Venkatasubramanian, "Autosec: An integrated middleware framework for dynamic service brokering," IEEE Distrib. Syst. online, vol. 2, no. 7, pp. 22–31, 2001.
[143] P. Costa et al., "The RUNES middleware for networked embedded systems and its application in a disaster management scenario," in Pervasive Computing and Communications, 2007.

PerCom'07. Fifth Annual IEEE International Conference on, 2007, pp. 69–78.
[144] M. Musolesi, C. Mascolo, and S. Hailes, "Emma: Epidemic messaging middleware for ad hoc networks," Pers. Ubiquitous Comput., vol. 10, no. 1, pp. 28–36, 2006.
[145] T. Sivaharan, G. Blair, and G. Coulson, "Green: A configurable and re-configurable publish-subscribe middleware for pervasive computing," in OTM Confederated International Conferences" On the Move to Meaningful Internet Systems," 2005, pp. 732–749.
[146] K. Hong et al., "TinyVM: an energy- efficient execution infrastructure for sensor networks," Softw. Pract. Exp., vol. 42, no. 10, pp. 1193–1209, 2012.
[147] P. Kang, C. Borcea, G. Xu, A. Saxena, U. Kremer, and L. Iftode, "Smart messages: A distributed computing platform for networks of embedded systems," Comput. J., vol. 47, no. 4, pp. 475–494, 2004.
[148] L. Baresi, S. Guinea, and P. Saeedi, "Achieving self-adaptation through dynamic group management," in Assurances for Self-Adaptive Systems, Springer, 2013, pp. 214–239.
[149] P. Bonnet, J. Gehrke, and P. Seshadri, "Towards sensor database systems," in International Conference on Mobile Data Management, 2001, pp. 3–14.
[150] T. Hasiotis, G. Alyfantis, V. Tsetsos, O. Sekkas, and S. Hadjiefthymiades, "Sensation: A middleware integration platform for pervasive applications in wireless sensor networks," in Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on, 2005, pp. 366–377.
[151] H. Alex, M. Kumar, and B. Shirazi, "MidFusion: An adaptive middleware for information fusion in sensor network applications," Inf. Fusion, vol. 9, no. 3, pp. 332–343, 2008.
[152] N. Bui and M. Zorzi, "Health care applications: a solution based on the internet of things," in Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, 2011, p. 131.
[153] A.-M. Rahmani et al., "Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems," in Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE, 2015, pp. 826–834.
[154] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.
[155] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in Information technology: new generations (ITNG), 2010 seventh international conference on, 2010, pp. 804–809.
[156] G. Acampora, D. J. Cook, P. Rashidi, and A. V Vasilakos, "A survey on ambient intelligence in healthcare," Proc. IEEE, vol. 101, no. 12, pp. 2470–2494, 2013.
[157] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[158] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014.
[159] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times, 2011, pp. 282–291.
[160] T. Bakıcı, E. Almirall, and J. Wareham, "A smart city initiative: the case of Barcelona," J. Knowl. Econ., vol. 4, no. 2, pp. 135–148, 2013.
[161] Y. Bo and H. Wang, "The Application of Cloud Computing and the Internet of Things in Agriculture and Forestry," Service Sciences (IJCSS), 2011 International Joint Conference on. pp. 168–172, 2011, doi: 10.1109/IJCSS.2011.40.
[162] J. Zhao, J. Zhang, Y. Feng, and J. Guo, "The study and application of the IOT technology in agriculture," Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 2. pp. 462–465, 2010, doi: 10.1109/ICCSIT.2010.5565120.
[163] G. Baldini et al., "A Cognitive Framework for Realizing and Exploiting the Internet of Things Concept," 2011.
[164] "IoT6 European research project, Deliverable D1.5:" http://www.iot6.eu (accessed Nov. 08, 2015).
[165] "IoTivity." https://www.iotivity.org/ (accessed Jan. 01, 2015).
[166] M. Weiser, "The computer for the 21st century.," Mob. Comput. Commun. Rev., vol. 3, no. 3,

pp. 3–11, 1999.
[167] Z. Shelby, “ETSI M2M Standardization, March 16, 2009.” .
[168] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Comput. Networks, vol. 76, pp. 146–164, 2015.
[169] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe: Lightweight secure CoAP for the internet of things,” IEEE Sens. J., vol. 13, no. 10, pp. 3711–3720, 2013.
[170] I. T. S. Headquarters, “e-Japan strategy,” Retrieved June, vol. 22, p. 2004, 2001.
[171] “AllJoyn Framework.” https://allseenalliance.org/ (accessed Nov. 13, 2015).
[172] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: a survey of existing protocols and open research issues,” IEEE Commun. Surv. Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.
[173] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, “Data mining with big data,” IEEE Trans. Knowl. Data Eng., vol. 26, no. 1, pp. 97–107, 2014.
[174] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, “Data mining for Internet of Things: A survey.,” IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 77–97, 2014.
[175] M. Moshtaghi et al., “Streaming analysis in wireless sensor networks,” Wirel. Commun. Mob. Comput., vol. 14, no. 9, pp. 905–921, 2014.
[176] A. Bialecki, M. Cafarella, D. Cutting, and O. O’MALLEY, “Hadoop: a framework for running applications on large clusters built of commodity hardware,” Wiki http//lucene. apache. org/hadoop, vol. 11, 2005.
[177] P. G. Brown, “Overview of SciDB: large scale array storage, processing and analysis,” in Proceedings of the 2010 ACM SIGMOD International Conference on Management of data, 2010, pp. 963–968.
[178] X. Meng et al., “Mllib: Machine learning in apache spark,” J. Mach. Learn. Res., vol. 17, no. 34, pp. 1–7, 2016.
[179] M. H. Iqbal and T. R. Soomro, “Big data analysis: Apache storm perspective,” Int. J. Comput. Trends Technol., pp. 9–14, 2015.
[180] D. Laney, “3D data management: Controlling data volume, velocity and variety,” META Gr. Res. Note, vol. 6, p. 70, 2001.
[181] B. Data, “Principles and best practices of scalable realtime data systems,” N. Marz J. Warren. Henning, 2014.
[182] M. Chen, S. Mao, and Y. Liu, “Big Data: A Survey,” Mob. Networks Appl., vol. 19, no. 2, pp. 171–209, 2014, doi: 10.1007/s11036-013-0489-0.
[183] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Comput. Networks, vol. 52, no. 12, pp. 2292–2330, 2008, doi: http://dx.doi.org/10.1016/j.comnet.2008.04.002.
[184] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, “What’s inside the Cloud? An architectural map of the Cloud landscape,” in Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009, pp. 23–31.
[185] “World Bank 2011-14.” http://data.worldbank.org/indicator/NV.AGR.TOTL.ZS.
[186] A. Giri, S. Dutta, S. Neogy, K. Dahal, and Z. Pervez, “Internet of Things (IoT): A Survey on Architecture, Enabling Technologies, Applications and Challenges,” in Proceedings of the 1st International Conference on Internet of Things and Machine Learning, 2017, pp. 7:1–7:12.
[187] K. Guravaiah and R. L. Velusamy, “Energy efficient clustering algorithm using RFD based multi-hop communication in wireless sensor networks,” Wirel. Pers. Commun., vol. 95, no. 4, pp. 3557–3584, 2017.
[188] P. Neamatollahi and M. Naghibzadeh, “Distributed unequal clustering algorithm in large-scale wireless sensor networks using fuzzy logic,” J. Supercomput., vol. 74, no. 6, pp. 2329–2352, 2018.
[189] R. Logambigai and A. Kannan, “Fuzzy logic based unequal clustering for wireless sensor networks,” Wirel. Networks, vol. 22, no. 3, pp. 945–957, 2016.
[190] L. A. Zadeh, “Fuzzy logic = computing with words,” IEEE Trans. Fuzzy Syst., vol. 4, no. 2, pp. 103–111, 1996.
[191] S. Augustine and J. P. Ananth, “Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks,” Wirel. Networks, 2020, doi: 10.1007/s11276-020-02352-w.

[192] E. H. Mamdani and S. Assilian, “An experiment in linguistic synthesis with a fuzzy logic controller,” Int. J. Hum. Comput. Stud., vol. 51, no. 2, pp. 135–147, 1999.
[193] T. Takagi and M. Sugeno, “Fuzzy identification of systems and its applications to modeling and control,” IEEE Trans. Syst. Man. Cybern., no. 1, pp. 116–132, 1985.
[194] M. Clerc, Particle swarm optimization, vol. 93. John Wiley & Sons, 2010.
[195] S. Dutt, S. Agrawal, and R. Vig, “Cluster-head restricted energy efficient protocol (CREEP) for routing in heterogeneous wireless sensor networks,” Wirel. Pers. Commun., vol. 100, no. 4, pp. 1477–1497, 2018.
[196] V. Rahmati, “Near optimum random routing of uniformly load balanced nodes in wireless sensor networks using connectivity matrix,” Wirel. Pers. Commun., pp. 1–17, 2020.
[197] H. Yoo, M. Shim, and D. Kim, “Dynamic duty-cycle scheduling schemes for energy-harvesting wireless sensor networks,” IEEE Commun. Lett., vol. 16, no. 2, pp. 202–204, 2011.
[198] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, “Wireless energy harvesting for the Internet of Things,” IEEE Commun. Mag., vol. 53, no. 6, pp. 102–108, 2015.
[199] S. Ulukus et al., “Energy harvesting wireless communications: A review of recent advances,” IEEE J. Sel. Areas Commun., vol. 33, no. 3, pp. 360–381, 2015.
[200] R. R. Swain, S. Mishra, T. K. Samal, and M. R. Kabat, “An energy efficient advertisement based multichannel distributed MAC protocol for wireless sensor networks (Adv-MMAC),” Wirel. Pers. Commun., vol. 95, no. 2, pp. 655–682, 2017.
[201] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, “Locating the nodes: cooperative localization in wireless sensor networks,” IEEE Signal Process. Mag., vol. 22, no. 4, pp. 54–69, 2005.
[202] W. Shanshan, Y. Jianping, C. Zhiping, and Z. Guomin, “A RSSI-based self-localization algorithm for wireless sensor networks,” J. Comput. Res. Dev., vol. 45, no. 1, pp. 385–388, 2008.
[203] Y. Shang and W. Ruml, “Improved MDS-based localization,” in IEEE INFOCOM, 2004, vol. 4, pp. 2640–2651.
[204] A. Giri, S. Dutta, and S. Neogy, “Fuzzy Logic-Based Range-Free Localization for Wireless Sensor Networks in Agriculture,” in Advanced Computing and Systems for Security, Springer, 2020, pp. 3–12.
[205] M. A. Jan, P. Nanda, X. He, and R. P. Liu, “A Sybil attack detection scheme for a forest wildfire monitoring application,” Futur. Gener. Comput. Syst., vol. 80, pp. 613–626, 2018.
[206] V. Daiya, J. Ebenezer, S. A. V. S. Murty, and B. Raj, “Experimental analysis of RSSI for distance and position estimation,” in Proceedings of the International Conference on Recent trends in information technology (ICRTIT), 2011, pp. 1093–1098.
[207] A. Giri, S. Dutta, and S. Neogy, “Information-theoretic approach for secure localization against sybil attack in wireless sensor network,” J. Ambient Intell. Humaniz. Comput., pp. 1–7, 2020.