LOVELY PROFESSIONAL UNIVERSITY

*Transforming Education Transforming India*

# Design and Evaluation of Localization Algorithm in Wireless Sensor Networks

thesis submitted to

**LOVELY PROFESSIONAL UNIVERSITY**

for the award of

**DOCTOR OF PHILOSOPHY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

| Submitted By: | Supervised By: |
|---|---|
| Gulshan Kumar | Dr. Mritunjay Kumar Rai |
| Reg. No. 41200451 | Associate Professor, SECE |

**FACULTY OF TECHNOLOGY AND SCIENCES**

**LOVELY PROFESSIONAL UNIVERSITY**

**PUNJAB**

February 25, 2017

# CERTIFICATE

This is to certify that the thesis entitled ”Design and Evaluation of Localization algorithm in Wireless Sensor Networks”, which is being submitted by Mr. Gulshan Kumar for the award of the degree of Doctor of Philosophy in Computer Engineering from the Faculty of Engineering and Technology, Lovely Professional University, Punjab, India, is entirely based on the work carried out by him under my supervision and guidance. The work reported, embodies the original work of the candidate and has not been submitted to any other university or institution for the award of any degree or diploma, according to the best of my knowledge.

Dr. Mritunjay Kumar Rai
Associate Professor
Department of Electronics and Communication Engineering
Lovely Professional University
Phagwara, Punjab-144411, India
Date: February 25, 2017

# DECLARATION

I declare that the thesis entitled ”Design and Evaluation of localization Algorithm in Wireless Sensor Networks” has been prepared by me under the guidance of Dr. Mritunjay Kumar Rai, Associate Professor, Department of Electronics and Communication Engineering, Lovely Professional University, India. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Gulshan Kumar
School of Computer Science and Engineering
Lovely Professional University
Jalandhar  Delhi G.T.Road (NH-1)
Phagwara, Punjab  144411
India
Date: February 25, 2017

# DEDICATION

*"I would like to dedicate my thesis to my beloved father Late Sh. Ram Lubhaya."*

# ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to my supervisor, Dr. Mritunjay Kumar Rai, for his supervision, advice, and guidance from the very early stage of this research as well as giving me extraordinary experiences throughout the work. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable.

I am grateful to the friends and fellow researchers, particularly Mr. Rahul Saha and Mr. Jaisukh Paul Singh for their constructive criticism and suggestions.

I would like to show my gratitude to the entire family of Lovely Professional University for providing me a suitable research atmosphere to carry out my work in proper time. I would like to thank the Division of Research and Development and School of Computer Science and Engineering for all the support and encouragement throughout the research work.

I am also very much grateful to my mother, Ms. Sneh Lata, and all my family members for their moral support and care that they shown towards me during the period of this work.

Finally, I thank God for sailing me through all the rough and tough times during this research work.

Date: February 25, 2017 Gulshan Kumar

# Abbreviations

| **Abbreviations** | **Description** |
|---|---|
| **WPAN** | Wireless Personal Area Networks |
| **WLAN** | Wireless Local Area Networks |
| **WMAN** | Wireless Metropolitan Area Networks |
| **WWAN** | Wireless Wide Area Networks |
| **MANETs** | Mobile Ad hoc Networks |
| **WSNs** | Wireless Sensor Networks |
| **MEMS** | Micro-Electro-Mechanical Systems |
| **GPS** | Global Positioning System |
| **UDG** | Unit-Disk Graph |
| **CDS** | Connected Dominating Set |
| **MCDS** | Minimum Connected Dominating Set |
| **MMSE** | Minimum Mean Square Error |
| **LAR** | Location Aided Routing |
| **GPSR** | Greedy Perimeter Stateless Routing |
| **DREAM** | Distance Routing Effect Algorithm for Mobility |
| **GHT** | Geographic Hash Table |
| **ToA** | Time of Arrival |
| **TDoA** | Time Difference of Arrival |
| **AoA** | Angle of Arrival |
| **RSSI** | Received Signal Strength Indicator |
| **RIPS** | Radio Interferometric Positioning System |

| | |
|---|---|
| **BST** | Base Station |
| **MSC** | Mobile Switching Center |
| **LoS** | Line-of-Sight |
| **ADC** | Analog-to-Digital Convertor |
| **ISM** | Industrial, Scientific and Medical |
| **TECDS** | Timer-based Energy aware Connected Dominating Set |
| **MST** | Minimum Spanning Tree |
| **CH** | Cluster Head |
| **DEA** | Differential Evolution Approach |
| **GA** | Genetic Algorithm |
| **HMAC** | Hash Message Authentication Code |
| **GTA** | Game Theoretic Aggregation |
| **LTS** | Least Trimmed Square |
| **RS** | Rank Selection |
| **RM** | Relative Mobility |

# ABSTRACT

Wireless Networking is evolving rapidly due to the human desires for mobility and freedom from tethers i.e. from physical networks to communication networks. Recent advancement in wireless technology have equipped portable systems such as notebook computers and personal digital assistants with wireless interfaces that allow network communication even a user is in movement. The primary concerns of such wireless networks are: scarce wireless bandwidth, highly dynamic topology due to node mobility, varying propagation characteristics and network availability.

The thesis focus on a particular type of wireless network: Wireless Sensor Networks (WSNs). These networks consist of a large of various sensor nodes which sense the network environment and exchange the gathered information with each other or transfer to the sink nodes.The sink nodes process the collected information and respond with commands to the sensor nodes. WSNs expand its applications in various domains such as environment monitoring which deals with monitoring air soil and water, condition based maintenance, habitat monitoring, seismic detection, military surveillance, inventory tracking, medical and home security to machine diagnosis etc.

There are several essential issues prevail in wireless sensor networks. Localization is one of the most important concern in such networks because most of the applications of WSNs depend upon knowing the location of sensor nodes. For the well suit with distinguishing characteristics of WSNs some approaches estimate location of the sensor nodes without measuring distance or angle information directly . These approaches are categorized as range free localization which is popular in the diversified domains of WSNs for its ease of applicability.

It is desirable for a resource constrained network that the process of localization should utilize minimum resources so that the overall network lifetime can be improved. Moreover, another concern with such localization process is to potentially secure the useful location information by applying adequate security services.

# CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER 1

# Introduction

## 1.1 Introduction

Wireless Networks [1][2][3] have become an important part of communication technologies. Wireless network defines to a domain of computer network that is generally associated with a telecommunication network [4] and does not use any kind of physical wires. Wireless telecommunication networks use electromagnetic waves and the implementation of such networks is done with different remote information transmission system at physical layer of the network. Such wireless networks can be categorized based on their architecture and communication coverage area. Wireless networks can be classified [1][2] depending upon the transmission range into the following types like Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN), Wireless Metropolitan area Networks (WMAN) and Wireless Wide Area Networks (WWAN). Based on the architecture the wireless networks are divided into two broad categories like Infrastructure-based networks and Infrastructure less networks.

Infrastructure-based network is defined as a type of network which has pre-defined infrastructure that is made by fixed network structure and controls the network processes. Infrastructure less network is formed dynamically through the cooperation of random set of wireless nodes. Each node is independent and free to take decision based on the network requirement. Mobile Ad hoc Networks (MANETs)[5] and Wireless Sensor Networks (WSNs)[6] are the examples of such type of wireless networks. WSNs have been expanded to a variety of application domains where close interactions with the physical world are important with respect to real time scenarios. The implementation of distributed infrastructure with sensing capabilities and the easy deployment feature make WSNs an important component of our daily lives. By providing distributed, real-time information from the physical world, WSNs extend the reach of current cyber infrastructures to the physical world. WSNs [7] consist of small sensor nodes, which act as both data generators to sense the data from the network environment and also as network relays to work as intermediaries or data forwarder. Each node consists of sensor(s), a microprocessor, and a transceiver. Through the wide range of sensors available for hard integration, capturing data from a physical environment is the standard for WSNs. Besides, the task of transmitting data, sensor nodes can be controlled to perform different complex computational functions through on-board microprocessors. The transceiver provides wireless connectivity to communicate the observed phenomena of interest. Sensor nodes are can be both stationary and mobile and are powered by limited capacity batteries. The dynamic demand of the applications has extended the WSNs from the static to the mobile for their scalability and robustness. Therefore, previously although the locations of the nodes do not change, the network topology dynamically changes due to the power management activities of the sensor nodes. But, at the present days, with the advancement of the technology the static sensors are supplemented with the mobile sensors. To save energy, sensor nodes are needed to turn their transceivers off and substantially to become a disconnected component from the network. In such dynamic environment, it is a major challenge to provide continuous connectivity of the sensor nodes while minimizing the energy consumption. The various application of WSNs in shown in Figure 1.1.

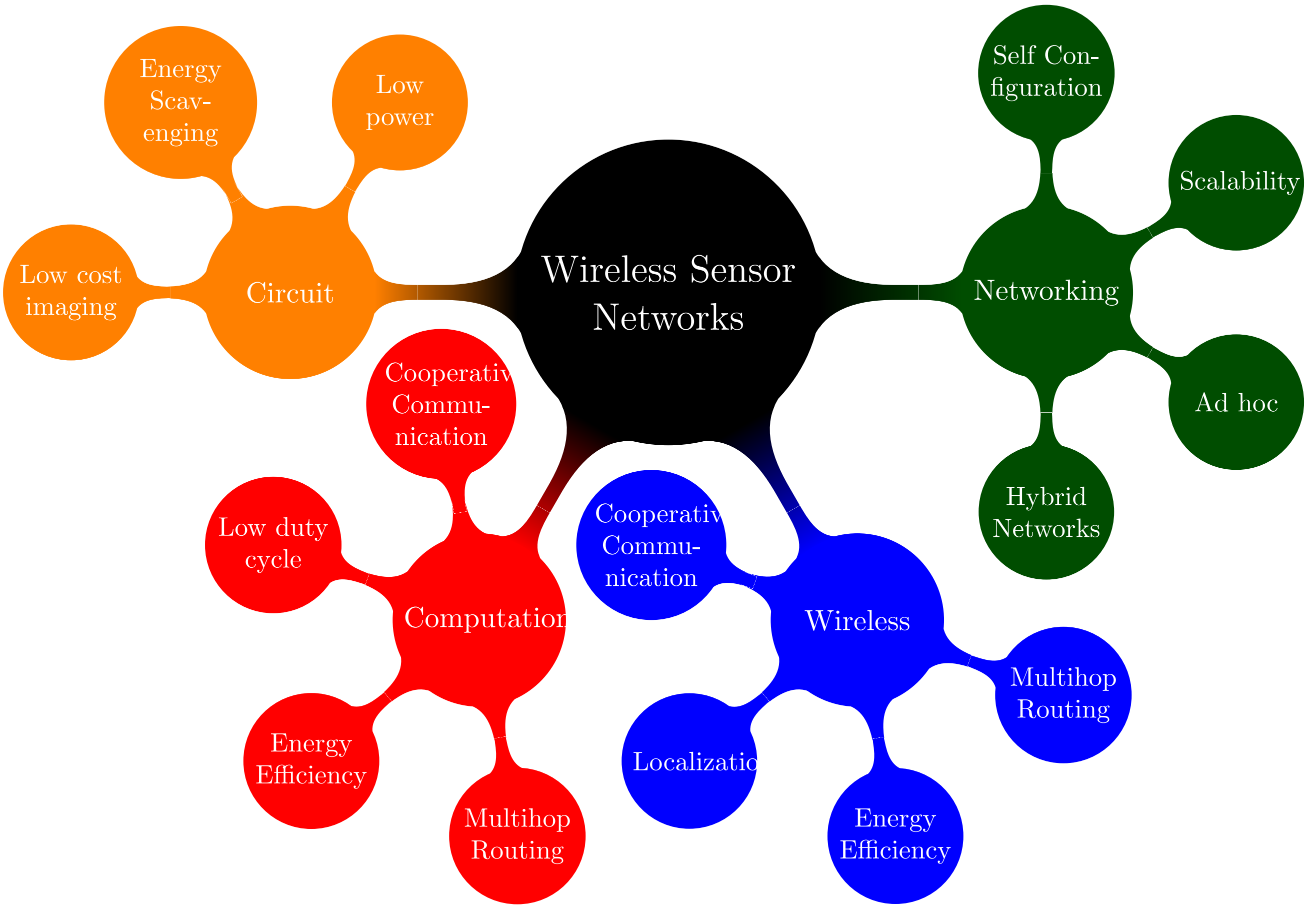


FIGURE 1.1: *Design factors of Wireless Sensor Networks*

The limited size and battery of the nodes impose limitation [6][7] on the power capacity as well as transmission range. In fulfilling the requirements of users, limited bandwidth of wireless channels and their transmission characteristics provide additional constraints on the exchange of management and control information. Design of network protocols in WSNs becomes challenging due to limited processing power and storage of the sensor nodes. Conventional routing algorithms are therefore not suitable for such networks. WSNs require efficient distributed algorithms with low computation complexity, low communication complexity and low storage complexity. Some algorithms give better results, when transmission range of all nodes is uniform but these algorithms are unable to perform well when nodes have different transmission ranges. Different types of routing such as unicast, multicast and broadcast are required in WSNs. In multi hop WSNs [8], routing is complex because of continual change in network topology due to mobility of hosts and limited power, computational capacity and memory of the hosts. Moreover, the lack of fixed infrastructure forces the hosts to act as routers. Other factors that are important to consider in a wireless environment are: variable wireless link quality, propagation path loss multipath fading, multi-user interferences, non-Gaussian noise and limited bandwidth render routing protocol design very complicated. The main goal of any protocol is to maximize performance with minimum resource utilization. This performance depends upon hop count, delay, loss rate, throughput and stability.

## 1.2 State of the Art

A sensor network [6] is designed and deployed to perform various level of information processing tasks such as detection, object tracking, or classification of multi objects. Different types of measures are also available to scale the performance for these tasks are including false alarms or misses, classification errors, and tracking quality. Applications [9] of sensor networks are wide and its range varies depending upon in application requirements, modes of deployment such as ad hoc or fixed environment, sensing modality, or means of power supply. Some of the such applications include:

- Environmental monitoring (e.g., traffic, habitat, security)
- Sensing and diagnostics of Industrial Applications (e.g., Machinery, workshop, supply chains)
- Substructure protection (e.g., power grids, water distribution)
- Battlefield awareness (e.g., multitarget tracking)
- Context-aware computing (e.g., intelligent home, responsive environment)

As the above applications have illustrated, there are a number of sensing functionalities exist that require a sensor network system to process data with cooperation

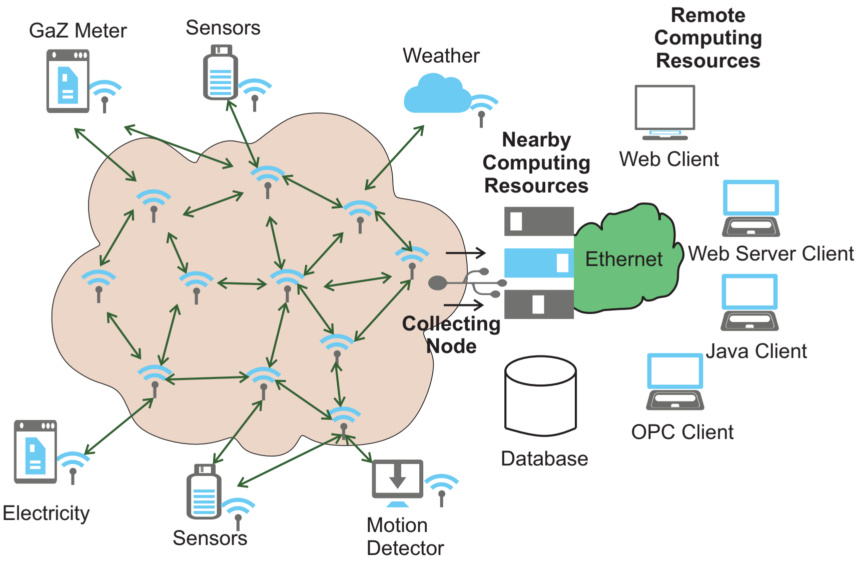


FIGURE 1.2: *Deployment of Wireless Sensor Networks*

of nodes after combining information from multiple sources. In the traditional centralized sensing and signal processing systems, raw data collected by sensors are relayed to the edges of a network where the data is processed. From the scalability aspect, the non-local processing at the edges depletes precious bandwidth. If every sensor has some data that it needs to send to another node in a network, then a wireless capacity result states that the per node throughput scales as $\sqrt{\frac{1}{N}}$ in other words, it goes to zero as the number of nodes N in a wireless sensor network increases [10]. This result holds even though the optimality is provided in routing, power control, or transmission. Intuitively, this is also interpreted as the number of nodes increases, every node spends almost all of its time forwarding packets of other nodes which actually decreases the significance of the WSNs. From the energy point of view, transmitting raw data to distant nodes or only to the boundary nodes is an insignificant process that exhausts the valuable energy resources. Such exhaustion of resources and the diminishing wireless capacity are controlled by introducing mobility to nodes but these applications need to be delay-tolerant [13].

Generally centralized systems have plenty of privileges regarding resources and implementation techniques. But a WSN is constrained by a set of limitations such as finite battery power and limited transmission bandwidth. In a typical sensor network, each sensor node operates untethered and has a microprocessor and a small amount of memory for signal processing and task scheduling. Each node is also configured with one or more sensing devices such as acoustic microphone arrays, video or still cameras, infrared, seismic, or magnetic sensors. Each sensor node communicates without any wired media with a few other nodes within its transmission range. Sensor networks extend the existing internet deep into the physical environment. Information collected by and transmitted on a sensor network describes conditions of physical environments for example, temperature, humidity, or vibration and requires advanced query interfaces and search engines to effectively support user-level functions as shown in Figure1.2. Sensor networks may work with an Internet Protocol (IP) core network via a number of gateways. A gateway node makes a proper route to transmit the required information to appropriate nodes in a sensor network. It also routes sensor data, at times aggregated and synchronized, to users who have requested for it or are expected to use the information. A data repository or storage service may be present at the gateway, in addition to data logging at each sensor.

Thus, minimizing the amount and range of communication as much as possible through local collaboration among sensors, removing duplication, or invoking only the nodes that are relevant to a given function can increase the lifetime of a sensor network. In different critical WSNs, it creates trouble to adapt with rapid changes of nodes due to fast depletion of resources. This actually also degrades the performance of the network. Therefore, from implementation point of view, the shorter radio frequency transmission range is beneficial to improve spectrum usage. This increases throughput for a sensor network. The information management and networking for this network requires more than just building faster routers, switchers, and browsers. A sensor network is implemented to collect information from a physical environment. Networking will be intimately coupled with the needs of sensing and control, and hence the application semantics. To optimize for performance and resources such as energy, one has to consider the existing Transmission Control Protocol/Internet Protocol (TCP/IP) stack and design an appropriate sensor network to support the required application. For example, in many applications, it is more appropriate to address nodes in a sensor network by physical properties, such as node locations or proximity, than by IP addresses. The process of data generation is executed by sensors and consumed by users. This is having an impact on the way the data is compressed, routed, and / or aggregated. Because of the peer-to-peer connectivity and the lack of a global infrastructure support, the sensors have to rely on discovery protocols to construct local models about the network and environment. Mobility and instability in wireless links prohibits the use of many existing edge-network gateway protocols for internetworking IP and sensor networks. To summarize, the challenges [6][7] we face in designing sensor network systems and applications include:

- Limited hardware: Each node has limited processing, storage, and communication capabilities, and limited energy supply and bandwidth.
- Limited support for networking: The network is peer-to-peer, dynamic, mobile, and unreliable connectivity. Each node acts both as a router and also as a data generator.
- Limited support for software development: The tasks are typically real-time and massively distributed, involving dynamic collaboration among nodes, and multitasking scenarios.

According to the different application aspects of WSNs, localizing and tracking moving stimuli or objects is an essential capability for the entire sensor network. Tracking exposes the most important issues surrounding collaborative processing, information sharing, and group management including which nodes should sense, which have useful information and should communicate, which should receive the information and how often, and so on. Moreover, in a dynamically evolving environment such localization and tracking the objects a major challenge too. This tracking scenario raises a number of fundamental information processing issues in distributed information discovery, representation, communication, storage, and querying as given below.

- In collaborative processing, WSNs face the problem of target detection, localization, tracking, and sensor tasking and control
- In networking, the problem occurs at data naming, aggregation, and routing

- In databases, the limitations are of data abstraction and query optimization
- In human-computer interface, the issues include data browsing, search, and visualization
- In infrastructure services, the issues of network initialization and discovery, time and location services, fault management, and security

The progressive advances of Micro-Electro-Mechanical Systems (MEMS), computing and communication technology have increased the need of distributed WSNs that consist of number of sensor nodes. Each node is able to sense the network environment, perform simple computations and communicate with its other sensors or to the central unit. One way of deploying the sensor networks is to distribute the nodes throughout the region of interest. This makes the network topology random. This randomness in the network is ad hoc as there is no a priori communication protocol,. These networks are tremendously being implemented to perform a number of tasks, ranging from environmental and natural habitat monitoring to home networking, medical applications and smart battlefields. Sensor network also works as a alerting or detection system because it can signal a systems malfunction to the control centre in a factory or it can warn about smoke on a remote forest hill indicating that a forest fire is about to start. On the other hand wireless sensor nodes can be designed to detect the ground vibrations generated by silent footsteps of a burglar and trigger an alarm.

Since most applications depend on a nodes localization in some fixed coordinate system, it is of great importance to design efficient localization algorithms. In large scale wireless sensor networks, node localization can assist in routing [14][15][16]. Smart kindergarten [17] , hospital environments [14] and many more, node localization is used to monitor the progress of the children or the patients. For these advantages, the domain of node localization in WSNs is an active and developing field of research in wireless networking. The easiest solution for the calculation of nodes position is to configure the Geographical Positioning System (GPS) with all the nodes. But, for a huge network with large number of sensor nodes, this solution of adding GPS to all nodes is not feasible because:

- GPS enabled applications are not tolerant for obstacles as GPS applications require the line-of-sight communication.
- The power consumption by GPS will reduce the battery life of the sensor nodes which will eventually lead to reducing the effective lifetime of the entire network.
- In a network with large number of nodes, the production cost factor of GPS is an important issue.
- Sensor nodes are required to be small. But the size of GPS and its antenna increases the sensor node form factor.

For these reasons an alternate solution of GPS is required which is cost effective, rapidly deployable and can operate in diverse environments.

Whenever, we talk about the network, the easiest and most understandable way of the network representation of network, it is the graph theory where each sensor or anchor node is represented as round vertex and the communication between two nodes is represented by a directed or undirected link. Moreover, a backbone is required to ensure connectivity in wireless networks. Since the nodes themselves act as routers in this infrastructure less wireless sensor network, the backbone is virtual [18]. A WSN can be modeled using Unit-Disk Graph (UDG), where hosts in wireless network are represented by vertices and unit distance corresponds to transmission range. The connectivity can be ensured by a Connected Dominating Set (CDS) in UDG [19][20][21] and establishes a virtual dynamic infrastructure. The CDS problem is defined as follows. Given a graph G(V,E), find a subset S of vertices, such that the sub-graph induced by S is connected and S forms a dominating set in G. Finding a CDS in a unit-disk graph is, however, an Non Polynomial (NP)-hard problem [22][23] and heuristics usually lead to a sub-optimal solution. To achieve a near optimality in the resource constrained environment, a heuristic endeavours to, (i) keep the formation process simple by considering only local information and small number of message exchanges among neighbors (ii) the resultant dominating set should contain minimum number of nodes. A Connected Dominating Set with minimum cardinality is called

Minimum Connected Dominating Set (MCDS) [24]. Minimizing the cardinality results in shorter routes that ultimately increases the network capacity.

## 1.3 Researcher's Contribution

The researchers contribution in this area is illustrated by the flow chart given in Figure 1.3 and is summarized as follows:

### 1.3.1 One hop neighbourhood based MCDS construction

This first method in the proposed algorithm utilizes the work [25] to create backbone of anchor nodes. A set of anchor nodes and a set of unknown nodes are initialized. Maximum degree of the anchor nodes for anchor node set is calculated. The anchor node having the maximum degree of connectivity becomes a member of the dominating set. The process continues till either the entire anchor nodes are the member of dominating set or all the unknown nodes are one hop neighbor of any anchor node that is a member of dominating set and the number of anchor nodes in the dominating set is greater than equal to three. The number of anchor nodes for dominating set should be more than three as to perform trilateration. Finally, pruning method is used to reduce the size of dominating set such that all the unknown nodes are covered up by the minimum number of anchor nodes. Thus, once MCDS is constructed, trilateration is applied on anchor nodes to get the location estimation of unknown nodes.

### 1.3.2 Optimized load balanced localization method

The anchor nodes in the MCDS are not equally load distributed as some anchor nodes have more one-hop neighbour unknown nodes as compared to others. This may

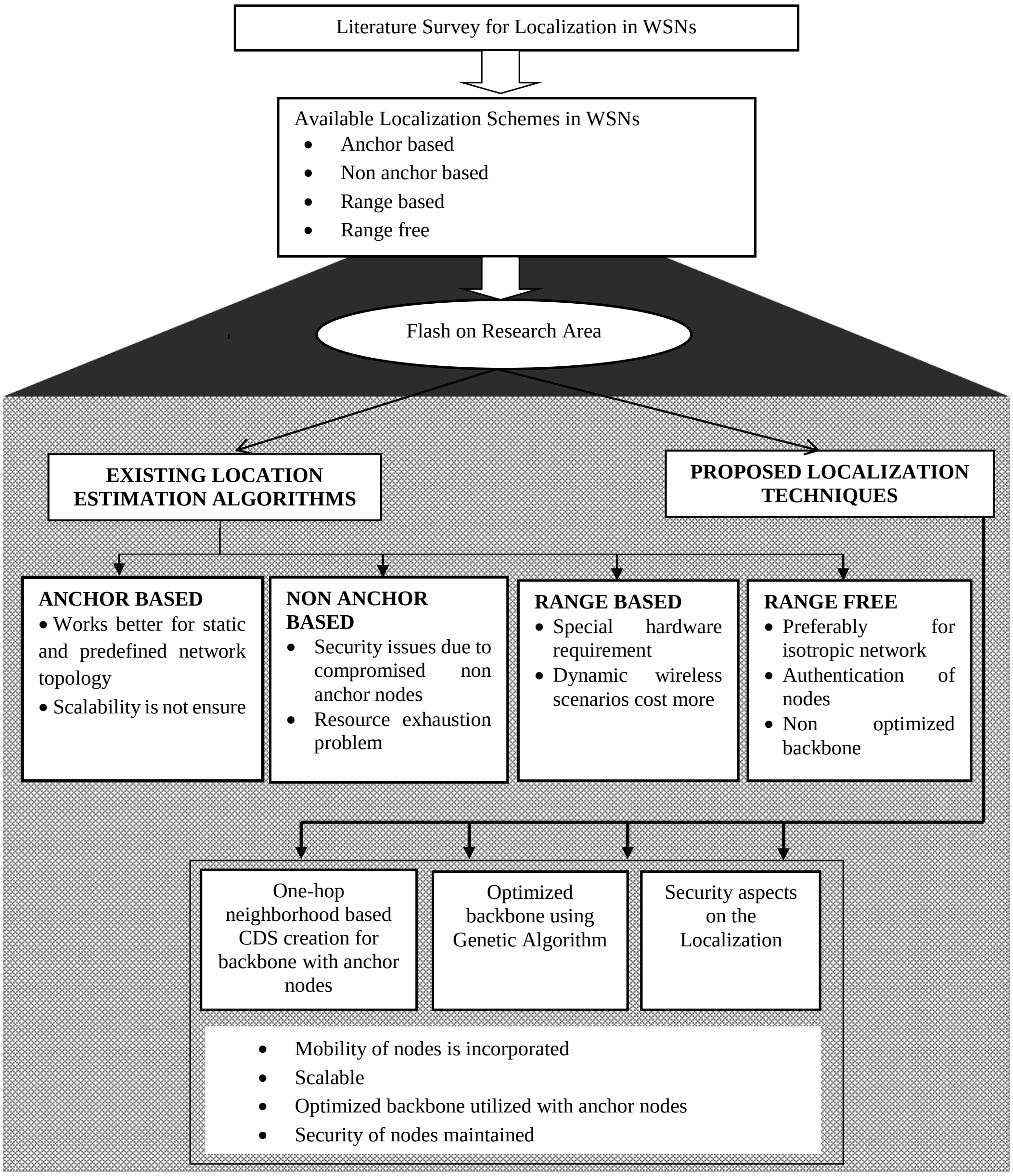

Literature Survey for Localization in WSNs
Available Localization Schemes in WSNs
• Anchor based
• Non anchor based
• Range based
• Range free
Flash on Research Area
EXISTING LOCATION ESTIMATION ALGORITHMS
PROPOSED LOCALIZATION TECHNIQUES
ANCHOR BASED
• Works better for static and predefined network topology
• Scalability is not ensure
NON ANCHOR BASED
• Security issues due to compromised non anchor nodes
• Resource exhaustion problem
RANGE BASED
• Special hardware requirement
• Dynamic wireless scenarios cost more
RANGE FREE
• Preferably for isotropic network
• Authentication of nodes
• Non optimized backbone
One-hop neighborhood based CDS creation for backbone with anchor nodes
Optimized backbone using Genetic Algorithm
Security aspects on the Localization
• Mobility of nodes is incorporated
• Scalable
• Optimized backbone utilized with anchor nodes
• Security of nodes maintained

Figure 1.3: *Research methodology*

lead to the fast resource drainage of particular anchor nodes and the network lifetime will decrease. To mitigate this problem, we have designed the optimized localization algorithm. The optimization process uses the genetic algorithm with elitism strategy so that the fittest solution can be retained accordingly for a fast convergence of the global solution. Obtaining the optimized CDS, the localization process executed that depends upon proximity matrices and transformation function. Finally, standard least square method is applied to get the estimated location of the unknown nodes. As the major calculations are taken care by the anchor nodes, the network lifetime is increased in the proposed algorithm.

### 1.3.3 Secured Localization method

Localization process deals with critical information about the sensor nodes which needed to be secure. A number of attacks are executed against the localization process in wireless sensor networks. To prevent such risks, a secured localization algorithm has been developed. This algorithm is having two phases: the first phase deals with the distribution of certificated and keys by the base station and second phase estimates the distance. Finally, Minimum Mean Square Error (MMSE) is applied to calculate the location of unknown nodes. The algorithm also validates the estimated distance so that it can detect the compromised insiders.

## 1.4 Organization of the thesis

The thesis is organized in seven chapters. A brief outline of the chapters is given below.

*Chapter 1* introduces to the domain of wireless networks leading to the basic information and working of WSNs. It highlights some of the key points in this domain and also gives brief about the application oriented development of WSNs. Authors contribution has also been highlighted in this chapter.

*Chapter 2* presents the detailed discussion of localization process. The categorization of manual and GPS based, range-based vs range-free have also been shown. Different computational techniques are also discussed in this chapter.

*Chapter 3* shows the recent research work by different researchers in this domain. Firstly, the detailed applications of WSNs are discussed. Secondly, as per the authors objective, the literature review work has been segmented in four categories: backbone creation, improvements of DV-hop algorithm, optimization of backbone and security in localization algorithms. Various research works related to these categories are analyzed.

*Chapter 4* proposes a novel algorithm for backbone creation in WSNs using MCDS properties. Along with the proposed algorithm, the network model is also discussed. The simulation of the algorithm and the results are thoroughly analyzed.

*Chapter 5* proposes a novel algorithm of optimizing a backbone using genetic algorithm, so that the backbone can have minimum anchor nodes. Different stages of genetic algorithm have been discussed with reference to the proposed algorithm. Results of the simulation are also analyzed in the chapter.

*Chapter 6* proposes a novel algorithm of securing the localization process using authentication and insider node validation. The use of keys and the signal transmission timings are taken into account. Various attacks are also described here. The results of the algorithm are analyzed with proper analysis.

*Chapter 7* concludes the thesis highlighting the prime outcomes of the current research of the author and significant contribution of the thesis and also notifies about the scope for future research in this area.

# CHAPTER 2

# Localization in Wireless Sensor Networks

## 2.1 Introduction

Localization [26][27] defines the calculation of the location or position of ad hoc nodes. As the ad hoc networks are dynamic in nature, this localization of nodes is also changeable. Thus the radical and frequent change of position of nodes makes it very sensitive for the ad hoc networks. The knowledge of the physical location of a network entity is always beneficial to execute new applications and services. Such information will also help to find critical resources and will improve the security of wireless networks. In addition knowledge of the location of entities in a wireless network makes it possible to perform existing functions more efficiently. For example, in a courier service, the landmark of the recipient is essentially needed to search the receivers location. It also takes less time to find the receiver using this landmark.

There are three basic advantages of knowing the location information of sensor nodes. First, location information is required to estimate the location of an event of interest.

For instance, the location of an intruder, the location of a fire, or the location of enemy tanks in a battlefield are of critical importance. Second, location awareness of the applications emphasizes numerous application services[71], such as location directory services that provide doctors with the information of nearby medical equipment and personnel in a smart hospital, target-tracking applications for locating survivors in debris, or enemy tanks in a battlefield. Third, location information can assist in various system functionalities, such as geographical routing network [28] coverage checking , and location-based information querying . Hence, with these advantages and much more, it is but natural for location-aware sensor devices to become the defacto standard in ad hoc networks in all application domains that provide location-based service.

Location information is also required in the routing process. Location Aided Routing (LAR)[29], (Greedy Perimeter Stateless Routing (GPSR)[30] and Distance Routing Effect Algorithm for Mobility (DREAM)[31] have shown performance improvement over routing protocols that do not consider location information. These protocols take decisions for data forwarding based on the location information of the neighbors as well as the destination node. As a result the geographic location based routing protocols provide low overhead. This leads to conservation of resources. Further, these protocols do not require that nodes maintain information on a per-hop basis. The information about the location of the neighbours combined with location information about the destination is sufficient to route the packets. Even traditional routing protocols benefit tremendously when provided with location information. The main component of this localization process deals with beacon nodes, sometimes this has been also referred also as anchor locator or seed nodes. The beacons nodes are GPS enabled and privileged with different multi functionality and resources. Using the location information of these beacons, other nodes compute their location as required. This geographic location information has also been implied in multicast routing which gives better performance. In sensor networks, Geographic Hash Table (GHT)[32] is used as centralized data storage which is also based on location information. Besides, the target tracking, environment monitoring, and different security mechanisms are also implied based on geographic location information. It is important to notice here that these location-based applications, services, and security mechanisms are sensitive to the accuracy of the location information. Localization errors due to accidental and not malicious reasons affects the performance of the geographic location based routing protocols. Localization process is also vulnerable to error which leads to incorrect behavior of the application services and eventually degrades the performance. It is necessary to configure the localization process in such a way so that it can be robust against statistically inaccurate information though there is the presence of adversary. The inaccurate information eliminates the benefits of localization process in different applications. It is also very critical to conclude that the applications such as data aggregation and target tracking will also suffer if the adversary modifies the location information.

Errors in the estimated [33][34]location of a sensor can be two types. Intrinsic errors are most often caused by the nodes' hardware and software problem, and can create many complications when estimating node positions. Extrinsic errors deal with the physical effects on the measurement channel including shadowing effects, changes in signal propagation speed, obstacles, etc. Extrinsic errors are not predefined, therefore difficult to handle. Measurement errors in a single sensor can significantly emphasize in the further process of estimation of the location. Also, use of lower-precision measurement technology along with higher uncertainty of beacon locations add-on errors in position estimates. Apart from the accuracy aspect, two more considerations are there that need to be addressed always for localization: energy efficiency and security. As security is a key metric, from the point of security, sensor networks are susceptible to the adversaries in a very general way. Attackers are two types: internal and external. It is very easy for an adversary to misrepresent the location to breach the security measures implemented. Therefore, it is also recommended that the localization techniques should be secured enough[35]. The secure location determination techniques should prevent both malicious insider nodes from misrepresenting their location or getting compromised under outsiders' control and outside entities from interfering with the location determination process being followed by the system. The security requirements for localization techniques must provide with privacy of the location determined, location information only by authorized sources, integrity of the location information, information availability to compute proper location, non-repudiation of the location information by sender or receiver.

## 2.2 Categories of Localization

Localization is the process by which ad hoc nodes determine their location. It can also be defined as a mechanism for discovering spatial relationships between nodes. The problem of localization has been solved [159] by various approaches which states different set of assumption device hardware, timing and energy requirements, signal propagation models, composition of network viz homogeneous vs. heterogeneous, operational environment viz indoor vs. outdoor, beacon density, time synchronization, communication costs, error requirements, and node mobility. The localization process is a conjugation of two related stages. In the first stage, a node simply evaluates its separation to different nodes in its region utilizing at least one feature of the received signal flag. In the second stage, a node uses all the distance estimates to compute its actual location. The method employed in stage two to compute the actual location depends on the signal feature used in stage one. Localization techniques are broadly classified [37][38] into two categories: Direct approaches and Indirect approaches.

### 2.2.1 Direct approaches

This approach is also known as absolute localization. The direct approach[39] can be further classified into two types: First is Manual configuration and second is GPS-based localization[40][41]. The manual configuration method is hard to maintain and expensive too. It is neither practical nor scalable for large scale of mobile network. In the GPS-based localization method, each node is equipped with a GPS receiver shown in Figure 2.1. This method adapts well for node mobility. However, there is a drawback of this method. It is not economically feasible to equip each node with a GPS receiver. In case of sensor networks, this also increases the size of each sensor, rendering them unfit for pervasive environments. Besides, the GPS receivers only work well outdoors on earth and have line-of-sight requirement constraints.

### 2.2.2 Indirect approaches

The indirect approach[36] of localization is also termed as relative localization since nodes position themselves relative to other nodes in their neighbourhood. In this approach, a small subset of nodes in the network, called the beacon nodes or reference points, are either equipped with GPS receivers to compute their location or are manually configured with their location. These beacon nodes then send beams of signals providing their location to all other general nodes in their vicinity that dont have a GPS receiver. Using the transmitted signal containing the location information, general nodes compute their location. This approach effectively reduces the overhead introduced by the GPS-based method. Though indirect approach eliminates the drawback of overhead due to GPS system, it includes the problem of security threat. The reason for security problem in indirect approach is in the environment of hostility and the reference nodes. It may happen that both of them reside in the same environment and the adversaries can easily physically capture the reference nodes by some means. So, to use the indirect approach it is necessary to consider the security issues for the reference nodes.

Indirect localization approach can be further categorized into two classes: Range-based and Range-free.

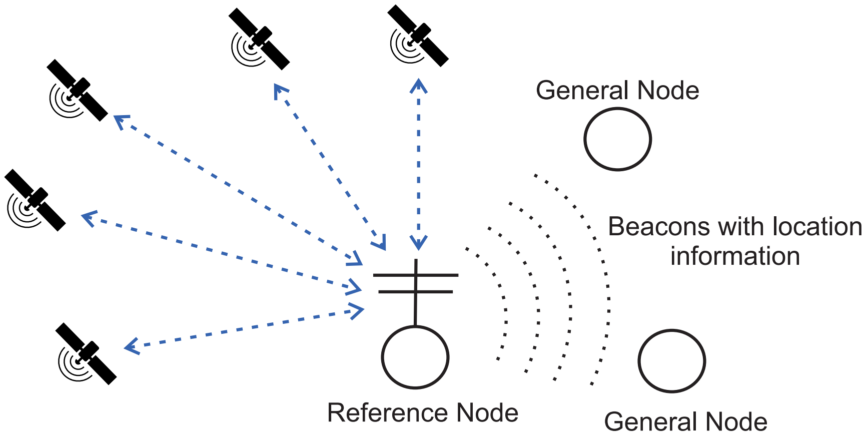


FIGURE 2.1: *Localization with GPS*

#### 2.2.2.1 Range-based Techniques

Range-based approaches[42] depend on calculating the location of a node relative to other nodes in the vicinity. It depends on the assumption that the absolute distance between a sender and a receiver node can be accurately calculated by some physical properties of the signal transmission and the surroundings such as Time of Arrival (ToA), Time Difference of Arrival (TDoA), Received Signal Strength Indicator (RSSI), or Angle of Arrival (AoA). In AoA, range information is obtained by estimating and mapping relative angles between neighbours. Received Signal Strength Indicator use a theoretical or empirical model to translate signal strength into distance. RAdio Detection And Ranging (RADAR)[42][43] is one of the first to make use of RSSI. To obtain range information using ToA, the signal propagation time from source to destination is measured. A GPS is the most basic example that uses ToA. To obtain the range information using TDoA, an ultrasound is used to estimate the distance between the node and the source. Range based approaches includes the following types

**Time-of-Flight Techniques** The basic concept behind time-of-flight techniques[165] is the direct relationship linking the distance between two points and the time needed for a signal to propagate between these two points. Time needed depends on the propagation speed of the signal. The distance between the points can then be estimated by measuring the time needed and multiplying this by the speed of propagation. The time needed for the signal to propagate from sender to receiver is called time of flight. Time-of-flight technique can be used with several underlying technologies such as visible light, infrared, radio frequency, and ultrasound. This technique can be used in two modes, one-way and two-way. In the one-way mode the sender transmits a single bit (signal) while the receiver measures the time at which the bit was received. The receiver can then compute the distance between the two. Here the sender will not be able to compute the distance unless the sender gets the time-of-flight information from the receiver. This needs time synchronization between the sender and the receiver. In case of the two-way mode, the sender transmits a single bit (signal) and the receiver is expected to reflect back the bit towards the sender as soon as the receiver receives the bit. The sender thereby measures the time taken for the round trip and uses this to compute the distance between the two. In this case the receiver cannot compute the distance. While the two-way mode does not require that the sender and receiver be synchronized in time, it does require that the receiver be able to reflect back the bit without any delay. A sequence of bits might be used in both these modes.

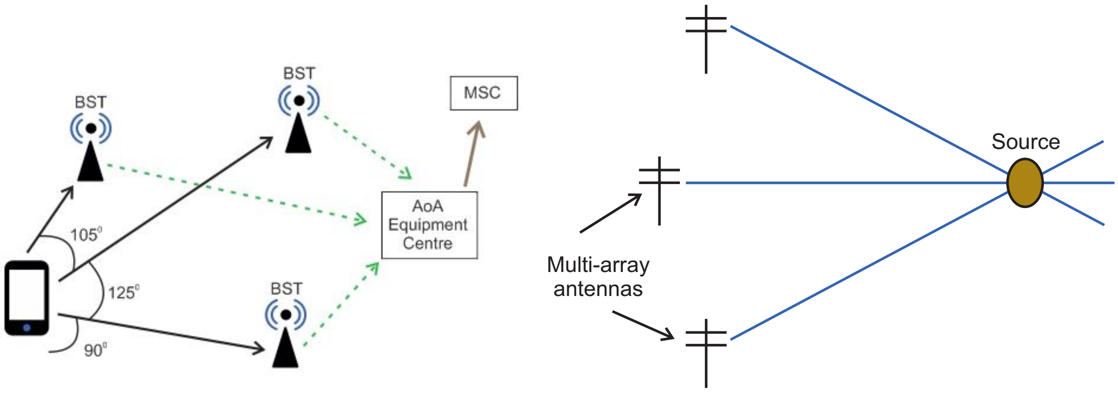
**Received Signal Strength Techniques** Location identification based on inferring the distance from the signal strength have also been introduced [44]. The underlying principle here is that signal strength changes as a function of the distance. One approach defines that the distance can be estimated based on the transmitted and received signal strengths at each of the nodes. This could be achieved by having either of nodes report on the transmitted or received power levels to the other node. The distance can then be estimated using the values of these power levels along with a theoretical model. Another approach involves the usage of empirical models. In this case the signal strength at various locations is measured in offline state and a signal strength map prepared. During the operation of the system in online state, the node that has access to such an Signal Strength map can measure the signal strength of the other node. Using this map, the node can then estimate the actual location of the other node by determining the value of the location that has the closest SS measurements.

Both these approaches suffer from inaccuracies due to multipath fading, interference, irregular signal propagation characteristics and more. An attacker can also make use of these properties to easily fool the system.

**Radio Interferometric Positioning System** Radio Interferometric Positioning System (RIPS) proposes to use two transmitters which are transmitting at frequencies that are nearly equal[45]. The interference caused by these two signals results in a composite signal that has a low frequency and whose envelope signal can be measured using the RSSI indicator on low precision Radio Frequency chips. It also includes the usage of two receivers to calculate the relative phase offset of the composite signal at the two receivers. This relative phase offset between the two receivers depends only on the four distances between the two transmitters and two receivers. By using relative phase offsets calculated at different frequencies, RIPS provides a method to calculate the relative positions of the transmitters and the receivers. The security aspect of RIPS is under research concern.

**AoA techniques** In AoA, a mobile device's signal is received by multiple base stations[46][47]. The Base Stations (BSTs) have additional equipment that determines the compass direction from which the user's signal is arriving. Each base station propagates the information to the Mobile Switch Centre (MSC), where it is examined, analyzed and used to generate an approximate latitude and longitude for the mobile device shown in Figure 2.2(a). AoA methods utilize multi-array antennas and try to estimate the direction of arrival of the signal. Thus a single AoA measurement cannot estimate the source location along a line in the estimated AoA.

If at least two such AoA estimates are available from two antennas at two different locations, the position of the signal source can be located at the intersection of the lines of bearings from the two antennas shown in Figure 2.2(b). Usually multiple AoA estimates are used to improve the estimation accuracy by using the redundant information. Although AoA methods offer a practical solution for wireless position location, they have certain drawbacks. For accurate AoA estimates, it is crucial



(a) Schematic diagram of AoA technique

(b) Source location estimation with multi-array antennas

FIGURE 2.2: *AoA Techniques*

that the signals coming from the source to the antenna arrays must be coming from the Line-of-Sight (LoS) direction. Another factor which is the considerable cost of installing antenna arrays.

**TDoA techniques** TDoA techniques emphasize on estimating the difference in the arrival times of the signal from the source at multiple receivers[48][49]. This is usually calculated in a particular time interval by the arrival of signal at a synchronized time period at multiple receivers. A particular value of the time difference estimate defines a hyperbola between the two receivers on which the mobile may exist, assuming that the source and the receivers are coplanar as shown in Figure 2.3. Another hyperbola is created if this procedure is done again with another receiver in combination with any of the previously used receivers, and the intersection of the two hyperbolas results in the estimated position location of the source.

This method is also sometimes called a hyperbolic position location method. Since, all the processing takes place at the infrastructure level, no modifications are needed in the existing mobile devices. This approach is more cost effective than a GPS-based solution. Since this technique does not require any special type of antennas, it is cheaper to put in place than the Difference of Arrival (DoA) methods. It can also provide some immunity against timing errors if the source of major signal reflections is near the mobile. If a major reflector effects the signal components going to all

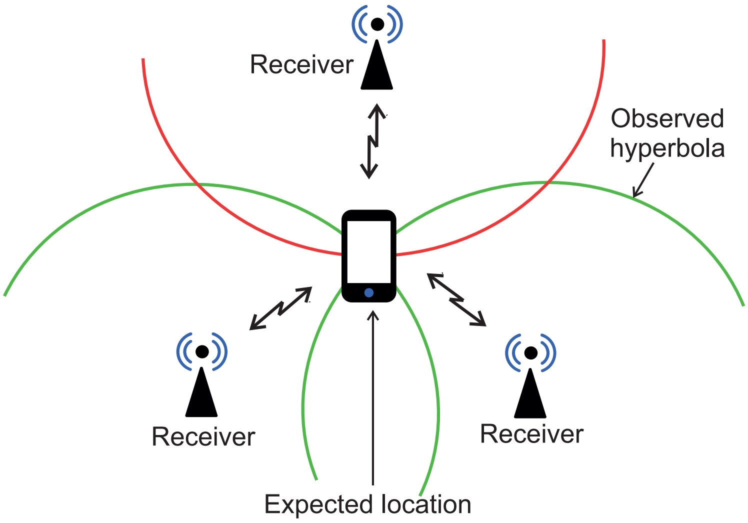


FIGURE 2.3: *TDoA Technique*

the receivers, the timing error may get canceled or reduced in the time difference operation. Hence, TDoA methods may work accurately in some situations where there is no LOS (Line of Sight) signal component. In this respect, it is superior to the DoA method.

#### 2.2.2.2 Range-free Techniques

Range-free localization is another category of ranging techniques to estimate localization. It does not deal to establish a direct relationship between point-to-point distance based on received signal strength or other features of the received communication signal like time, angle, etc. This approach greatly simplifies the design of hardware, making range-free methods a cost-effective alternative for localization in ad hoc and sensor networks. Amorphous localization[50] , Centroid localization[51] , Approximate Point in Triangulation (APIT)[52] ,Distance Vector-Hop (DV-Hop) localization[53] are some examples of range-free localization techniques. All these techniques either or includes hop count, neighbour location identification and region inclusion.

**Hop-count based schemes** In this scheme several anchor or beaconing nodes are engaged[54][142][55]. The beaconing from anchor nodes is flooded through the network. The beacons contain the information about the location of the anchor nodes and a parameter called hop count which is initialized to one. Each node that receives this beacon copies the value of the hop count from the source of the beacon , increments the hop count value by one and transmits further, as shown in Figure 2.4. Beacons from the same source that are received with a higher hop count value than that maintained by the node are ignored. Now when hop count is estimated, it is the step for calculating physical distance. For this, average distance per hop is used. Average distance can be calculated by the location information and hop counts of all the anchor nodes. Once a node has the estimated distance from three or more anchors, it uses trilateration to estimate its own location. For example, DV-hop localization[54] uses this scheme. Hop-count based scheme is a matter of security concern as the attackers (internal or external) can be misguide the calculation of hop counts by creating wormhole, black-hole region or by increasing or decreasing the transmitting power.

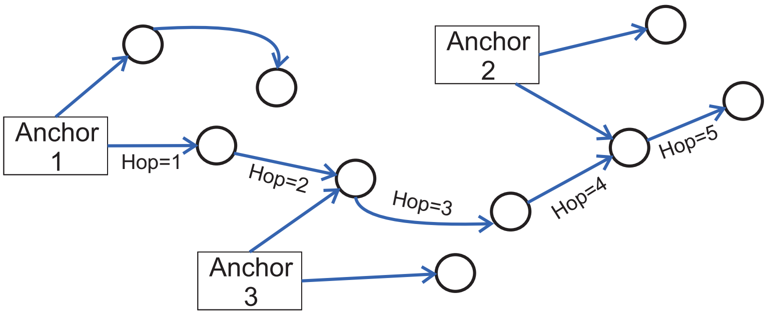


FIGURE 2.4: *Basic structure and functioning of Hop-count based scheme*

**Neighbour Location** The neighbour location [56][36] schemes imply the centroid calculation of the locations of the anchor nodes from which they receive the beacons. It is assumed here that wireless devices are uniformly distributed. The main advantages of this scheme are its simplicity, low overhead and ease of implementation. Centroid localization uses this approach. The drawback is that it can lead to very coarse-grained location determination. This scheme can also be affected by some security attacks like jamming, biased location, modifying the radio region and so on.

**Region Inclusion** In this scheme, the area of the network is divided into some triangles where each vertex comprises of anchor node[57][58][59]. The general nodes of the network select three anchor nodes from the list of anchors from which they were receiving beacons and tests whether the node is inside the region of the triangle, if the triangle can be created by joining the three anchor nodes. The test consists of the node checking the signal strengths at all its neighbors of the three locators that form the vertices of the triangle. A node is determined to be further away if its signal strength is smaller. If no neighbor of the node is further from or closer to all the three anchors simultaneously, then the node assumes that it is inside the triangle. Otherwise, the node assumes that it is outside the triangle. This process of test is repeated with different combinations of anchors until either all the combinations are exhausted or the required accuracy is achieved. The center of gravity of the intersection of all the triangles that a node resides in is assumed to be the estimated location of the node as shown in Figure 2.5.

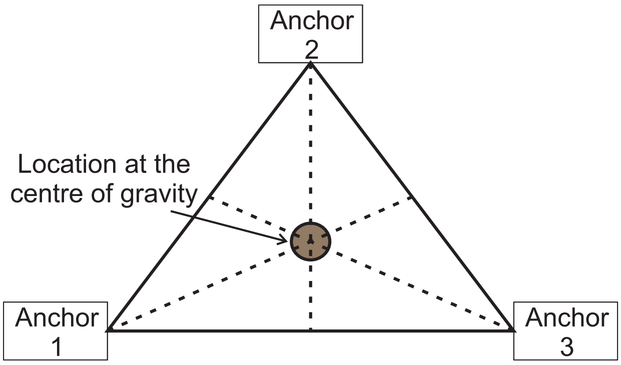


FIGURE 2.5: *Region Inclusion scheme*

## 2.3 Computation

From the discussion above about the various categories of the localization techniques, we can see that every technique shown there needs some kind of calculation to estimate the location of the sensing node. This calculation is done by the general nodes or anchor nodes based on the information gathered during the ranging phase. There are several ways to perform this calculation.

### 2.3.1 Trilateration

Trilateration is a type of measurement used to determine the location of a point by using the geometry of spheres, circles, or triangles[60][61][62]. Unlike triangulation, which uses the measurement of angles to determine location, trilateration uses measures of distance. For example, a GPS receiver uses trilateration (a more complex version of triangulation) to determine its position on the surface of the earth by timing signals from three satellites in the Global Positioning System. Let us consider a problem. Suppose, a node $N$ has determined its distances from other nodes say A, B, C and so on where the co-ordinates of the nodes are known say: A($x_1$, $y_1$), B($x_2$, $y_2$), C($x_3$, $y_3$) and so on. Trilateration says to find the co-ordinates information of the node $N$ with help of above information. Non-linear least squares and circle intersections with clustering are the two methods that can be done to solve the above trilateration problem.

#### 2.3.1.1 Non-linear least square

From the given information, we can formulate the following equations to show the relation between the coordinates of $N$, and other nodes' coordinates and distances of $N$ from the other nodes[63][64].

$$(N_x - A_x)^2 + (N_y - A_y)^2 - {A_r}^2 = 0 \tag{2.1}$$

$$(N_x - B_x)^2 + (N_y - B_y)^2 - {B_r}^2 = 0 \tag{2.2}$$

$$(N_x - C_x)^2 + (N_y - C_y)^2 - {C_r}^2 = 0 \tag{2.3}$$

Where, $A_r$, $B_r$, $C_r$ are the radius of the range of the node A, B and C respectively. The only variables that we need to calculate is $N_x$ and $N_y$ which can be considered as overestimated as number of variables to be determined are less than the number of the equations. In this situation, unique solution is not feasible. Therefore, we are applying least square as it gives the unique solution. Now replacing the right hand side zeros of the above three equations by some non-zero residuals, we can rewrite the equations as follows:

$$(N_x - A_x)^2 + (N_y - A_y)^2 - {A_r}^2 = {A_\delta}^2 \tag{2.4}$$

$$(N_x - B_x)^2 + (N_y - B_y)^2 - {B_r}^2 = {B_\delta}^2 \tag{2.5}$$

$$(N_x - C_x)^2 + (N_y - C_y)^2 - {C_r}^2 = {C_\delta}^2 \tag{2.6}$$

The least squares solution is the unique solution $(N_x,\ N_y)$ that minimizes the sum of the squares of the residuals $(A_\delta^2 + B_\delta^2 + C_\delta^2 + ....)$. The system of above equations is also non-linear in parameters of $(N_x, N_y)$ because of squared terms in the equation.

#### 2.3.1.2 Circle Intersection with Clustering

Suppose there are three nodes A, B, C in the vicinity of a location sensing node say N as shown in Figure 2.6. Draw circles of radius $A_r,\ B_r\ and\ C_r$ around node A, B and C respectively. As, the radius of the circles are not predefined it is feasible that the circles intersect each other in a small region rather in intersecting points. The undefined node (location sensing node) N must be somewhere in this intersecting region or in the circles of the defined nodes of A, B and C.

Here is one way to find the cluster[65][66][67]. Compute the distance between each pair of circle intersection points. To do this we need to calculate the coordinates of the intersection points. First, let us find the distance between the centers of the circles; say $\triangle$ which can be calculated as follows:

$$\triangle_x = B_x - A_x \tag{2.7}$$

$$\triangle_y = B_y - A_y \tag{2.8}$$

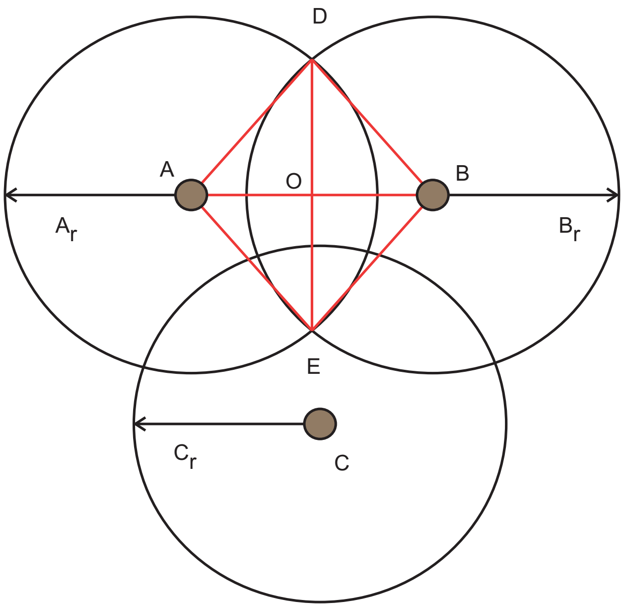


FIGURE 2.6: *Circle Intersection with Clustering*

Where $(A_x, A_y)$ is the coordinates of point A and $(B_x, B_y)$ is the coordinates of point B. Now,

$$\triangle^2 = \triangle_x^2 + \triangle_y^2 \tag{2.9}$$

$$\triangle = \sqrt{\triangle^2} \tag{2.10}$$

If, $\triangle > A_r + B_r$, then the circles do not intersect each other and if $\triangle < B_r - A_r$, it means that one circle is inside the other. We now need to find the coordinate of the point O $(O_x, O_y)$. Let $d_1$ be the distance AO and $d_2$ be the distance OB and $d_3$ is the distance of OD (OE as OD = OE). Then,

$$d_1{}^2 + d_3{}^2 = A_r{}^2 \tag{2.11}$$

$$d_2{}^2 + d_3{}^2 = B_r{}^2 \tag{2.12}$$

Subtracting the above two equations, we can get:

$$d_1{}^2 - d_2{}^2 = A_r{}^2 - B_r{}^2 \tag{2.13}$$

expanding the above equation

$$(d_1 + d_2)\ (d_1 - d_2) = {A_r}^2 - {B_r}^2 \tag{2.14}$$

Since $d_1 + d_2 = \triangle$ and $d_2 = \triangle - d_1$, we can write the above equation as:

$$(d_1 - (\triangle - d_1))\triangle = {A_r}^2 - {B_r}^2 \tag{2.15}$$

$$2d_1\triangle - \triangle^2 = {A_r}^2 - {B_r}^2 \tag{2.16}$$

$$d_1 = \frac{(\triangle^2 + {A_r}^2 - {B_r}^2)}{2\triangle} \tag{2.17}$$

Now, the coordinates of point O are:

$$O_x = \frac{A_x + \triangle_x d_1}{\triangle} \tag{2.18}$$

$$O_y = \frac{A_y + \triangle_x d_1}{\triangle} \tag{2.19}$$

Finally, we can calculate the intersection points D and E. We have, $d_3 = \sqrt{{A_r}^2 - {d_1}^2}$. Then the coordinates of point D are:

$$D_x = \frac{O_x - \triangle_y d_3}{\triangle} \tag{2.20}$$

$$D_y = \frac{O_y + \triangle_x d_3}{\triangle} \tag{2.21}$$

$$E_x = \frac{O_x + \triangle_y d_3}{\triangle} \tag{2.22}$$

$$E_y = \frac{O_y - \triangle_x d_3}{\triangle} \tag{2.23}$$

Thus, we can have the coordinates of all the intersection points; take the two closest intersection points to be the initial cluster. Compute the centroid of the cluster. The centroid's $x$ coordinate is the average of the $x$ coordinates of the points in the cluster; the centroid's $y$ coordinate is the average of the $y$ coordinates of the points in the cluster. Next, find the circle intersection point that is closest to the cluster centroid. Add this intersection point to the cluster and re-compute the cluster centroid. Continue in this way until k intersection points have been added to the cluster, where k is the number of circles. The final cluster centroid gives the location of node N.

#### 2.3.1.3 Triangulation distances

Triangulation is a method of determining horizontal positions of the nodes based upon the trigonometry proposition that if one side with direction and two angles are known previously, the remaining sides along with the direction are calculated[68][69][70]. A triangulation system is basically a network of nodes where the nodes can be connected with a triangle or overlapped triangles. The nodes in the triangulation network are called triangulation nodes and the side whose length is predetermined is called base line of the network. Figure 2.7 shows the basic concept of triangulation system. For $\triangle ABC$, length of all lines,

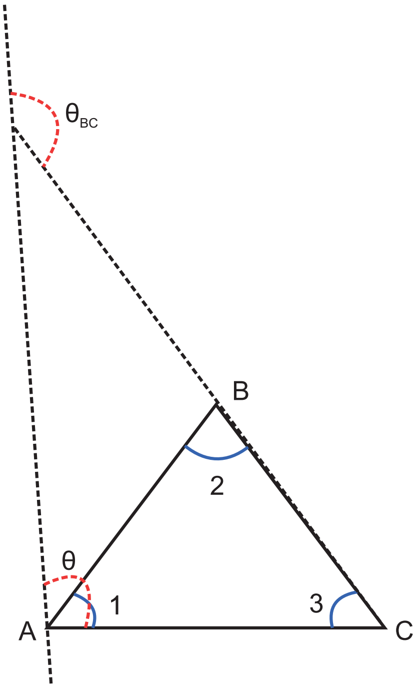


FIGURE 2.7: *Triangulation*

$$\frac{AB}{Sin3} = \frac{BC}{Sin1} = \frac{CA}{Sin2} \tag{2.24}$$

$$AB = L = 1_{AB} \tag{2.25}$$

$$BC = \frac{LSin1}{Sin3} = 1_{BC} \tag{2.26}$$

$$CA = \frac{LSin2}{Sin3} = 1_{CA} \tag{2.27}$$

Azimuth of $AB = \theta = \theta_{AB}$

Azimuth of $AC = \theta + \angle 1 = \theta_{AC}$

Azimuth of $BC$ = 180° - $(180^\circ - ((\theta + \angle 1) + \angle 3))$

= 180° - $(180^\circ - (\theta + \angle 1 + \angle 3))$

= 180° - $(180^\circ - (\theta + 180^\circ - \angle 2))$

= 180° - $(180^\circ - \theta - 180^\circ + \angle 2)$

$= 180^\circ + \theta - \angle 2 = \theta_{BC}$

Latitude of $AB = l_{AB}\ Cos\ \theta_{AB} = L_{AB}$

Departure of $AB = l_{AB}\ Sin\ \theta_{AB} = D_{AB}$

Latitude of $AC = l_{AC}\ Cos\ \theta_{AC} = L_{AC}$

Departure of $AC = l_{AC}\ Sin\ \theta_{AC} = D_{AC}$

Latitude of $BC = l_{BC}\ Cos\ \theta_{BC} = L_{BC}$

Departure of $BC = l_{BC}\ Sin\ \theta_{BC} = D_{BC}$

The desired coordinates of triangulation stations B , C , D are as follows : $X_B = X_A + D_{AB}$

$X_C = X_A + D_{AC}$

$Y_B = Y_A + L_{AB}$

$Y_C = Y_A + L_{AC}$

# CHAPTER 3

# Review of Literature

## 3.1 Introduction

The progressive development in the Micro-Electro-Mechanical Systems technology, the advances in wireless communication systems and integrated digital circuits have developed a number of tiny efficient sensors that work collaboratively in a WSNs[71]. They collect or sense the data, process the data and also transmit the data. In recent years, WSN has been a global interest where a number of significant research contribution has been made. A WSN can be defined as a network of small devices called sensors which are distributed spatially. These nodes coordinate among themselves to work with the gathered information from the network scenario. The data gathered is finally dispatched to a sink which can be local or gateway of other network using wireless links. As the technology advances, the sensor networks get smarter and cheaper too. A number of rapid growing potential applications have made this domain of science a multi -billion dollar market[72][73]. With this much of expectation, the WSNs also need to upgrade its standards and technologies so that it can support the upcoming sophisticated applications in future.

The positioning of the sensors is an important part in the networks. They can be positioned far from the actual scenario to work with sense perception. But, some privileged sensors are also required to deploy so that the noise data can be differentiated from the original data. Another way to deploy the network is to position the sensors in the network scenario only with the sensing capabilities from the environment. This data are accumulated and sent to some sink nodes for further analysis and or fusion of data. Whatever the process is the position of the sensor nodes need not be precomputed as it can create the overhead in the application. Moreover, the random deployment of the nodes is beneficial for any sudden event. This ensures that WSNs [74] should have self-organizing capability. Besides, the sensor nodes work in cooperative way by processing the data locally and partially for the desired information to be sent to the sink. Realization of the WSNs applications need a detailed understanding of ad hoc wireless networking through which the sensors will be communicating. A number of protocols and algorithms are introduced for wireless ad hoc communication, but they do not suit for WSNs as these networks are resource constrained and very dynamic.

## 3.2 Applications of WSNs

The expanding need of society, the variable technological advances, the integration of the devices and the dynamic scenarios of the network have emerged an exponential growth of WSN applications [72] in a very short period. The sensors are able to sense the data, to detect a required target, to calculate a undefined location and even to control the actuators accordingly. The use of micro-sensing and wireless communication technology along with these nodes extends many new application areas. We have categorized the vast application domains of WSNs into defense, natural environment, health monitoring, smart home and other commercial areas. The classification can be top-downed with more detailing to expand it with more categories such as space exploration, chemical processing and disaster relief.

### 3.2.1 Defense Applications

WSNs are integral part in defense applications [75][76] due to its scalability, sensing and fault-tolerance capabilities. It may also happen that the enemies destroy the sensors, but as the sensors are low cost and densely deployed in the network, the destruction affects a minimum. Command, control, monitoring, targeting and many more tasks are performed in this defense domain with the help of WSNs. The coordinators or the heads of the soldiers troops monitor the status and the availability of the equipment and the ammunition in a battlefield. For this, every troop, vehicles, equipment and critical ammunition require to be attached with small sensors that report the status. These reports are accumulated and forwarded to sink nodes and sent to the troop leaders who may further proceed to the higher commanding authority. Critical locations, probable opponent entry routes can be pre-configured with sensors to have a close watch for the activities of the opposing forces. If new application dimension exists, it is also easy to reconfigure the sensors or to deploy new sensors. Defense personnel also use such networks to get the information of the opposing forces in a critical terrain and also to monitor their activities. Intelligent ammunition is also equipped with sensors to attack the target properly. Battle damage assessment data can also be analysed using such WSNs. As the warfare technologies have also been evolved with the progress of science and technology, the detection accuracy is required in the process and WSNs work efficiently in this domain.

### 3.2.2 Natural Environment Applications

Different sensors are programmed with different conditions of environmental parameters [77][78][79][80]. Utilizing the multivariable capabilities, different types of environmental applications of WSNs exist. It includes birds movement tracking, habitat monitoring of small animals, and insects, detecting natural environmental conditions important for agriculture activities, irrigation level monitoring macro-instruments for large-scale Earth monitoring and space exploration; bio-chemical reaction and analysis; monitoring in marine, soil, and atmospheric contexts; detecting forest fire, flood detection and pollution study [81][82]. The densely deployed WSNs in a forest can give the clarity of information regarding the source of fire or even any sudden event in an area. The sensor nodes collaborate with each other to perform distributed sensing and overcome obstacles, such as trees and rocks that block wired sensors line of sight. WSNs can also map biocomplexity [83] of the environment across temporal and spatial scales. Such mappings help in observing the minute details of biodiversity specifically for very small size of plant species at ground level which is having a significant role in analysing the biocomplexity issues in the environment.

### 3.2.3 Medical Applications

Expanding the hands of applications, WSNs have also proved its significance role in different medical applications [84][85] . Telemonitoring of human psychological data helps in medical research and to analyze the human behaviour. The sensor networks also help the doctors and medical assistants for free movement and also allow doctors to detect predefined symptoms of a patient in an earlier stage[86][87]. Patient monitoring system is also comprised of several sensors that observe the blood pressure, heart rate, body temperature and so on. Even the doctors are also having sensors to locate another doctor in the hospital whenever required. Moreover, drug administration in hospitals can provide the patients proper allergetic factor analysis.

### 3.2.4 Smart home

In this present age of machines, not only the technology, but our lives have also become automated. The automation of home services has given a clear cut emphasized on this aspect. Sensor nodes and actuators are equipped with home appliances [88] such as electric lights and fans, television, air conditioner, refrigerator, vacuum cleaner and many more. These sensors can communicate with each other and also a room server and the room servers also communicate with other room servers for coordination and collaborative functionalities. The sixth sense enabled refrigerator, the feeling estimation Air Conditioner's, the talking washing machine are some of the examples [89][90] that we use in our daily lives. Besides, the smart home also exist where starting from your door open to next door close all things are automated according to the users' notification or just speech recognition. The security of such smart home has also been ensured with smart sensor locks which generate alarms if someone tries to invade.

### 3.2.5 Others Commercial Applications

Apart from the above categories, some more applications [91][92][93] have been seen in WSNs. Material fatigue can be monitored well with the help of sensors to detect the localized structural damage of materials. Virtual keyboards, inventory management, inspecting product quality are some of the useful applications of WSNs. Like smart homes, constructing smart office spaces along with smart office environment makes the professional life more interesting and innovative. Interactive toy has become an influential mean to analyze the childrens mental growth. Interactive museum [94], automated machines and factories, vehicle tracking [95], theft detection [93], robotics control all these are some examples of applications in WSNs.

## 3.3 Design factors of Wireless Sensor Networks

Whenever we talk about the deployment of a WSN, a set of design factors need to be considered for the better performance of the network. Though the different factors have been addressed by different researchers but the integrated solution of all the factors is not available. The factors, we are going to discuss are important because they provide the rules or guidelines to design any algorithm or protocol for WSN.

### 3.3.1 Fault tolerance

The failure of a sensor node in a WSN is very common and obvious due to various reasons that include: power exhaustion, environmental interference or malicious activities. The fault tolerance [96][97][98] capability of a WSNs ensures that the network will be in operation mode even though one or more sensor nodes are getting deactivated from the network. The level of fault tolerance to be applied in the design parameter depends upon the type of application. For example, if you are deploying the network in home environment, interference is low and therefore fault tolerance can be relaxed. But, the same network if we deploy for an outside network (e.g. agriculture field, battle field, vehicular monitoring etc.), the fault tolerance needs to be in priority as interference and noise is higher in outside scenarios.

### 3.3.2 Scalability

The number of sensor nodes in a WSNs is also important. Depending upon the application requirements this number may vary from a few to thousands. It also required that the algorithms and protocols must adapt to work with the dynamic requirement of the scalability [99][100][101] of a sensor network. They must also utilize the high density feature of the network.

### 3.3.3 Production cost

Building up a system or a network also considers some budget. As WSNs comprises of densely deployed sensor nodes, the total cost [102] of the network depends on single sensor node. With the technology advancement the integrated devices along with the sophisticated sensors make it more economic for deployment. The sensor nodes sometime also equipped with mobilizers, location identifiers which may provide some additional cost to the overall WSN deployment cost. Therefore, the cost [103][104] for WSN needs to be justified for different application requirements.

### 3.3.4 Hardware requirements

As per the progress of technology, the hardware specification [105] and requirement is another important part. A sensor node is made up of four basic modules: sensing modules, processing module, transceiver module and power module. Most of the applications of WSNs require a better precision of location information. Therefore, the location identification module is also an integral and compulsory part of sensors now-a-days. Besides, a sensor node can also have mobilizer or power unit too. The sensing modules have sensors to sense data from environment. This analog data is converted to digital by Analog-to-Digital Converter (ADC) and then finally input to the processing unit. All these functional units are integrated into a very small sized and light weighted box [106]. This total unit is expected to use low power resources, it should be autonomous and should be operated unattended manually. This type of sensor units needs to be adaptive to the network environment.

### 3.3.5 Sensor Network topology

The rapid growth of technology and the increasing need of humans have extended the static wireless sensor networks to the mobile sensor networks where sensor nodes are mobile in nature and the structure of the networks change very often. In such scenarios, the maintenance of the network structure or topology [107][108] is very critical to maintain as a number of sensor nodes get off the network for various reasons such as battery exhaustion, hardware failure, software failure or even malicious intrusion. Moreover, due to dynamic requirements of the applications, it is also needed to add new nodes in the network which again creates ripple changes in topology. The algorithms and protocols must adapt to such dynamic changes of the topology of WSNs.

### 3.3.6 Network Environment

The vast application domains of WSNs make them critical and concerning to use in different harsh conditions such as: under the sea water, with the wild animals bodies, beneath the debris of battlefield or natural calamity, in a large warehouse and many more. It is very easy to understand that, the deployed WSNs get almost unattended once they are deployed. Because of these different severe environmental conditions [109][110], noise and interference are always dominating in real life applications of WSNs.

### 3.3.7 Transmission Media

WSNs work on either one hop or multi-hop communication. Both the cases use some wireless media such as radio frequency, infrared or optics. The first option of radio links is to use Industrial, Scientific and Medical (ISM) band that are made license-free for communication. Sensor networks always require low-cost, small and ultra-low powered transceivers. Sometime the contradiction among hardware constraints, antenna efficiency and power consumption limits the choice of carrier frequencies for such transceivers. It is very advantageous to use ISM band as it is free for use and also globally available. The next option for the wireless communication in a WSN is infrared. It is also license free and not sceptical to the interferences from electrical devices. Though it is a cheaper solution in terms of economy and also easy to implement, the main drawback of this technology is line-of-sight communication between a sender and a receiver. As we have seen the different severe conditions and the application scenarios, the line-of-sight communication is not always possible for such networks. A new advancement in recent years has been observed with using the optical technology in WSNs [111][112].Depending upon the application requirements, one has to choose appropriate transmission media for minimum noise and interference so that performance of the network can be better.

### 3.3.8 Power Consumption

A sensor node generally performs three basic tasks: sensing, transmission and processing. Each of these tasks requires some of the energy. As the sensor nodes are equipped with a very small power resource, we cannot expect the sensor nodes to work seamlessly after installation. Each of the tasks said above also depends upon the complexity level. If complexity is high, resource drainage is faster and if the tasks are less complex the sensor nodes can perform for a larger duration. A WSN's performance depends on its sensor nodes' functionalities. If the sensor nodes get resource exhausted, they will cut off the WSN and the topology needs a rearrangement because it is always not possible to replace an exhausted or non-working sensor node. Therefore, the algorithms and the protocols for WSNs must be efficient in utilizing the power resources [113][114][115] to maximize the WSNs' lifetime.

## 3.4 Categorization of the Literature Review

Our contribution in this research emphasizes the localization process with three objectives: first, creating a backbone for WSNs with MCDS method; second, optimizing the backbone and third, providing security to the localization process. Following these objectives, we have also categorized our review of literature in the subsections below.

### 3.4.1 Literature review for creating backbone

In the paper [116] by Wang and et. al., the authors have proposed an architecture called All-IP for WSN. This architecture provides the benefit of performing routing without route discovery. This architecture depends upon gateway tree and hierarchical address structure. The All-IP architecture deals with three types of nodes: gateway nodes, fixed nodes and mobile nodes. The gateway nodes and fixed nodes have routing and forwarding capabilities, whereas mobile nodes do not have. A gateway node is connected to an access router in the IPv6 network. The gateway tree is created by a gateway node and a number of fixed nodes: the gateway node is located at the root node and the intermediate nodes and leaf nodes are comprised of fixed nodes. In this architecture, the routing backbone is constructed by all gateway trees. The mobile nodes communicate only through backbone with the help of an associated node from that tree. The authors have applied this architecture for patient monitoring purpose, but the architecture can be applied for small scale WSNs.

In paper [117], Singdh and et. al. have presented a scheme for WSNs for the proper placement of the sink node in backbone assisted communications. The proposed approach emphasizes that, the best sink position falls at either at the theoretic centre of the tree or at the centroid of the graph irrespective of the backbone formation. Generally, the routing scheme deals with hop counts for the best route from a source to a destination. In this work, the authors have shown the optimized sink node placement so that the network parameters can be improved. The proposed approach proves its efficiency in terms of delay, load and energy consumption.

In the paper [118] by Reza and et. al., a virtual backbone generation method has been proposed for WSNs. The proposed method uses connected dominating set and its optimization is also addressed. Moreover, a clustering method is also used for sensor nodes in this method. The authors have divided the WSNs into clusters consisting of a high-energy gateway node and several sensor nodes. This reduces the routing overhead. The overall network set up depending upon two sub-processes: bootstrapping and clustering. Bootstrapping process consists of two phases: node discovery and topology formation. In node discovery phase, the gateways and sensor nodes identify their own neighbours and n topology formation phase internode links are established. In the clustering process, gateways calculate the cost of the communication and broadcast with all other gateways. Depending upon this broadcast information clusters are made and all the sensor nodes are informed about the ID of the cluster in which a particular sensor node is in. Once the clusters are created, CDS algorithm is applied for the backbone formation.

In the paper [119] by S. M. Nazrul Alam and Zygmunt J. Haas, the authors have shown two architectures for underwater WSNs: one is hierarchical and another is non-hierarchical. The hierarchical architecture uses less number of sensor nodes for backbone. The other sensor nodes communicate with these backbone nodes for information is shared to the sink node by message transferring among backbone nodes only. The backbone nodes though expensive but are small in number and similarly the mobile sensors are inexpensive but large in number. This makes the overall network deployment economic. In non-hierarchical structure, the nodes are assumed to be randomly deployed. It divides the whole network into identical cells. Each cell consists of several sensor nodes among which only one is active for sensing and connectivity. This approach helps in energy conservation of the network.

In the paper [120] by Mancilla et.al., the authors have surveyed the formation of WSNs. The positioning of sensor nodes and the overall structure of the WSN has a significant role in the efficiency evaluation of the network performance in terms of network longevity. The authors have proposed one classification of such formation of WSNs as shown in Figure 3.1.

In the paper [121] by P.S. Vinayagam, the author has surveyed the Connected Dominating Set (CDS) algorithms used for creating virtual backbones in ad hoc networks. CDS is always has been proved as a beneficial method of creating backbone where some nodes are treated as backbone nodes and all other sensor nodes are connected with atleast one backbone node for communication. The author has shown a classification of such CDS construction algorithms as shown in Figure 3.2. The centralized algorithms require knowledge of the network but provide a small sized CDS. In spite of this advantage, this category lacks behind as the network information is not always feasible to collect in the scenario of mobile sensors. It also creates trouble to centrally monitor the overall network if the network size increases. On the other hand, the decentralized algorithms require only the local network information. These algorithms can be divided into two subsets: Addition based algorithms starts with initial set of nodes and eventually add up nodes to create CDS; Subtraction based algorithms starts with considering all the nodes in the CDS set and then systematically delete

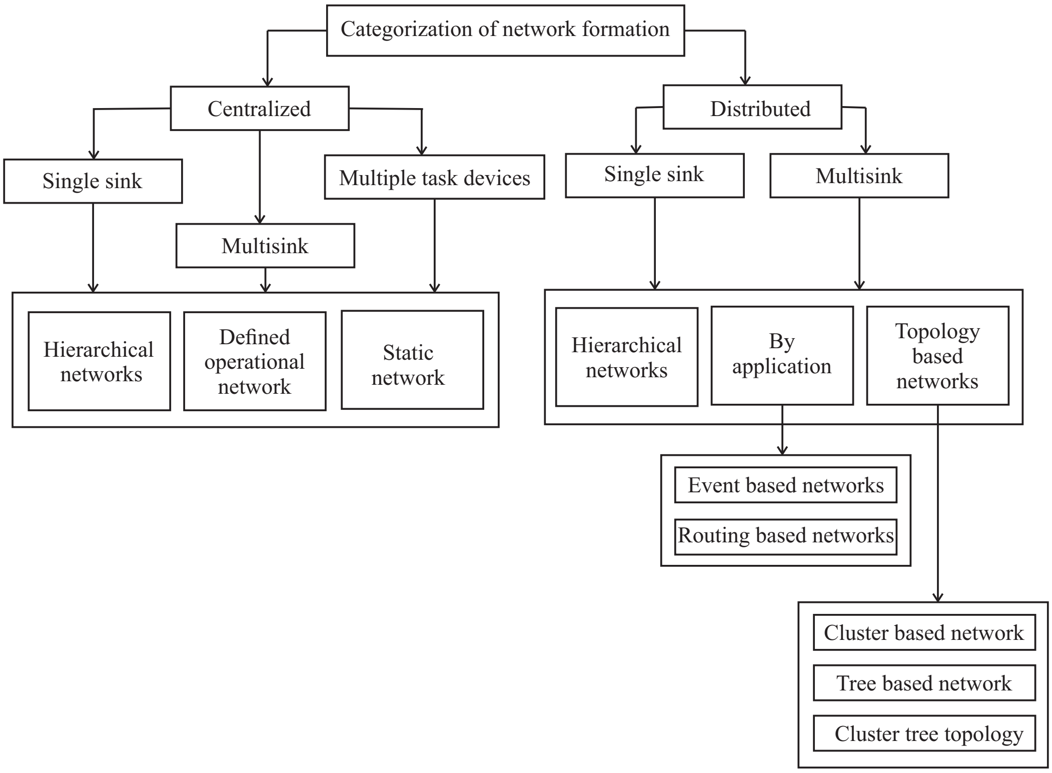


Figure 3.1: *classification of such formation of WSNs*

nodes to form the final CDS. The author has also surveyed some of the contemporary CDS based virtual backbone approaches such as revised-CDS (r-CDS), Timer-based Energy aware Connected Dominating Set (TECDS), greedy approximation for MCDS and many more.

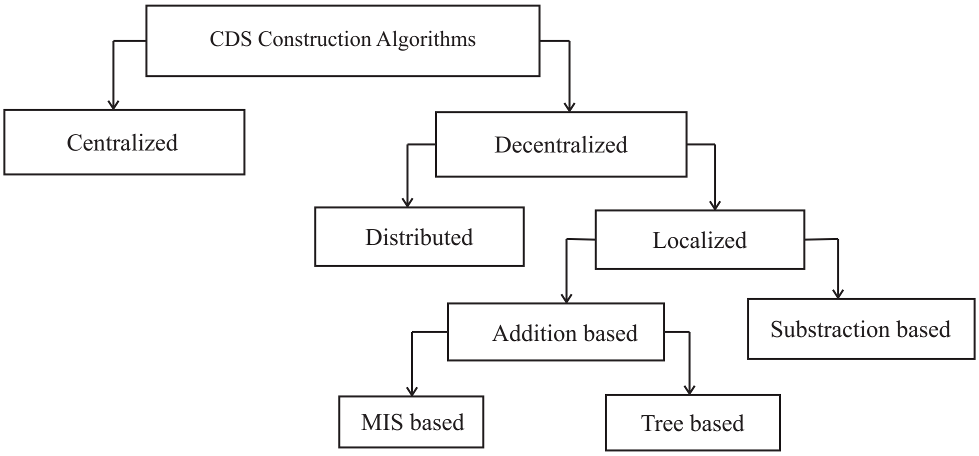


Figure 3.2: *CDS construction algorithms*

In the paper [122] by Ren et. al., the authors have researched an algorithm for distributed construction of CDS for wireless ad hoc sensor networks. The CDS is made priori and then Minimum Weight Spanning Tree is applied to optimize the CDS. The authors have introduced a new terminology as effective degree which is updated after a predetermined time interval. This update process is divided into two phases: initialization phase and updating phase. More than single round of iteration is required to achieve the optimal CDS for use.

In the paper [123] by Sutagundar and Manvi, the authors have shown a fishbone structure of WSNs to aggregate data from sensor nodes. The authors have also used some mobile agents in their scheme. The proposed scheme works in the following steps: creation of backbone and identifying master centres on this backbone, selection of local centres on the backbone ribs that can communicate with master centres with the help of mobile agents, local aggregation process and transmission of information to master centres and finally mobile agents transmit the aggregated data to the sink nodes. Master centre identification depends on the parameters of Euclidean distances, residual energy, backbone angle and connectivity.

In the paper [124] by Kui et.al., the authors have introduced an energy based CDS scheme called as Data Gathering Algorithm based on Energy-Balanced Connected Dominating Set (DGA-EBCDS) for WSNs. The CDS is created based upon two prime factors: energy and degree of node. The algorithm is distributed and requires only node level information. It has two stages of processing. The first stage selects dominators and second stage identifies the connectors. Once all such dominators and connectors are identified, CDS is formed. To make this CDS energy balanced, the authors have assigned weight to calculate the capability of nodes depending upon the above two factors.

In the paper [125] by McLauchlan et.al., the authors have compared two CDS based topology construction protocols: Simple Weighted Spanning Tree and Energy Aware Spanning Tree. Both the protocols have an objective to reduce the number of broken links. These broken links may have been caused due to single node becoming drained of the resource or behaving compromised. The Simple Weighted Spanning Tree protocol balances the energy consumption between the parent and children nodes. The Energy Aware Spanning Tree algorithm balances the load among the communication branches of the virtual communication backbone. The results of the research work shows that the proposed method with neighbourhood discovery process performs better in the experimental setup but at the same time faces the problem of large number of dead nodes when network density increases.

In the paper [126] by Emran et.al., the authors have shown a honeycomb tessellation approach for virtual backbone creation with multisinks in WSNs. In different critical applications, data availability in real time is required. Moreover, if the sinks are mobile, the situation gets more concerning. In such applications, reliable data dissemination of events and handling the mobility of both sinks and event sources become very important. The proposed architecture consists of 'highways' in a honeycomb tessellation, which is the three main diagonals of the honeycomb where the data flow is directed and event data is cached. The highways are considered as predefined regions of the events and queries. The proposed protocol called Hexagonal cell-based Data Dissemination (HexDD), is fault-tolerant. In this algorithm, individual sensor nodes in the network are bound to cells of the virtual hexagonal tessellation based on their geographic locations. The architecture also defines three principle diagonal lines'highways' (or 'border lines') as said above which divide the sensor field into six parts. The lines those intersect at the centre of the network form the rendezvous region for queries and data. In the honeycomb tessellation, each cell has six neighbours covering the surroundings from all directions. For every sensor node in one cell can communicate with all the nodes in the other cell. This actually defines the edge length of the hexagonal cell. In this approach, a hexagonal cell placement and node-cell association scheme is also established.

In the paper [127] by Guadalupe et. al., the authors have proposed an approach for cluster-based self-organizing virtual backbone. The authors have shown that each mobile device is controlled by a multi-role agent that performs some important tasks such as building a backbone, detecting network holes or segmentations and recovery.

These tasks are performed locally. The role management attribute of the agents allows the backbone for reconfiguration whenever a node leaves or joins the network. The proposed algorithm is distributed and creates clusters too. Each agent (nodes) can act with four probable roles: leader, gateway, bridge and member. Each group is composed by single agent acting as leader, zero or more agents acting as gateway and bridge, and one or more agents acting as member. The leader controls the communication among members of its group or different groups. A gateway agent is responsible of communicating members of different groups through leaders of groups; bridge nodes connect different segments of the network. Finally, members are connected to a single leader. The authors have also developed the energy management of the proposed model and show that he proposed approach saves energy.

In the paper [128] by Lehsini et. al., the authors have shown an efficient approach with cluster-based self-organizing algorithm for WSNs. The proposed algorithm is weight based and groups the sensor nodes into a disjoint set of clusters. The cluster heads are selected based upon weight which is calculated upon two parameters: residual energy and 2-desnsity. 2-density parameter has been used by the authors to apply the algorithm with homogeneous clusters and to emphasize a node that is having most 2-neighbours. The cluster heads performs various tasks such as coordinating the cluster members, aggregating collected date and transmitting them to the remote sink, directly or via multi-hop transmission mode. As cluster heads are responsible for such computational and transmission task and no other cluster member cannot send cumulative data directly to the sink, the cluster heads may be overloaded and therefore, the election of cluster head is executed periodically. The authors have also used threshold value for each cluster size and the cluster members are bounded with in at most 2-hop distances from the cluster head. He authors have shown that the proposed algorithm provides less number of balanced clusters, minimizes rebuilding of clusters and maximize sensor nodes' lifetime.

In the paper [129] by Khan et. al., the authors have introduced a class of local algorithms called Nearest Neighbour Trees (NNT). These algorithms are energy efficient and approximate a Minimum Spanning Tree (MST). The authors have shown NNT algorithms for the complete graph model where the maximum transmission range of the nodes are large enough so that any pair of nodes can communicate directly with each other. In this scenario, local broadcasting is used. Request, available and connect- these three types of messages are used in NNT. The authors show that this proposed approach provides low-cost spanning trees. Moreover, dynamic version of these algorithms has also been analysed in the paper.

Table 3.1: *Literature review of backbone creation*

| Ref no. | Author(s) | Year | Remarks |
|---|---|---|---|
| [116] | Wang et. al | 2014 | IP address allocation can be a troublesome work in large scale WSNs. Vulnerability exists for cache poisoning and routing table poisoning attack. |
| [117] | Snigdh et. al. | 2016 | Single node failure near to the sink can lead to network disruption. |
| [118] | Reza et. al. | 2006 | Gateway selection process is not validated. Not suitable for mobile environment. Resource exhaustion of sensor nodes may lead to network disruption. |
| [119] | Alam et. al. | 2010 | Energy consumption is low but number of nodes in backbone is not given any upper or lower bound. |
| [120] | Mancilla et.al | 2016 | Different types of formation approaches of WSNs have been surveyed. |
| [121] | P.S. Vinayagam | 2016 | Different types of CDS construction algorithms and CDS based virtual backbones for WSNs have been surveyed. |

| | | | |
|---|---|---|---|
| [122] | Ren et. al. | 2014 | Advantageous for WSN. But as per the results more number of rounds provide better CDS which is in turn a resource exhaustive task in case of WSNs. Moreover, in case of mobile environments, CDS optimality becomes a problem with such round iterations. |
| [123] | Sutagundar and Manvi | 2013 | Fish bone maintenance is a concern in mobile environment, isolated nodes may increase and several reconstructions required. |
| [124] | Kui et. al. | 2013 | If a node is having higher energy but lower degree of connectivity it may not be selected as a dominator which may be a disadvantage for the algorithm. Moreover, this algorithm needs validation for mobile environment with experimentation. |
| [125] | Mancilla et.al | 2014 | Validation in mobile environment required. |
| [126] | Erman et. al. | 2011 | Localization error with mobile sinks needs to be verified. Fault tolerance in real applications need to be validated. |
| [127] | Guadalupe et. al. | 2011 | The algorithm is well suited for static networks, but for mobile environment it will be hard to manage the different roles of nodes whenever their cluster changes. |

| | | | |
|---|---|---|---|
| [128] | Lehsaini et. al. | 2010 | The algorithm is suitable for static networks. If mobility is incorporated isolated nodes will exist which will lead to re-execute the re-affiliation process very often increasing the delay and complexity. |
| [129] | Khan et. al. | 2009 | Dynamic arbitrary point of distribution of nodes needs to be analysed. Mobile sensors or sinks incorporation may degrade the performance. |

### 3.4.2 Literature review on DV-Hop improvements

In the most recent research work in [130] by Xiao and Zheng, the authors have introduced a three-dimensional node localization hybrid algorithm called DV-Hop-AC-PSO, which combines the advantages of DV-Hop, Ant Colony(AC) and Particle Swarm OptimizationPSO algorithm. In the proposed algorithm, particle swarm algorithm is adopted to optimize the parameters of the ant colony algorithm, and DV-Hop algorithm is used in the iterative process of ant colony algorithm to improve the localization accuracy.

An energy efficient algorithm extended from DV-Hop has been shown in [131] by Kumar and Lobiyal, where the anchor nodes communicate only one time with the unknown nodes to inform about the coordinates of the anchors themselves. By calculating hop-size at unknown nodes reduces the communication between anchor nodes and unknown nodes which results in minimization of the energy consumption.

In the paper [132] by Kumar and Lobiyal, the error reduction method has been shown by the authors. The advanced DV-Hop algorithm uses the effective aspects of the parameters. Using the effective distance calculated, estimated locations of unknown nodes are calculated by Two Dimensional hyperbolic location algorithm. Covariance matrix of range estimation error is used as weight matrix for location improvement.

A novel localization algorithm, Various Average Hop distance-DV-Hop(VAH-DV-Hop), has been introduced in the paper [133] by Liu et. al. The anchor estimates both the distance and the hops between the other anchors. The angle-method is applied to reduce the negative factors which are caused by routing void. Each anchor node estimates the average hop distance and this value is broadcast. Values are reserved when unknown node receives average hop distance for several anchors. Next, the distance between the unknown nodes and the three anchors is computed using the average hop distance multiplied by individual hops of anchors. Finally, the trilateration method is used for the location estimation.

An improvement in DV-Hop is proposed with three modifications in the paper [134] by Yinget.al. Firstly, secondary reference node is located by three anchor nodes using trilateration or centroid methods. The second modification depends on the node of last hop, and the third is the use of Max-Min method. A number of researches have been done to check the effect of localization in presence of mobile anchor nodes.

Localization algorithm with a Mobile Anchor node based on Trilateration (LMAT) is proposed in the paper [135] by Han et.al. The algorithm uses mobile nodes that move along the trilateration trajectory. Simulation results show that the algorithm provides better efficiency as compared to other algorithms in this regard.

A recent work in this line is done in the paper [136] by Han et. al. The paper introduces mobile anchor based localization algorithm Mobile Anchor Assisted Localization algorithm based on Regular Hexagon (MAALRH) which is based on regular hexagonal in 2D wireless sensor networks. The unknown nodes use trilateration technique to estimate the location.

In the paper [137] by Hu et. al., the authors describe a localization algorithm called Mobile Anchor Centroid Localization (MACL). The technique discussed here uses single mobile anchor. The localization method is radio frequency based and therefore extra hardware cost is invalid. Using a single mobile anchor node is a scenario specific and does not support the random node deployment procedure with complete mobile environment. Further, single mobile anchor node will be more resource exhausted if the number of unknown node increases.

In the paper [25] by Rai et.al., Minimum Connected Dominating Set (MCDS) using Dominating Set (DS) has been introduced by the authors. The algorithm consists of three phases. The first phase deals with the searching for a dominating set, the second phase identifies the connectors and the third phase prunes the generated connected dominating set to get the minimum connected dominating set. Deactivation of nodes due to power constraint is also taken into consideration for this algorithm with repairing process.

In the paper [138] by Tang et.al., the authors have introduced an efficient approximation MCDS construction algorithm (E-MCDS) energy efficient MCDS construction algorithm for the virtual backbone construction. The proposed algorithm contains two stages: the CDS construction stage and the pruning stage. The constructed CDS is approximately composed of two independent sets. The algorithm starts with initial bootstrapping process where the nodes are given some initial status and they start gathering their neighbouring information. Once all the information is gathered, then CDS construction process starts. Pruning takes place once the CDS is constructed and finally it provides near optimal MCDS for the backbone of the WSNs.

In the paper [139] by Hu and Li, the authors have shown an improved DV-HOP localization based on the traditional DV-HOP localization method. The proposed algorithm introduces threshold M, and also uses the weighted average hop distances of anchor nodes within M hops to calculate the average hop distance of unknown nodes. Moreover, the positioning results are corrected in the algorithm.

In the paper [140] by Zhang et. al., the authors have proposed an improved DV-Hop location algorithm. The algorithm is based on reduce the accumulation errors of the average hop distance of the unknown nodes in WSNs. The authors have used the weighted averaged method for calculate to the average hop distance in the second stages. Then two beacons are used to estimate a region and the centroid of the region is calculated as the coordinates of the unknown node.

In the paper [141] by Chen and Jhang, an improved algorithm is shown as an improvement of the locating performance of the DV-Hop algorithm, popular and most used range-free algorithms in WSNs. The authors set some anchor nodes at the border land of monitoring regions. Modification is done on the average one-hop distance between anchor nodes. Each unknown node uses the average one-hop distance to estimate its location using some weighing function on the received average one-hop distances from anchor nodes. Finally, the particle swarm optimization is used in the algorithm to correct the position estimated by the 2D hyperbolic localization algorithm performance.

In the paper [142] by Assaf et.al., the authors have proposed a novel hop-count based localization algorithm. It is able to reduce errors due to mapping the hops into distance units. Using the proposed algorithm, unknown nodes locally calculate the mean hop size and therefore anchor nodes need not to broadcast. Node distribution priori knowledge is not required for this algorithm.

TABLE 3.2: *Literature review of backbone creation*

| Ref no. | Author(s) | Year | Remarks |
|---|---|---|---|
| [130] | Xiao and Zheng | 2014 | The algorithm lacks behind with higher complexity and dependency of other supportive algorithms. |
| [131] | Kumar and Lobiyal | 2013 | Hop size will change in mobile environment and then communication among unknown nodes and anchor nods will increase leading to resource exhaustion. |
| [132] | Kumar and Lobiyal | 2012 | Validation required for mobile environment. |

| | | | |
|---|---|---|---|
| [133] | Liu et. al. | 2012 | The algorihm is suitable for static environment with trilateration method. But to apply the same method in mobile scenarios, we need some other tolerant method of location computation phase. |
| [134] | Ying et.al. | 2010 | If unknown nodes get mobile, complexity arises and last hop count need to be validated to generalize. |
| [135] | Han et.al. | 2013 | The movement of the nodes follow a particular mobility pattern which may not be the compulsory event for a dynamic network deployment. |
| [136] | Han et. al. | 2013 | This algorithm faces the problem in case of random deployment. |
| [137] | Hu et. al. | 2008 | Using a single mobile anchor node is a scenario specific and does not support the random node deployment procedure with complete mobile environment. Further, single mobile anchor node will be more resource exhausted if the number of unknown node increases. |
| [25] | Rai et. al. | 2009 | The algorithm is considered to be beneficial to form backbone in WSNs in case of mobile environment. |

| | | | |
|---|---|---|---|
| [138] | Tang et. al. | 2012 | Neighbouring information gathering creates overhead in mobile environment. Security measures to detect outsider noded need to be validated in such process. |
| [139] | Hu and Li | 2013 | Normalization required in the algorithm if we apply the method in mobile environment else the range of hop distances will vary a large that will create location error in further calculation. |
| [140] | Zhang et. al. | 2012 | Centroid will be frequent change if nodes become semi-mobile or mobile. Three beacons works better in such cases. |
| [141] | Chen and Jhang | 2012 | One hop usage will eliminate the wormhole probability, but authentication mechanism required for compromised nodes. Further, the average hop distance calculation is applicable for small networks but if scalability increases, average hop distance calculation will be depending on multihop else isolated nodes will be there. |

| | | | |
|---|---|---|---|
| [142] | Assaf et.al. | 2013 | Random node deployment can be possible with this algorithm. But calculation of mean hop size will be given a load to the resource constraint nodes; rather the traditional method of calculation of this parameter by anchor nodes is better as per the resource exhaustion concern. |

### 3.4.3 Literature review on optimization Techniques

Once, the backbone is created, the next step according to our objective is to optimize the backbone. A number of techniques [143] have been identified in the previous research. Some of the relevant works have been discussed below.

In the paper [144] by Kulia and Jana, the authors have shown a load balanced clustering algorithm called as Energy Efficient Load- Balanced Clustering (EELBC). This algorithm uses the concept of minimum heap which is built using cluster heads (CHs) or gateway nodes. Gateways nodes can have a long-haul communication compared to the sensor nodes. All nodes are assumed to be aware of their position through GPS. Network setup is performed in two phases; bootstrapping and clustering. In the bootstrapping process, all the sensor nodes and gateways are assigned unique IDs. In this algorithm, sensor nodes broadcast their location and IDs to the gateways within communication range of each other. So, the distance from a sensor node to all the gateways within its range is calculated. In clustering phase sink executes the clustering algorithm depending upon minimum heap algorithm.

In the paper [145] by Liao et.al., the authors have shown a load balanced cluster based algorithm for WSNs. The algorithm creates clusters depending upon distances and distribution density of the nodes. Node distribution follows Poissons process and the algorithm has been applied for fixed locations of the nodes. CHs are also used in this algorithm and are selected by two parameters of connected density and distance from the base station. The simulation of the proposed algorithm shows superior results but insignificant redundancy of clustering nodes is a drawback factor.

In the paper [146] by He et.al., the authors have considered three NP-hard problems: MinMax Degree Maximal Independent Set (MDMIS) problem, the Load-Balanced Virtual Backbone (LBVB) problem, and the MinMax Valid-degree non-Backbone node Allocation (MVBA) problem. The authors have also proposed an approximation algorithm by using the linear relaxing and random rounding techniques. Though the load balanced virtual backbone is beneficial but use of minmax valid degree non-backbone node allocation arises complexity in the process.

In the paper [147] by He et.al., the authors have shown a virtual back bone creation providing a solution to the Load-Balanced CDS (LBCDS) problem. The algorithm applies genetic algorithm on CDS to increase lifetime of the network with the help of allocation scheme and CDS p-norm values. The simulation results show that using the algorithms the network lifetime has been increased by 65%.

In the work [148] by He at.al. a load balanced data aggregation tree has been constructed by the authors. They have used multi-objective genetic algorithm for probabilistic network model. The authors have highlighted the use of lossy links for data aggregation trees. This problem has been investigated by searching the solutions of three problems simultaneously: Load-Balanced Maximal Independent Set (LBMIS) problem, the Connected Maximal Independent Set (CMIS) problem, and the Load Balanced Data Aggregation Trees (LBDAT) construction problem. They have also used two new metrics for load measurement: potential load and actual load. This model increases the lifetime of the network further by 69%.

In the paper [149] by Raha et.al., the authors have shown a genetic algorithm based mechanism. The algorithm also identifies the trustworthy route among the different alternatives between a source and a sink node. It also distributes the traffic in a balanced way in different paths. This genetic algorithm based approach provides a solution for virtual backbone creation but do not show their effect on localization process.

In the paper [150] by Sayali, the identification of balanced nodes in wireless sensor networks for data aggregation has been shown. The authors have constructed probabilistic network model for data aggregation tree. Moreover, algorithm for identification of Load Balanced Maximal Dominator node Set (LBMDS) and connector nodes for LBMDS have been developed in the paper. The authors also have proposed an Expected Allocation Probability algorithm (EAP) to solve Parent Node Assignment (PNA) problem. The proposed algorithm is applicable for the static WSNs environment and therefore does not confirm the random mobile sensor deployment.

In the paper [151] by Wan et.al., a distributed approach for constructing CDS has been show by the authors. The approach shown in the paper helps to generate small size CDS. It also reduces the message complexity for a nontrivial CDS. In the problem of creating virtual backbone with CDS, the relation between maximum size of independent set and the size of minimum connected dominating set has an important effect on the performance.

In the paper [152] by Kalantari et.al., the authors have introduced a mathematical model that uses the flow of information by a continuous vector filed. The information ow vector field implies a set of Neuman boundary conditions and a Partial Differential Equation (PDE) including the divergence of information. The authors have introduced a measure called as p-norm flow optimization that has been solved by sequential quadratic programming.

In the paper [153] by Larios et.al. a novel tracking distributed method Location based on an intelligent distributed fuzzy system, called LIS, for localization of the sensor nodes has been introduced by the authors. Two algorithms are used by the authors: one based on a local node using a fuzzy system providing a partial solution and the other one is based on a centralized algorithm that merges all the partial solutions. The centralized algorithm is based on the calculation of the centroid of the partial solutions.

In the paper [154] by Singh and Sharma, the authors have shown a genetic algorithm based energy efficient routing strategy. The applied genetic algorithm uses the elitist strategy where the best individual replaces the worst individual after crossover and mutation. The work described in this paper considers a powerful Base Station having sufficient resource and the sensor nodes are homogeneous and have limited energy. The first-order radio model is used for calculation of the energy dissipation in the process of transmission and reception. The node energy falling below predefined level is taken off the routing path based on some probability to prolong the network lifetime. The energy load balancing strategy prevents uneven energy dissipation and thus the network lifetime is increased.

In the paper [155] by Peng et.al., genetic algorithm is applied on DV-Hop localization algorithm to improve its efficiency. The fitness function used in this algorithm depends upon the deviation from the true location of the unknown nodes. Though the algorithm improves the localization error but does not guarantee for optimized or load balanced aspects.

In the paper [156] by Wang et.al., improvement on DV-Hop localization error has been shown by the authors. The authors have used genetic algorithm with simplex method to optimize the error minimization problem in DV-Hop. The simplex method helps out for searching a local optima and the fitness function used here is based on cost and penalty. The algorithm proves its efficiency but does not support mobility of nodes.

The paper [157] by Li and Qin, shows a solution with neural networks applied for range free localization process to solve the nonlinear equalities. The authors have also explored analog circuit implementation of the neural network for such an application. The proposed neural network functions a parallel computing method and a distributed topology need to be isomorphic to the corresponding graph. Thus it is appropriate for distributed real-time computation.

The work in the paper [158] by Cottone et.al., the authors address the localization problem and also provides a solution with machine learning approach. The proposed approach is featured by an automated parameter selection option. The algorithm does not require any prior knowledge of network topology rather it depends on the knowledge of positions of a subset of nodes.

In the paper [159] by Cespedes-mota et.al., Differential Evolution Approach (DEA) is used to optimize the distribution and localization process in wireless sensor networks. The proposed algorithm uses genetic approach to provide a balance among the maximal effective coverage rate, the minimum sensor power communication, and the overlap. Obstacles are used in the algorithm to check its effect. At each generation node distribution is examined to have a minimum spanning tree. Further, Hungarian algorithm is used by the authors.

In the paper [160] by Chen L-W, a Cooperative Energy efficient Localization Framework (CELF) has been shown. The framework uses cycling ad hoc network with fleet cyclists by using mobile phones. As cyclists need to upload their location data and download global fleet information, GPS usage is required for obtaining their current positions. Distributed localization among cyclists without central control is designed to minimize the energy consumption of positioning. The proposed algorithm does not rely on costly road side infrastructures but only employs cyclist-to-cyclist communications; can supply group members with the up-to-date locations without activating GPS receivers and can estimate member positions only based on single mobile anchor instead of multiple static anchors.

In the paper [161] by de S AO et.al., a solution for localization for swarm configurations has been shown. The algorithm uses Min-Max method and Swarm Optimization to find out the efficient solution. Sequential Monte Carlo Localization method has been introduced to consider mobility and does not require additional hardware and work with the movement of seeds. Authors claim that mobility factor lowers down cost of implementation and also achieves higher accuracy.

In the paper [162] by Sharma and Grover, the authors have used ant colony optimization algorithm to identify the optimal energy efficient routing path in WSNs. The authors consider that base station energy resourced and privileged. Two optional node models can be used. If energy is below a threshold value free-space model is used and if it more than the threshold then indirect path model is used.

In the paper [163] by Shakibian et.al., novel distributed method for parametric regression in a clustered WSN using particle swarm optimization has been introduced by the authors. The authors have re-formulated the distributed regression method in

WSNs as a multi-objective optimization problem in which an objective is dedicated to each cluster. Moreover, a distributed algorithm based on Vector Evaluated Particle Swarm Optimization method is used to address the multi-objective optimization problem in two phases. The proposed algorithm obtains a set of candidate network regressors and computes the final model using a weighted averaging rule.

In the paper [164] by Bhatia et.al., the authors have coined a novel algorithm called as Genetic Algorithm based Distance Aware-Low Energy Adaptive Clustering Hierarchy (GADA-LEACH). This is an improved LEACH protocol. The concept of relay node is introduced which acts as an intermediary between CHs and BST to ease the communication between the CH and BS. The proposed algorithm makes ease of CH selection process by using genetic algorithm. Fitness function is computed by using parameters such as energy of all nodes, energy of CHs, distance of CH with its associated nodes, number of nodes in cluster, distance of base station from all CHs and number of CHs formed.

In the paper [165] by Khalily et.al., the authors have presented a problem of optimization for energy consumption in WSNs. The proposed optimization problem is transformed into a convex problem Karush-Kuhn-Tucker optimality conditions are applied to achieve the global optimum solution.

In the paper [166] by Yousif et.al., the authors have proposed a Genetic Algorithm (GA) for optimizing the WSNs lifespan. Four crossover operators combined with four mutation operators were developed to enhance the GA efficiency. The traditional one-point crossover operator referred as the ”simple crossover”, is used to evaluate the modified ”partially matched” and the ”order” crossovers. Also, a new crossover operator referred as ”rotated” crossover is also proposed and evaluated. Different combinations of these crossover operators with the one-point and two-points deterministic and random mutations are used to optimize the WSNs lifespan.

Table 3.3: *Literature review of optimization techniques*

| Ref no. | Author(s) | Year | Remarks |
|---|---|---|---|
| [144] | Kulia and Jana | 2012 | Load is not balanced and sensor nodes are performing all major functionalities except clustering. But broadcasting of sensor nodes will lead to resource depletion of the network. GPS will increase the cost of the network. |
| [145] | Liao et.al. | 2013 | Insignificant redundancy of clustering nodes is a drawback factor. |
| [146] | He et.al. | 2013 | The load balanced virtual backbone is beneficial but need to analysis of the energy consumption is required. |
| [147] | He et.al. | 2011 | Beneficial for WSNs. |
| [148] | He et.al. | 2015 | DATs are beneficial for routing but need to be validated for localization process in mobile environment. |
| [149] | Raha et.al. | 2013 | The proposed genetic algorithm is a good solution but its effect on localization process need to be evaluated. |
| [150] | Sayali | 2016 | The proposed algorithm is applicable for the static WSN environment and therefore does not confirm the random mobile sensor deployment. |
| [151] | Wan et.al. | 2002 | Beneficial for backbone creation, need to be experimented for localization. |

| | | | |
|---|---|---|---|
| [152] | Kalantari et.al. | 2008 | Quadratic programming is a good solution with partial differentiation equations but random mobile sensor nodes equation requires proper construction of the equations. |
| [153] | Larios et.al. | 2012 | The drawback of this algorithm is that mobility of nodes is not considered in this algorithm. |
| [154] | Singh et.al. | 2014 | Good genetic algorithm. It can be applied for optimization in WSNs aspects. |
| [155] | Peng et.al. | 2015 | Though the algorithm improves the localization error but does not guarantee for optimized or load balanced aspects. |
| [156] | Wang et.al. | 2015 | The algorithm proves its efficiency but does not support mobility of nodes. |
| [157] | Li and Qin | 2013 | Applicability only for isomorphic graph structures. More parallel computing for neural network may increase the hardware cost. |
| [158] | Cottone et.al. | 2016 | Subset creation will be difficult in mobile environment. Moreover, Machine learning approach must provide automated learning for its acceptability. |
| [159] | Cespedes-mota et.al. | 2016 | Verification and validation is required for moving obstacles or mobile sensors. The method of obstacle handling can be improved with some obstacle model. |

| | | | |
|---|---|---|---|
| [160] | Chen L-W | 2016 | Mobile environment validity is not ensured. GPS usage will increase the cost of the network. Single anchor usage may lead to single point of failure. |
| [161] | de S AO et.al. | 2016 | Authors claim that mobility factor lowers down cost of implementation and also achieves higher accuracy. Seeds selection need to be proper. |
| [162] | Sharma and Grover | 2015 | The significance of two models in the optimization requires more clarity explaining how they lead to optimization. |
| [163] | Shakibian et.al. | 2014 | Identifying the multi objective functions for a given set of mobile nodes is a hasty task. It may create overhead in the network too. |
| [164] | Bhatia et.al | 2016 | Only LEACH type protocol can be applied with this method. Real life test bed experimentation is due. |
| [165] | Khalily et.al | 2016 | Good solution for optimization. In addition, convex optimization problem can be solved efficiently using cluster heads as they are having more energy resources in a WSN. |
| [166] | Yousif et.al. | 2016 | The nature is probabilistic because random crossovers are used in he algorithm. |

### 3.4.4 Literature review on Secure Localization

Whenever we talk about the secure localization [167] several related problems emerges like location privacy and location reporting. To mitigate the attacks on location identification or location calculation many researchers have proposed different schemes and approaches. They are classified into two types, node-centric and infrastructure-centric. Node centric approaches deal with the calculation of information at node level. Based on their design goals, existing solutions can be further classified into three methods: (1) the prevention method, to prevent the adversaries from producing erroneous information, for example: High-Resolution robust Localization (HiRLOC) [168], Secure Range-independent Localization (SeRLOC) [169], Robust Positioning Estimation (ROPE) [170], Secure Positioning in Wireless Networks (SPINE) [171]; (2) the detection method, to detect and revoke the nodes producing erroneous information, for example: Distributed Reputation based Beacon Trust System (DRBTS) [172], Temporal Spatial Consistent based Detection (TSCD) [173], Location Anomaly Detection (LAD) [174] and (3) the filtering method, to filter the received erroneous information in the location computation step such as i-Multihop [175]. On the other side, infrastructure centric approaches emphasize on the overall network structure for localization security, such as Secure Localization Algorithm (SLA) [176] and Secure Localization Scheme (SLS) [177]. If a localization system is infrastructure centric, the infrastructure will trust the estimation locations and no verification is needed, because the locations are computed by the infrastructure itself. However, if a localization system is node-centric, the nodes may be compromised and may intentionally report false locations. So the infrastructure may not simply trust the reported locations. Thus, when localization system is node-centric, location verification is a sound method for the infrastructure to check the validity of nodes' reported estimation. Different types of secure location verification methods [178] have been introduced such as Sector [179] and Distance Bounding Protocol [180]. Some of the recent research works in this direction have been identified.

In the paper [181] by Han et.al., a very recent collaborative approach for secure localization has been shown. The proposed approach is based upon a trust model applied for under water wireless sensor networks. Based on the trust model, the secure localization process can be divided into the following five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. In order to maximize localization ratio and improve localization accuracy a Multi-Anchor Nodes Collaborative Localization (MANCL) algorithm is used. The MANCL algorithm divides the whole localization process into four sub-processes:

- unknown node localization process
- iterative location estimation process
- 3D Euclidean distance estimation process
- DV-hop distance estimation process

In the paper [182] by Zhang et. al., a cryptography based approach [16] is used for the secure localization using signature and encryption to provide confidentiality and integrity of the location information. It uses public key infrastructure along with Hash Message Authentication Code (HMAC) digest. Further, trilateration is used to calculate the coordinates of the unknown nodes.

In the paper [183] by Garg et.al., the proposed algorithm uses iterative gradient descent with selective pruning of inconsistent measurements to achieve high localization accuracy. The authors have also shown the accuracy of estimated location in mobile environment but have not emphasized on the external nodes or elementary attacks. The proposed algorithm has not addressed the issue of false alarm.

In the paper [184] by Jadliwala et. al., different class of distance based localization algorithms have been classified. The authors have also proposed a polynomial-time algorithm and two heuristic-based algorithms using a threshold value of the compromised nodes. Using this threshold value, the bounded error can be measured and verified.

In the paper [185], by Mi et. al., a novel approach of secure localization has been observed. The authors have used GPS systems and inertial guidance modules on special master node to provide the location accuracy. They have also used an efficient key-distribution process in the algorithm.

In the paper [186] by Shu et. al., the authors has shown an encryption based secure localization algorithm. The proposed algorithm, based on Paillier cryptosystem, provides a multilateral privacy preserving solution for secured least square estimation. The authors have generated overdetermined linear system and have developed three privacy-preserving solutions by leveraging combinations of information-hiding and homomorphic encryption. The proposed algorithm does not need to open up the anchor nodes location information.

In the paper [187] by Srinivasan, a novel approach of secured localization using CDS is discussed. CDS is applied for both anchor nodes and sensor nodes. The proposed approach is applied on a static network. Only anchor nodes participate in CDS construction phase. Rule-k algorithms are also used in this approach. Beacon nodes execute a neighbour discovery algorithm to differentiate among beacon and sensor neighbours of each beacon node.

In the paper [188] by Zhu et.al., the proposed method uses triangle inequality to detect the attack and then applies localization process based upon some reference points. Both the processes use voting mechanism. The approach is modular having harness simple geometric triangular rules and an efficient voting technique to enable the attack detection module, which identifies and filters out malicious location references. A secure localization module is invoked that computes and clusters certain reference points, and the position of the concerned regular node is estimated with the centroid of the most valuable reference points identified.

In the paper [189] by Jha et.al., a novel approach of using game theory has been applied in the work. The proposed algorithm combines two methods: Least Trimmed Square (LTS) algorithm is used in regression to identify and remove regression factors which are anomalous and Game Theoretic Aggregation (GTA) solves the problem of combining outputs from a number of predictors to generate a more accurate predictive model. To improve the performance of LTS, a single phase weight-based combination of factors is used by combining GTA with LTS, without any threshold specification.

In the paper [190] by Merhi et. al., the use of decentralized dynamic key generation for secure localization has been researched. The proposed algorithm uses symmetric key which are autonomous and never transmitted over. Further, the algorithm uses bitwise XOR operations and produces robustness with low overhead.

In the paper [191] by Chang et. al., the authors have shown a smart card based approach. The proposed algorithm implements a secure and lightweight authentication scheme for heterogeneous wireless sensor networks using smart cards and dynamic identities to prevent threats to users' privacy. The algorithm is cluster based and cluster heads are responsible for mutual authentication and key agreement. The algorithm consists of five phases, i.e., initialization, registration, login, mutual authentication and key agreement, and changing passwords.

In the paper [192] by Lin et. al., mutual trust in wireless sensor network has been discussed. The algorithm pre-distributes the random keys securely and uses identity based cryptography. In the proposed approach, base station assigns an identity and adds n number of secrets into the private secret keys for every sensor node. Mutual trust is built up based on the identities and keys among the neighbourhood nodes.

In the paper [193] by Rashid and Mahapatra, a three tier security framework is shown. The proposed framework uses two polynomial pools: the mobile polynomial pool and the static polynomial pool. Authentication mechanism used between stationary access nodes and sensor nodes, makes it more capable to withstand to node replication attacks. One way hashing scheme is also used with static polynomial pools.

In the paper [194] by Liu et. al., the node capture attacks and flooding of packets in DV-hop localization is addressed. The proposed approach has used broadcast authentication and weight based computation for secure localization purpose. The proposed scheme includes four phase: initialization phase, hop count computation, hop size and weighted computation and location estimation.

Table 3.4: *Literature review of Secure Localization*

| Ref no. | Author(s) | Year | Remarks |
|---|---|---|---|
| [167] | Srinivasan and Wu | 2007 | A comparative study of all the secure localization process has been explained. |
| [168] | Lazos and Poovendram | 2006 | no range measurements are required for localization, sensors do not rely on other sensor nodes for computing their location. |
| [169] | Lazos and Poovendram | 2004 | The localization accuracy is less, either more locators require to be deployed or more directional antennas have to be used. The assumption that no jamming of the wireless medium is feasible is very critical in real world. |
| [170] | Lazos and Poovendram | 2005 | ROPE achieves a significantly lower Maximum Spoofing Impact while requiring the deployment of a significantly smaller number of reference points. |
| [171] | Capkum and Hubaux | 2006 | Verifiable multilateration requires a high number of reference points. It is a centralized approach creating a single point failure problem. Also, it is very unlikely that an attacker will not try to collude with other compromised nodes. |

| | | | |
|---|---|---|---|
| [172] | Srinivasan et.al. | 2006 | Its distributed approach not only alleviates the burden on the base station, but also reduces the damage caused by the malicious nodes by enabling sensor nodes to make a decision on which beacon neighbors to trust, on the fly, when computing their location. |
| [173] | Pandey and Agrawal | 2005 | Consistency will be an issue when the nodes are mobile. |
| [174] | Du et.al. | 2005 | Depends on deployment knowledge to minimize error which may be not feasible for all real life scenarios. |
| [175] | Wang and Xiao | 2008 | Multihop requires critical security measures. |
| [176] | Liu et.al. | 2005 | Consistent beacon signals are not always possible due to different obstacles in the practical scenarios. |
| [177] | Zhang et.al. | 2006 | Local authentication and keys cannot provide full security for jamming and outsider attacks. |
| [178] | Shastry et.al. | 2003 | Compromised insider nodes need to be taken care of. The algorithm should also take care of the verification of the node authentication and authorization. |
| [179] | Apkun et.al. | 2003 | Authentication explicitly provides a strong point for the algorithm. Mobility need to be verified with this algorithm. |

| | | | |
|---|---|---|---|
| [180] | Rasmussen and Apkun | 2008 | Excessive massive change can lead to the resource depletion. Similarly any outsider or insider compromised nodes can get this use of attack. |
| [181] | Han et.al. | 2016 | Water force and water mobility can affect the localization accuracy. |
| [182] | Zhang et.al. | 2012 | The algorithm is simple and can be modified accordingly to apply for other applications. |
| [183] | Garg et.al. | 2012 | The proposed algorithm has not addressed the issue of false alarm. |
| [184] | Jadliwala et. al. | 2010 | Bounded error has been identified for three distance based localization algorithm. They need to be validated for mobile environment. |
| [185] | Mi et.al. | 2012 | Keys need to be distributed only for neighbours else interception ratio will be higher. Further enabling GPS may increase the cost of the network and noise interference will hamper the network. |
| [186] | Shu et.al. | 2015 | Applicable for range based systems only. |
| [187] | Srinivasan | 2011 | CDS reconstruction aspect needs to be done. CDS size is not mentioned explicitly. Attack model need to be emphasized. |

| | | | |
|---|---|---|---|
| [188] | Zhu et.al. | 2011 | Scalability is present in the algorithm but compatibility of the modules can be an issue for WSNs applications. |
| [189] | Jha et.al. | 2014 | The algorithm is applicable for static network. |
| [190] | Merhi et.al. | 2012 | Robust key generation but processing power may exhaust the network if such keys are used. |
| [191] | Chang et.al. | 2016 | Cluster head selection process is not mentioned and algorithm basis of whether it can be applied for range free or range based, that idea is missing. |
| [192] | Lin et.al. | 2016 | Energy consumption needs to be experimented as the message exchange with each sensor nodes with secrets create extra traffic that leads to resource exhaustion. |
| [193] | Rasheed and Mahapatra | 2012 | Node segregation is a critical task as they are classified in mobile sinks, stationary access and general sensor nodes. Stationary access nodes may increase the traffic overhead. |
| [194] | Liu et.al. | 2015 | Insider node verification required because it creates more severe impact on the network. |

# CHAPTER 4

# An Improved DV-Hop Algorithm with Minimum Connected Dominating Set for Mobile Nodes

## 4.1 Introduction

The use of Wireless Sensor Networks (WSNs) enhances variety of applications ranging from habitat monitoring, target tracking, disaster management and many more. The advancement in Micro Electro Mechanical Systems technology, such applications of WSNs extend to a wider zone due to compactness of nodes. Out of these, localization is one of the fields that always demands attention of researchers' community. The sensor nodes are spatially distributed over a wide area. Thus tracking the actual location of a wireless node is always has been considered as a challenging task. The computation process of localization should be such that it consumes least amount of time and resources with accurate location estimation. The inclusion of Global Positioning System(GPS) modules would not turn out as an optimum solution where there is a line of sight problem exists. Therefore, location estimation depending upon the anchor nodes' priori known location comes into existence. The nodes whose location are computed based on these anchor nodes are known as unknown nodes. Basically, the localization approaches are divided into two broad categories: a) range based and b) range free [26]. In range based approach, there are certain inbuilt hardware devices attached with sensor nodes that guide them regarding location information such as inclusion of GPS within a node. Some special hardware are also used to apply the techniques including Angle of Arrival (AoA)[46][47],Time Difference of Arrival(TDoA)[48][49],Time of Arrival(ToA)[42] etc. On the other hand, in range free approaches the nodes generate the location information taking the required data from their neighbour nodes. There are various algorithms in the past that work on range free mechanism such as DV-Hop.

## 4.2 DV-Hop Localization

The American Drags Niculescu [53] proposed the DV-Hop localization algorithm using the distance vector routing protocol and GPS positioning principle. The basic idea of the algorithm is to calculate distance between the unknown node and the anchor nodes with the product of hop distance and the average number of hops among nodes. Using trilateration method position of unknown nodes are calculated. DV-Hop algorithm follows three stages. Firstly, using distance vector exchange agreement, anchor nodes broadcast its own information to its neighbouring nodes. Anchor nodes contain the information $(id_i, h_i, x_i, y_i)$ where $id_i$ refers to the serial number of anchor nodes, $h_i$ refers to the current hop count initialized to zero, $(x_i, y_i)$ refers to the current anchor node azimuth coordinate information. The second stage uses the following formula to estimate average distance for one hop and is given by:

$$hops_i = \frac{\sum \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum(h_i)} i \neq j \tag{4.1}$$

Among them $(x_i, y_i)$ and $(x_j, y_j)$ are anchor node A and anchor node B with their coordinate information, $h_i$ is hop count between A and B anchor nodes. Although there are multiple anchor nodes in the network, but the unknown node accepts only one of average. The third stage uses the trilateral measurement method for the unknown nodes azimuth estimation. The distance between the anchor nodes are given by the equation:

$$(x_N - x)^2 + (y_N - y)^2 = d_{Nu}^2 \tag{4.2}$$

where $N$ is number of anchor nodes and we can get $N$ such equations. $(x_i, y_i)$ for $[i = 1, 2, ....N]$ denotes anchor node i's coordinate information, $d_{iu}$ is the distance from unknown node $U$ to the anchor node $i$. The above equation for$[i = 1, 2, ....N]$ can be transformed [140] into the $AX = b$ form where,

$$A = \begin{vmatrix} (x_1 - x_{\mathrm{N}}) & (y_1 - y_{\mathrm{N}}) \\ . & . \\ . & . \\ (x_{\mathrm{N\text{-}1}} - x_{\mathrm{N}}) & (y_{\mathrm{N\text{-}1}} - y_{\mathrm{N}}) \end{vmatrix} \tag{4.3a}$$

$$X = \begin{vmatrix} x \\ y \end{vmatrix} \tag{4.3b}$$

$$b = \frac{1}{2} \begin{vmatrix} d_1^2 - d_N^2 + d_{Nu}^2 - d_{1u}^2 & \\ d_2^2 - d_N^2 + d_{Nu}^2 - d_{2u}^2 & \\ . & . \\ . & . \\ d_{N-1}^2 - d_N^2 + d_{Nu}^2 - d_{N-1}^2 & \end{vmatrix} \tag{4.3c}$$

Equation $AX = b$ is available for the standards of Least-Square solution to provide the value of x given by, $x = (A^T A)^{-1} A^T b$.

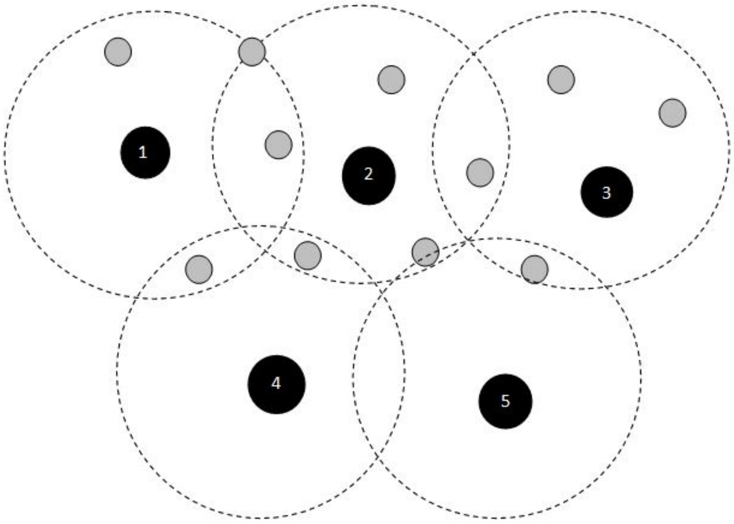


FIGURE 4.1: *Shows the Topology and aerial distances between the radios.*

## 4.3 Proposed Algorithm

We know that, in WSNs anchor nodes are more privileged in the term of resources and communication.Thus utilizing the anchor nodes in an efficient way is the prime goal of our research. In the proposed algorithm, we have considered the unknown nodes in one-hop neighbourhood of each anchor node. Among all the anchor nodes in the set, we have selected only those anchor nodes which are having maximum degree of connection with one-hop distanced unknown nodes. Such anchor nodes have created the dominating set of anchors. This dominating set acts as the backbone of the network to localize the unknown nodes. Finally pruning is also used to minimize the size of the dominating anchor nodes and to avoid redundancy. For example, consider the Figure 4.1.

The black color nodes numbered from 1 to 5 are the anchor nodes. All the grey color nodes are the unknown nodes in the network. The maximum degree of connectivity will be calculated for each of the anchor nodes depending upon two considerations: range and one-hop neighbours. If two anchor nodes are having same degree of connection, one anchor node among them will be randomly chosen for the dominating set at a particular iteration. Considering our algorithm for the above example, let's suppose the anchor node numbered 2 has the maximum degree of connectivity with the unknown nodes as it has six neighbours in its range. So, in the first iteration, anchor node numbered 2 is in the dominating set. Similarly, anchor nodes numbered 1 and 3 also become members of that set. These anchor nodes (1, 2 and 3) are covering all the unknown nodes in their vicinity and therefore there is no need of adding anchor node 4 and anchor node 5 in the dominating set as the neighbours of these anchor nodes are already the neighbours of anchor nodes 1, 2 and 3 respectively. This dominating set is connected and however contains the minimum number of nodes as of three (minimum requirement for trilateration) out of five anchor nodes to cover up all the unknown nodes and therefore it is considered as Minimum Connected Dominating Set (MCDS).

### 4.3.1 Description of proposed algorithm

A set of anchor nodes $A$ and a set of unknown nodes $U$ have been initialized. An empty dominating set $D$ is initialized to $\Phi$ which further contains the anchor nodes that are the members of MCDS. Maximum degree of the anchor nodes in set $A$ is calculated. The anchor node having the maximum degree of connectivity becomes a member of the dominating set $D$. The process continues till either all the anchor nodes are the member of $D$ or all the unknown nodes are one hop neighbour of any anchor node that is a member of $D$ and the number of anchor nodes in the dominating set is greater than equal to three. The number of anchor nodes for dominating set should be more than three as to perform trilateration. Pruning method is used to reduce the size of dominating set such that all the unknown nodes are covered up by the minimum number of anchor nodes. Once MCDS is constructed, trilateration is applied on anchor nodes to get the location estimation of unknown nodes. The process is summarized in Algorithm 1. The calculation of maximum degree in the set of anchor nodes has been proposed in Algorithm 2. The anchor node set A is given as input for this algorithm. For each of the anchor nodes in the set A its degree is initialized to 0. The connection status with unknown nodes is checked for each of the anchor nodes in the network. If the connection status is true, degree of the corresponding anchor node is increased by 1. Thus, once the degree of all the anchor

**Algorithm 1** Generating Backbone with Anchor Nodes

```
 1: procedure LOCATION ESTIMATION FOR UNKNOWN NODES
 2:     Initialize:- $A \leftarrow \{a_1, a_2, ........., a_N\}$ (Anchor Nodes),
 3:                  $U \leftarrow \{u_1, u_2, ........., u_n\}$ (Unknown Nodes)
 4:     Domination Set $(D) \leftarrow \Phi$ (Dominating Set is Empty)
 5:     while { True } do
 6:         if $(\forall\ a_i \in D \parallel \forall\ u_i \in (\exists\ N(a_i))$ && $(D(a_i) \geq 3))$ then
 7:             Break while loop    ▷ if all anchor nodes are in dominating set or all
       the unknown nodes are one-hop neighbour of any anchor node and No. of anchor
       nodes in dominating set is $\geq 3$
 8:         else
 9:             Compute $Max\_degree[A]$    ▷ calling Max_degree[] for the set A
10:             $D = D \cup a_d$    ▷ Generating dominating set with Anchor Nodes
11:             $\{A_j\} = \{A_{j-1}\} - \{a_d\}$
12:         end if
13:     end while    ▷ Iterate until condition in 7 is achieved
14:     Prune (D)
15:     Compute Trilateration on the set D
16: end procedure
```

nodes are received, the maximum degree is calculated and the anchor node with its degree is processed.

**Algorithm 2** Calculation on Maximum Degree from Anchor Set

```
 1: procedure ANCHOR NODE HAVING MAXIMUM DEGREE
 2:     Initialize:- The Anchor Set in algorithm 1 operation 2
 3:     for all Anchor Node $\{A\}$ do
 4:         Initialize $deg[a_i] \leftarrow 0$;    ▷ 'i' is the index variable for anchor nodes
 5:         for all Unknown Nodes $\{U\}$ do
 6:             Compute $connection\_status$;
 7:             if $connection\_status = true$ then
 8:                 $deg[a_i] = deg[a_i] + 1$;
 9:             end if
10:         end for
11:     end for
12:     compute Maximum $(deg[A])$;    ▷ Calculate maximum degree in the set of
       Anchor Nodes
13:     Return $(a_d)$;    ▷ return the Anchor Node having maximum degree
14: end procedure
```

To check the connection status between an anchor node and an unknown node, the process is depicted in Algorithm 3.

Each anchor node broadcasts a ReQest Neighbour Set (RQNS) packet which consists

**Algorithm 3** Checking Connection Status between Anchor Node and Unknown Node

```
procedure CONNECTION STATUS BETWEEN $a_i$ AND $u_j$
    Input Anchor Node $a_i$ and Unknown Node $u_j$
Broadcast by Anchor Node $a_i$
    Send $RQNS : \{SrcAddr, Leash\_C = 1, I\_SEQ, Accept\_S = 0\}$
On Receiving node $u_j$ Compute
    $Leash\_C = Leash\_C - 1;$
    $Accept\_S = 1$
    Send $RPNS : \{SrcAddr, Leash\_C, I\_SEQ, Accept\_S, U\_Addr\}$
    if $Leash\_C = 0$ && $Accept\_S = 1$ then
        Return $True$;
    else
        Return $False$;
    end if
end procedure
```

the source address (*SrcAddr*), leash count variable (*Leash_C*), sequence number of the request packet (*I_SEQ*) and acceptance status (*Accept_S*). The variable *Leash_C* is used to control hop count to 1 and therefore initialized to 1. *Accept_S* is initialized to 0. On receiving RQNS, each unknown node who are in one hop neighbourhood they reply with RePly Neighbourhood Set
$(RPNS) : SrcAddr, Leash\_C = 0, I\_SEQ, Accept\_S = 1, U\_Addr$. *U_Addr* is the address of the unknown address from where the RPNS is coming to the corresponding anchor node. After receiving the RPNS, the anchor node checks the values of *Accept_S* and *Leash_C*. If *Accept_S*=1 and *Leash_C*=0, then the anchor node enlist the corresponding *U_Addr* as its one hop neighbour.
To calculate the maximum degree from the anchor node set, an array consisting degree of all anchor nodes has been taken as input. The first anchor nodes degree is initialized to be the maximum and then compared with rest of all anchor nodes' degree. Finally the index of the node having maximum degree is returned to Algorithm 1. The method is shown in Algorithm 4.

It may happen that single unknown node is a neighbour of more than one anchor node. To avoid such redundancy and to have the minimum number of anchor nodes in the dominating set D, pruning method, as shown in Algorithm 5, is applied that

**Algorithm 4** Calculate Maximum ($deg[A]$)

```
procedure ANCHOR NODE HAVING MAXIMUM DEGREE
    $Max \leftarrow deg[a_0]$;    ▷ degree of Anchor Node $a_0$ has been assigned to the variable $Max$
    for All Anchor Nodes do
        if $deg[a_i] > Max$ then
            $Max = deg[a_i]$
            $d = i$    ▷ Storing the index of anchor node having maximum degree
        end if
    end for
    return ($a_d$);    ▷ return the index of anchor node with highest degree
end procedure
```

**Algorithm 5** Pruning of Dominating Set D

```
procedure MINIMUM DOMINATING SET
Input Dominating Set D
    if $(D(a_i) > 3)$ then    ▷ No. of anchor nodes in dominating set D is greater than 3
        $min \leftarrow min\_degree(D)$
        if $N[min] \subset N[a_1] \cup N[a_2] \cup ...... \cup N[a_n]$ then
            $D = D - \{min\}$;
            $Prune(D)$;    ▷ Recursively call Prune after deleting min from dominating set
        else
            $Prune(D - \{min\})$    ▷ Recursively call Prune excluding min but not deleting from dominating set
        end if
        return D
    else
        return D
    end if
end procedure
```

returns the MCDS which acts as backbone to locate the unknown nodes.

## 4.4 Network Model

The sensor network is modeled using a graph $G = (V, E)$ where V represents the nodes (both the anchor and unknown nodes) and E represents the connectivity set. Considering $a$ as anchor node, $u$ as unknown node and $a, u \in V$, $(a, u) \in E$ iff $a$ and $u$ are within one hop neighbourhood transmission range. The dominating set of graph $G$ is $D \subseteq V$ such that $D$ consists of only anchor nodes and each non-anchor node in $V$ is an one hop neighbour of atleast one anchor node in $D$. A connected dominating set for a given graph $G$ is a dominating set $D$ with the feature that the nodes in $D$ must create a connected subgraph. The minimum connected dominating set for the graph $G$ can be defined as a dominating set $D \subseteq V$ such that $D$ consists only minimum number of anchor nodes and all non-anchor node in $V$ is an one hop neighbour of atleast one anchor node in $D$.

### 4.4.1 Design Parameters

The features of the nodes and the overall network take part to create significant effect in the efficiency of localization. We have considered such features as design parameters of our proposed localization algorithm including connectivity, transmission range and local stability. Each of these metrics has its own priority depending on the service or application. Parametric weights are therefore needed to be included with those design parameters.

*Node degree:* Each anchor node computes its degree of connectivity with its neighbour nodes defined the Algorithm 3. The degree of an anchor node $a$ is the total number of unknown nodes within its one hop distance and is computed as:

$$Deg_a = \sum a \in V, a \neq u \quad \{hop_{a,u} = 1\} \tag{4.4}$$

where $Deg_a$ is the total degree of an anchor node $hop_(a, u)$, is the one hop distance between anchor node $a$ and unknown node $u$, which is one in our case.

*Transmission Range:* The transmission range $T_r$ of an anchor node is dependable on the application scenario. As network scenario is considered to be dynamic, transmission range varies within the interval of minimum range $T_{rmin}$ and maximum range

$T_{rmax}$. The transmission range $T_r$ is therefore given by

$$T_r = T_{rmin} + Random(0,1) \times (T_{rmax} - T_{rmin}) \tag{4.5}$$

where $Random(0,1)$ generates a randomized number between 0 and 1.

*Mobility:* To compute the mobility, each anchor node in the dominating set requires to calculate the distance from its neighbouring unknown nodes. For this purpose, Friis free space propagation model [195] is used. The received power $P_r$ is computed as:

$$P_r = P_t \times G_t \times G_r \times \frac{\lambda^2}{(4 \times \pi\mathcal{D})^2} \tag{4.6}$$

where $P_r$ is the power received by receiving antenna of the anchor node, $P_t$ is the power input to the transmitting antenna, $G_t$ and $G_r$ are the transmitting gain and receiving gain respectively, $\lambda$ is the wavelength and $\mathcal{D}$ is the distance with the condition $P_r$ is inversely proportional to the square of the distance. An approximate distance at time $t$ between an anchor node a $\in$ dominating set $D$ and an unknown node $u$ is calculated as:

$$Dist_t^{a,u} = \frac{k}{\sqrt{P_r}} \tag{4.7}$$

Where $k$ is constant and $Dist_t^{a,u}$ is the distance between $a$ and $u$ at time $t$.
Relative mobility in the network indicates whether any two nodes are coming closer to or moving away from each other. The relative mobility of an unknown node $u$ with respect to anchor node $a$ at a given time $t$ is given by:

$$RM_t^{a,u} = Dist_t^{a,u} - Dist_{t-1}^{a,u} \tag{4.8}$$

where $RM_t^{a,u}$ is positive if node u is moving away from $a$ and negative if $u$ is coming closer to $a$. The distance from $a$ to $u$ is measured at certain time interval for $T$ times and we get the values $RM_1^{a,u}$, $RM_2^{a,u}$...........$RM_T^{a,u}$. The standard deviation of relative mobility ($SD_{RM}$) defines the variation of the distances over a period of time $T$ as,

$$SD_{RM} = \sqrt{\frac{\sum_{i=1}^{T}(RM_i - \overline{RM})^2}{T}} \tag{4.9}$$

Where,

$$\overline{RM} = \frac{1}{T}(RM_1^{a,u} + RM_2^{a,u} + ...... + RM_T^{a,u}) \tag{4.10}$$

## 4.5 Implementation and results

In the simulation process, we have considered the number of nodes as 25, 50, 75, and 100 respectively. The graphs shown in Figure 4.2 depict the comparison of number of anchor nodes participated in location estimation of unknown nodes with the number of unknown nodes respectively. The DV-Hop algorithm and proposed algorithm have been compared on this aspect. Through results we can observe that proposed algorithm generates a better result i.e. less number of anchor nodes are able to localize all the unknown nodes. The simulation data of proposed algorithm has been statistically analyzed.

The localization error is inexorable in evaluations. we have considered two metrics to calculate the localization error. The metrics can be described as:

*Average Localization Error*: It is defined as the ratio of the difference between estimated location and the actual location of all the nodes

$$Average\ Localization\ Error = \frac{1}{N}\sum_{i=1}^{N}\sqrt{(x_i - x)^2 + (y_i - y)^2} \tag{4.11}$$

*Root Mean Square Error*: It is defined as mean square root of squared differences of estimated location and the actual location.

$$Root\ Mean\ Square\ Error\ = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - x)^2 + (y_i - y)^2} \tag{4.12}$$

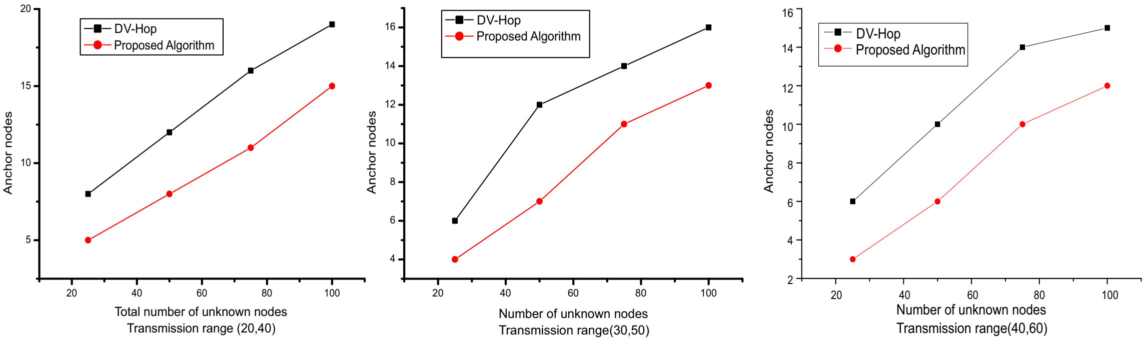


FIGURE 4.2: *Localization of unknown nodes with different transmission range*

where, $(x, y)$ are actual locations, $(x_i, y_i)$ are estimated locations and $N$ denotes the number of nodes.

The average localization error for different transmission range with variable anchor and unknown nodes has been shown in table 4.1.

TABLE 4.1: *Average Localization Error(%)*

| Transmission Range (Min, Max) | No. of Anchor Nodes | Average Localization Error (%) for all the scenarios of 20,40,60,80 and 100 unknown nodes |
|---|---|---|
| 20,40 | 5 | 10.113 |
| | 10 | 9.762 |
| | 15 | 8.001 |
| | 20 | 7.997 |
| 30,50 | 5 | 8.321 |
| | 10 | 8.007 |
| | 15 | 7.147 |
| | 20 | 6.009 |
| 20,40 | 5 | 8.121 |
| | 10 | 6.735 |
| | 15 | 5.989 |
| | 20 | 5.334 |

### 4.5.1 Statistical Analysis of Data

The objective of the statistical analysis is to check whether our introduced algorithm is providing an error improvement over the DV-Hop algorithm or not. To examine this, we have set our hypothesis as per the following.

$H_0$: There is no improvement of localization error in our algorithm as compared to the DV-Hop algorithm.

$H_1$: There is a significant improvement of localization error in our algorithm as compared to the DV-Hop algorithm. To test the above hypothesis, the NS2 simulated data is processed for paired T-test with 0.05 of significance level. We have executed the paired T-test on the average localization error and root mean square error of DV-Hop algorithm and the proposed algorithm. The application of paired T-test has provided the following results shown in table 4.2.

Table 4.2: *Paired T-test Results*

| Number of Unknown Nodes | P-values(Sig. 2 tailed) of paired T-test for Average Mean Error | P-values(Sig. 2 tailed) of paired T-test for Root Mean Square Error |
|---|---|---|
| 25 | 0.001 | 0.000 |
| 50 | 0.000 | 0.001 |
| 75 | 0.000 | 0.000 |
| 100 | 0.000 | 0.000 |

In the above results of Paired T-test, it is observed that all the p-values (Sig. 2 tailed) are < 0.05 of significance level. Therefore the null hypothesis $H_0$ has been rejected and the alternate hypothesis $H_1$ has been accepted. It means that there is a significant improvement using the proposed algorithm over DV-Hop Algorithm with respect to average localization error and root mean square error for location estimation.

Table 4.3: *Paired T-test Results for time consumption*

| Number of Unknown Nodes | P-values(Sig. 2 tailed) of paired T-test for time |
|---|---|
| 25 | cannot be determined as standard error of the difference is zero |
| 50 | cannot be determined as standard error of the difference is zero |
| 75 | cannot be determined as standard error of the difference is zero |
| 100 | 0.000 |

Considering the scenarios of 25, 50 and 75 nodes, the standard error of the differences between the time consumption of DV-Hop Algorithm and the time consumption of proposed algorithm are 0 and therefore, p-value cannot be computed. It means that the time for localization is neither degraded nor upgraded using the proposed algorithm. But it is noticed in the results of 100 nodes given in the table 4.3, that the p-value is 0 which is $< .05$ of significance level. It means that the algorithm is also providing an improvement in time consumption of localization.

## 4.6 Conclusion

In this chapter, an algorithm for localization in wireless sensor network with effectively utilizing anchor nodes is proposed. The algorithm uses the concept of Minimum Connected Dominating Set with anchor nodes which can cover all the unknown nodes for location estimation. The mobility factor for both the anchor nodes and unknown nodes is considered for the algorithm which can be used for wide range of applications. Simulation results show the efficiency of the proposed algorithm that achieves approximately 95% accuracy level of estimated location of unknown nodes along with the random mobility.

# CHAPTER 5

# Energy Efficient and Optimized Load Balanced Localization

## 5.1 Introduction

Localization defines the estimation of location of unknown nodes deployed in Wireless Sensor Networks (WSNs)[27]. Variety of applications of wireless sensor network ranges from environment conditions observation, agriculture, smart home environment, defence environment etc. The dynamic need of the technology and human requirement has made the WSNs from static to mobile. The mobility is incorporated in the environment for the robust output of an observation. In mobile environment estimating the location of unknown nodes is more critical. The accuracy of the location estimation in such networks depends on two basic processes[26]. The first one is location estimation [56] that deals with the calculation of unknown nodes' location and the second process is location verification [56], which verifies the calculated location with the actual location. Numerous algorithms have been introduced to improve the accuracy level of the localization process.

The wireless sensors are resource constrained. The anchor nodes are privileged in this regard with more power resources, but the unknown nodes are not having such resources to utilize. To perform a heavy computational task, the sensor nodes become exhausted and therefore either it has to be replaced or the communication at that part of the sensor node will be untouched further. But, the replacement of such sensors becomes vital and infeasible in some applications due to the dynamic configuration. Thus, the localization process should be efficient in the terms of resource utilization. To dynamically allocate the load among anchor nodes load balancing has been introduced in the localization process[11]. The objective behind distributing the load among anchor nodes for location estimation is to increase network lifetime[12].

## 5.2 Proposed Network Model

The first consideration of the network model is to be self-organizing that is having no central control of deploying the sensor nodes in the network. The sensor network model $\mathcal{N}$ has been considered to be in Two-Dimensional (2-D) and is represented by a graph $G(V, E)$ consists of $V$, a set of vertices and $E$, a set of edges. The connectivity in such a network is an important parameter to analyse the overall performance metrics in localization algorithm. The size of the network can be defined as:

$$|\mathcal{N}| = |A| + |U| = |V| \tag{5.1}$$

Where, $|A|$ is the size of anchor node set $A$, $|U|$ is the size of the unknown node set $U$ and $A, U \subseteq V$. The nodes are located within a plane and locations are defined by the coordinates $(x_i, y_i)$. The plane is assumed to be squared plane consists of $M \times M$ discrete points. The transmission area is also considered to be a circle where the centre of the circle consists of the corresponding node itself. The transmission range is predefined and variable transmission range can be used for different anchor nodes. The average range for each transmission is computed as:

$$R_{avg} = \frac{min \sum_{e\varepsilon\ E} \psi(|e|)}{m} \tag{5.2}$$

Where $m$ is the number of anchor nodes in the network, $\psi(|e|)$ is the weighing function of a connection between an anchor node and an unknown node and interpreted as:

$$\psi(|e|) \sim |e|^{\alpha}\ where\ 2 \leq \alpha \leq 4 \tag{5.3}$$

The weighing function also calculates the average weight for each of the connectivity between an anchor node and unknown node as:

$$R_{avg} \sim c(\alpha, \varepsilon) \frac{n^{(\varepsilon-\alpha)/d}}{m}\ where\ 0 < \alpha < \varepsilon \tag{5.4}$$

where $c(\alpha, \varepsilon)$ is a positive constant with probability 1 and also depends upon the signal attenuation factor $\alpha$ and Euclidean distance space $\varepsilon$.
As the number of nodes can be different in different time interval, the expected number of connectivity for each anchor node in the network can be given as

$$\zeta = \frac{|U|}{M^2} \pi r^2 \tag{5.5}$$

$G'(V', E') \subseteq G(V, E)$, where $G(V, E)$ is the original sensor network scenario and $G'(V', E')$ consists only of the dominator anchor nodes of the dominating set $D$ and its links to the unknown nodes $u_1, u_2, ..., u_n \in U$, the set of unknown nodes, such that $\forall\ u_i,\ a_j \in V'\ , where\ i = 1, 2, ...n\ and\ j = 1, 2, ..., m.$ All the unknown nodes in the set $U$ are the one hop neighbours of any anchor node present in the dominating set $D$ such that $D \subseteq A$, the set of anchor nodes $a_1, a_2, ..., a_N$, $V'\ \subseteq\ V$ and $V' = D\ \cup\ U.$ Dominating set $\theta$ value for the dominating set $D$ given as:

$$|D_\theta| = \left( \sum_{i=1}^{m} |d_i - \bar{d}|^\theta \right)^{\frac{1}{\theta}} \tag{5.6}$$

where $d_i$ is the degree of each dominator in the set $D$ and $\bar{d}$ is the mean of all the degrees of the dominator in the set $D = \{d_1, d_2, ..., d_m\}$.

The calculation of allocation scheme value is defined as:

$$|Al_\theta| = \left( \sum_{i=1}^{m} |d'_i - \zeta|^\theta \right)^{\frac{1}{\theta}} \tag{5.7}$$

It is considered that, there are $m$ disjoint sets for $m$ anchor nodes present in the set $D$, such that $N(a_i) \cap N(a_j) = \phi$ and $\forall\ u_i \in N(a_i)$, $1 \leq i \leq m$ and $u_i \neq u_j$, so that $(u_i, a_i) \in E'$. $d'_i$ is the valid degree of an anchor node $a_i$, i.e., the number of unknown nodes already allocated to the anchor node $a_i$.

### 5.2.1 Optimized backbone creation using Genetic Algorithm

Genetic Algorithms (GAs) helps to search for the heuristic optimum solution for the given problem. It works with the population of chromosomes that are made up of genes. Each chromosome is provided a fitness score which indicates accuracy of the solution. Depending upon the fitness score, fittest chromosomes are selected to execute the process of reproduction by crossover with other chromosomes in the population. This crossover produces offsprings which adopts some good features of current generation. The highly fittest chromosomes are selected for the crossover, the new generation after the crossover contains a higher ratio of the features possessed by the fittest chromosomes of the previous generation. Over the generations, GAs provide the optimal solution to a given problem. The method of applying genetic algorithm in our backbone construction process has been explained below.

i. Identifying Genes and Chromosomes

Each unknown node in the network is allocated to one of the anchor node in the network. Each anchor node is mapped to a chromosome. This mapping corresponds to the gene values of our chromosomes in the population given as:

$$C^g = \{C_j^g | 1 \leq j \leq m,\ C_j^g = (g_1, g_2, ..., g_n)|\} \tag{5.8}$$

Where $m$ is the number of chromosomes in each generation of population

$$g_i = \begin{cases} 1 & \text{if } u_i \text{ is allocated to } a_j, 1 \leq i \leq n \text{ and } 1 \leq j \leq m,\ a_j \in D \\ 0 & \text{else} \end{cases} \tag{5.9}$$

Additionally, the meta-gene value is calculated as all the options of unknown nodes which come into the one hop neighbourhood of a particular anchor node. The generation of chromosomes with meta-gene values is given as:

$$C^G = \{C_j^G | 1 \leq j \leq m,\ C_j^G = (G_1, G_2, ..., G_n)|\} \tag{5.10}$$

Where $m$ is the number of chromosomes in each generation of population and for $1 \leq i \leq n$,

$$G_i = \begin{cases} 1 & \text{if } u_i \text{ is onehop neighbour to } a_j, 1 \leq i \leq n \text{ and } 1 \leq j \leq m,\ a_j \in D \\ 0 & \text{else} \end{cases} \tag{5.11}$$

For example, consider the network scenario of three anchor nodes $\{A1, A2, A3\}$ and seven unknown nodes $\{U1, U2, U3, U4, U5, U6, U7\}$, as shown in the Figure 5.1. The doted lines represent the one-hop neighbourhood and the solid lines represent the allocated nodes. Figure 5.2. represents the chromosomes with meta-genes for the anchor nodes as: $C_1^G, C_2^G$ and $C_3^G$. The meta-gene value, $G_i$, represents the neighbourhood among nodes i.e. the value is 1 in the meta-genes, if the corresponding unknown node $u_i$ is one hop neighbour of the corresponding anchor node $a_j$, where $i = 1, 2, .., 7$ *and* $j = 1, 2, 3$. Similarly, chromosomes with gene representation, shown in Figure 5.3, provides the view of allocation of unknown nodes with one hop neighbourhood to an anchor node. If the value of gene $g_i$ is 1, it means the corresponding unknown node $u_i$ is allocated to that particular anchor node $a_j$ and 0 elsewhere.

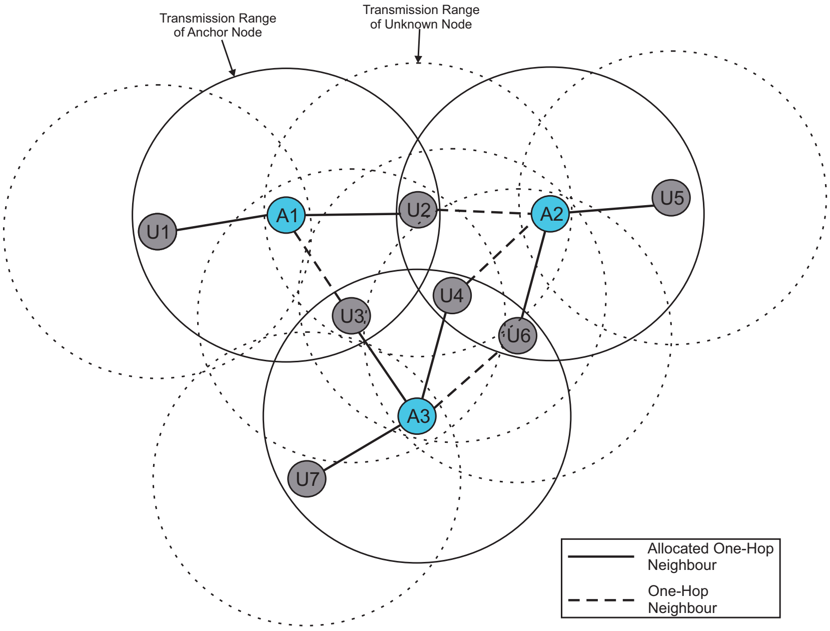

Transmission Range of Anchor Node
Transmission Range of Unknown Node
U1
A1
U2
A2
U5
U3
U4
U6
A3
U7
Allocated One-Hop Neighbour
One-Hop Neighbour

FIGURE 5.1: *Example of Node Allocation.*

After, the representation of chromosomes and encoding of genes and meta-genes, the population need to be initialized for $GA$. In the given problem, the population has been created by considering all the anchor nodes present in the dominating set $D$ and the unknown nodes present in the network.

ii. Creating Fitness Function

|  | $G_1$ | $G_2$ | $G_3$ | $G_4$ | $G_5$ | $G_6$ | $G_7$ |
|---|---|---|---|---|---|---|---|
| $C_1^G$ | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| $C_2^G$ | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| $C_3^G$ | 0 | 0 | 1 | 1 | 0 | 1 | 1 |

FIGURE 5.2: *Meta-Gene Representation*

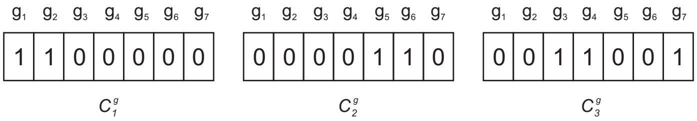


FIGURE 5.3: *Gene Representation*

*GA* provides different sub solution and eventually converged to the optimal one. It is important to formulate the fitness function in such a way that the highly fittest chromosomes can be selected always. The objective of the problem defined in this work is to optimize CDS with minimum $D_\theta$ and $Al_\theta$ values. Therefore the fitness function can be computed as:

$$\begin{cases} f(C_i^g) = \frac{n-|D|}{w_1|D_\theta|+w_2|Al_\theta|} \\ w_1 + w_2 = 1, 0 < w_1, w_2 < 1 \end{cases} \tag{5.12}$$

The linear combination of the two metrics $D_\theta$ and $Al_\theta$ helps to adjust the bias factors $w_1$ and $w_2$ according the network environment. The observation of the above equation emphasizes that the denominator needs to be minimized and the numerator needs to be maximized, so that the overall fitness function will be maximized accordingly.

iii. Selection Process

Selection is an important part of *GAs* in executing the evolution in the population. It should be formulated in such a way that the chromosomes with higher fitness scores need to be selected for mating and crossover. This will help the *GA* to reach to a global optimum point. Rank selection process has been adopted in the purpose. The rank of each of the chromosomes can be given by:

$$R_i = log\,(1 + f(C_i^g)) \tag{5.13}$$

A real valued interval, S, is determined as the sum of the chromosomes' expected selection probabilities given as:

$$P_i = \frac{R_i}{\sum_{j=1}^{m} R_j} \tag{5.14}$$

thus, the value of $S$ can be calculated as:

$$S = \sum_{i=1}^{n} P_i \tag{5.15}$$

Chromosomes are mapped in the contiguous interval of $[0, S]$. A random number generator is used to generate a number in the interval $[0, S]$ and the chromosome whose segment spans the random number is selected. This process is repeated until desired number of chromosomes is selected.

iv. Genetic Operations

The two generic operations, crossover and mutations, are applied here. With the crossover probability $p_c$, two chromosomes $C_i^g$ and $C_j^g$ are selected by using the Rank Selection (RS) process. Two types of crossovers, single-point and two-point are performed randomly in the process. One of the important part in this crossover, that need to be taken care of is the validity of the offsprings after the crossover. Therefore, correction method is also applied for the purpose of getting valid offspirngs for the next generation population. The Figure 5.4 and Figure 5.5 shows the examples of single point and two-point crossover along with their respective corrective methods.

Let us consider that, RS scheme has selected the two chromosomes $C_1^g$ and $C_2^g$ as parent chromosomes. After performing the single point crossover randomly at crossover point at 5 we get the offsprings as shown in Fig. 5.4

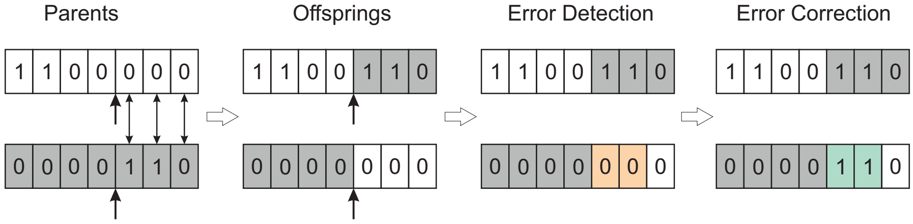


FIGURE 5.4: *Single-point Crossover and Related Correction.*

While performing two-point crossover, two crossover points are needed in between those points, the genes will be going under the operation of crossover for the new offsprings. Randomly two points are selected as, left point $P_L = 2$ and right point $P_R = 5$. All the genes lies between these two points will go for crossover.

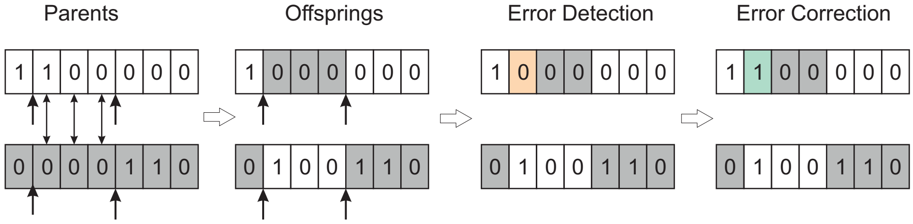


FIGURE 5.5: *Two-Point Crossover and Related Correction.*

The correction process applied for single-point and two-point crossover is same. The genes in the offsprings are scanned one by one whether gene value is 0 or not; it is then matched with original parent chromosome genes (before crossover and mutation). If gene value of the parent chromosome becomes 0 in the offspring after crossover, then in the correction method, we change the gene value of the current offspring from 0 to 1. This correction method will help to get the offsprings among the valid meta-genes solutions and also will help to achieve the local optima within a short period. The changing of values from 0 to 1 signifies the connections among the anchor nodes and unknown nodes along with the fitness value. Moreover, the mutation will help the chromosomes to converge to a global optima.

In similar manner, mutation process is also performed. It just flips one gene value randomly from 0 to 1 or vice-versa with a mutation probability $p_m$. This process is executed to create diversity in the population which helps to identify the global optima. This mutation is also performed in meta-gene to increase the diversity in the dominatees' allocation schemes. In the present work, the process of mutation of meta-gene automated as, the network scenario is random, each time we get the evolution of the meta-genes with better diversity.

v. Replacement of Chromosome

The last step of this GA is to create a new population applying a suitable replacement policy. Using the parent chromosomes, we can get $m$ numbers of offsprings and another $m$ chromosomes by applying mutation operation on meta-genes. In this algorithm, we use $m$ numbers of chromosomes having better fitness scores among those $2m$ numbers of chromosomes. Elitism strategy is used to retain the fittest chromosome over the generations. This property also helps the $GA$ to converge to a solution faster. The algorithm iterates until desired number of generations are reached or the highest fitness value does not change with simultaneously for $l$ number of iterations.

**Algorithm 6** Generating optimized Backbone with Anchor Nodes using CDS

```
1: procedure LOCATION ESTIMATION FOR UNKNOWN NODES
2:     Input:- Dominating set $D \subseteq A$ where $A = \{a_1, a_2, ........., a_m\}$
3:         A set of unknown nodes $U = \{u_1, u_2, ........., u_n\}$
4:     Calculate $|D_\theta| = \left(\sum_{i=1}^{m} |d_i - \bar{d}|^\theta\right)^{\frac{1}{\theta}}$
5:     Calculate expected number of connectivity of each anchor node given by $\zeta$
6:     Calculate the allocation value given as:- $|Al_\theta| = \left(\sum_{i=1}^{m} |d'_i - \zeta|^\theta\right)^{\frac{1}{\theta}}$
7:     Initialize the first generation of chromosomes, $C^g$
8:         and chromosomes with meta-gene $C^G$
9:     Calculate fitness function $f(C_i^g)$
10:    if $f(C_i^g)$ does not change in simultaneously $l$ iterations then
11:        Go to Step 18
12:    else
13:        Apply $R_i = log\,(1 + f(C_i^g))$
14:    end if
15:    Execute crossover, mutation and meta-gene mutation
16:    Apply replacement policy
17:    Go to Step 9
18:    Return the current fittest solution
19: end procedure
```

A Connected Dominating Set (CDS) is an efficient technique to generate a virtual backbone to avoid excessive broadcast in the resource constrained WSNs. In the proposed work, we have considered that the CDS is constructed only with anchor nodes as they are having more energy resources rather than the unknown nodes. It also provides optimized load balanced CDS using genetic algorithm to enhance the network lifetime. Moreover obtaining an optimized CDS, the location estimation process of unknown nodes has been emphasized.

The first part of our proposed approach gets input of a connected dominating set $D$. We have calculated the $\theta$ value of the dominating set $D$ and $\theta$ value of allocation scheme $A_l$. These two values are used to generate the fitness function for the genetic algorithm. Further expected allocated neighbor value $\zeta$ is also calculated.We have also calculate $\theta$ value of the allocation scheme $Al$. These two values have been used to generate the fitness function for the genetic algorithm. The process has been summarized in Algorithm 6.

### 5.2.2 Localization of Unknown Nodes

The second part of the proposed model deals with the localization process. It is assumed that the wireless sensor network is built up by $m$ anchor nodes whose locations are known and $n$ unknown nodes whose locations are unknown. Any node, whether anchor node or unknown node, will have a location interpreted as: $(x_i, y_i)$. The geographical distance between one anchor node and an unknown node can be defined as:

$$d_{a,u} = ||a_j - u_i|| = \sqrt{(x_a - x_u)^2 + (y_a - y_u)^2} \tag{5.16}$$

Where, $(x_a, y_a)$ and $(x_u, y_u)$ are the coordinates of an anchor node and an unknown node respectively, $u_j$ is used to represent an unknown node and $a_i$ as an anchor node.

As the network model is mobile for both the anchor nodes and unknown nodes, Relative Mobility(RM) need to be considered in the network that indicates whether any two nodes are coming closer to or moving away from each other. The relative mobility of an unknown node $u$ with respect to anchor node at a given time $t$ is defined as:-

$$RM_t^{a,u} = d_{a,u_{(t-1)}} - d_{a,u_{(t)}} \tag{5.17}$$

$RM_t^{a,u}$ is positive, if node $u_i$ is moving away from $a_j$ and negative, if $u_i$ is coming closer to $a_j$. The distance from $a_j$ to $u_i$ is measured at certain time interval for $T$ times and we get the values $RM_1^{a,u}$, $RM_2^{a,u}$, ..., $RM_T^{a,u}$. The Standard Deviation of relative mobility ($SD_{RM}$) defines the variation of the distances over a period of time $T$ as:-

$$SD_{RM} = \sqrt{\frac{\sum_{i=1}^{T_m}(RM_i - \bar{RM})^2}{T_m}} \tag{5.18}$$

where,

$$\bar{RM} = \frac{1}{T_m}(RM_1^{a,u} + RM_2^{a,u} + ... + RM_{T_m}^{a,u}) \tag{5.19}$$

We have also considered another metric of proximity information between two anchor nodes depending upon number of hops, given as:

$$p_{i,j} = \begin{cases} 0 & \text{if } i = j \\ \{1, 2, 3, ...\}, & \text{else} \end{cases} \tag{5.20}$$

Now, we can create a proximity vector for each of the anchor node representing the proximity between $i_{th}$ anchor node and other anchor nodes shown as below:-

$$p_i = [p_{i,1}, p_{i,2}, ..., p_{i,m}]^T \quad \in Z^{m\times 1} \tag{5.21}$$

So, using the above equation, the overall proximity matrix for $M \times M$ data points can be given as:

$$\wp = [p_1, p_2, ..., p_m]^T \in Z^{m \times m} \tag{5.22}$$

Similarly, we can create the distance vector $d_i$ and distance matrix $\mathcal{M}$ for the anchor nodes represented as:

$$d_i = [d_{i,1}, d_{i,2}, ..., d_{i,m}]^T \in Z^{M \times 1} \tag{5.23}$$

$$\mathcal{M} = [d_1, d_2, ..., d_m]^T \tag{5.24}$$

Now, the proximity vector $p_{u,i}$ between an unknown node and the anchor nodes is given as:

$$p_{u_i} = [p_{u_{i,1}}, p_{u_{i,2}}, ..., p_{u_{i,m}}]^T \in Z^{m \times 1} \tag{5.25}$$

$p_{u_i}$ can have only two values. $p_{u_i} = 1$, if the unknown node is one hop neighbour of an anchor node, else $p_{u_i} = 0$.

This equation leads to the generation of overall proximity matrix for all the unknown nodes calculated as:

$$\wp_u = [p_{u_1}, p_{u_2}, ..., p_{u_n}]^T \in Z^{m \times n} \tag{5.26}$$

Now, we need a linear transform matrix $T$ to map the proximity matrix $\wp$ to the distance matrix $M$ represented by,

$$T = \begin{bmatrix} t_1 \\ . \\ . \\ . \\ t_m \end{bmatrix} = \begin{bmatrix} t_{1,1} & . & . & . & t_{1,m} \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ t_{m,1} & . & . & . & t_{m,m} \end{bmatrix} \tag{5.27}$$

where $t_{i,j}$ represents the transformation effect of proximity to the $j^{th}$ anchor node on the geographic distance to the $i^{th}$ anchor node.

Following the above matrices and transformation matrix, we can get estimated geographical distances between the $i^{th}$ unknown node and the anchor nodes.

$$L_j = [L_{j,1}, L_{j,2}, ..., L_{j,m}]^T = T\wp_u = \begin{bmatrix} ||a_1 - \bar{u_i}|| \\ . \\ . \\ . \\ ||a_m - \bar{u_i}|| \end{bmatrix} \tag{5.28}$$

where, the estimated position $\bar{u_i}$ satisfies the given series of equations.

$$\begin{array}{ccc} ||a_1 - \bar{u_i}||^2 & & (x_1 - \bar{x_{u_i}})^2 + (y_1 - \bar{y_{u_i}})^2 \\ . & & . \\ . & = & . \\ . & & . \\ ||a_m - \bar{u_i}||^2 & & (x_m - \bar{x_{u_i}})^2 + (y_m - \bar{y_{u_i}})^2 \end{array} \tag{5.29}$$

where, $a_j$, $\forall j = 1, 2, ..., m$, is having coordinates $(x_j, y_j)$ and $u_i$ , $\forall i = 1, 2, ..., n$, having estimated coordinates $(\bar{x_{u_i}}, \bar{y_{u_i}})$.

Lastly, using the standard least square method we get to the solution as:

$$\bar{u_i} = \begin{bmatrix} \bar{x_{u_i}} \\ \bar{y_{u_i}} \end{bmatrix} = (F^T F)^{-1} F G \tag{5.30}$$

where,

$$F = \begin{bmatrix} 2(x_1 - x_m) & 2(y_1 - y_m) \\ . & . \\ . & . \\ . & . \\ 2(x_{m-1} - x_m) & 2(y_{m-1} - y_m) \end{bmatrix} \tag{5.31}$$

and

$$G = \begin{bmatrix} x_1^2 - x_m^2 + y_1^2 - y_m^2 + L_{j,m}^2 - L_{j,1}^2 \\ . \\ . \\ . \\ x_{m-1}^2 - x_m^2 + y_{m-1}^2 - y_m^2 + L_{j,m}^2 - L_{j,m-1}^2 \end{bmatrix} \tag{5.32}$$

The above process is summarized in the Algorithm 7.

**Algorithm 7** Localization

```
procedure INPUT: OPTIMIZED CDS I.E. THE OUTPUT OF THE ALGORITHM 6
    Create proximity matrix $\wp$ for the anchor nodes between inner anchor node communications.
    Create distance matrix $\mathcal{M}$
    Define proximity matrix for unknown nodes.
    Calculate the position with standard least square method.
end procedure
```

## 5.3 Result and Discussion

The proposed algorithm has been simulated in Network Simulator-2 with parameters enlisted in the Table 5.1.

TABLE 5.1: *Simulation parameters and rules*

| Parameters | Values |
|---|---|
| Simulation Area | 100 × 100 $m^2$ |
| No. of Unknown Nodes | 100 to 200 |
| No. of Anchor Nodes | 10 to 40 |
| Mobility | Random |
| Population size | 10 to 40 |
| Selection scheme | Rank Selection |
| Replacement policy | Elitism |
| Crossover probability | 1 |
| Gene mutation probability | 0.2 |
| Meta-gene mutation probability | 1 |

The performance of the algorithm has been analysed in the terms of, localization error and network lifetime.

Localization error is defined as squared error of the estimation given as:

$$e_i = \sum_{k=1}^{m}(d_{i,k} - t_i p_k)^2 = ||d_i^T - t_i \wp||^2 \quad for\ i = 1, 2, ..., m \tag{5.33}$$

and the average localization error as:

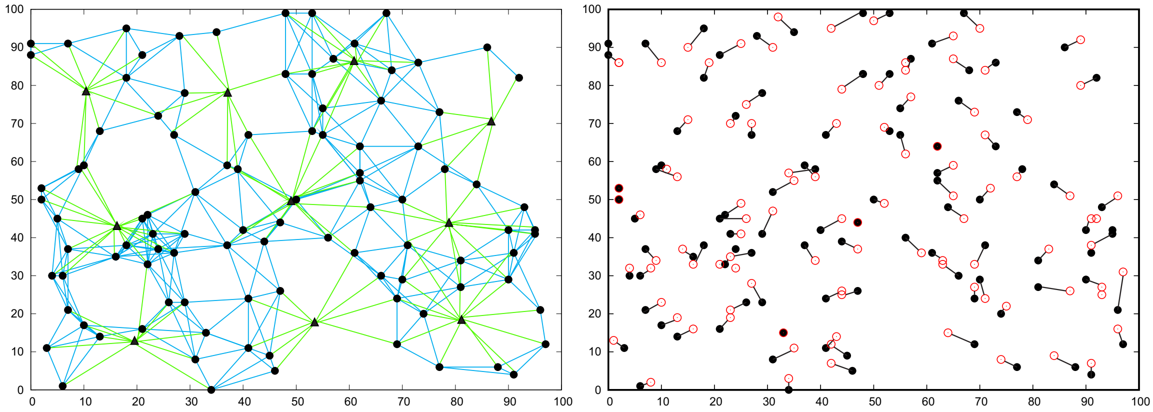
$$e_{avg} = \frac{\sum_{i=1}^{m} e_i}{m} \tag{5.34}$$

The proposed algorithm uses linear energy model for each anchor node given as:

$$Energy_a = c_1 \times R_a \tag{5.35}$$

where $R_a$ is transmission range of anchor node $a_j$ and $c_1$ is defined as:

$$c_1 = \frac{E}{2}(\sum_{i=1}^{m} R_i) \tag{5.36}$$



(a) Actual position of nodes in WSN

(b) Estimated position of nodes

FIGURE 5.6: *Graphical representation of the simulation scenario showing actual vs. estimated nodes position*

where $E$ is the initial energy of anchor node. Network lifetime is calculated in terms of residual energy of the anchor nodes. In the proposed algorithm, anchor nodes computes the position of all unknown nodes and therefore energy consumption of anchor nodes is more rather than the unknown nodes. The residual energy of the backbone of anchor nodes is calculated as the sum of the residual energy of all the anchor nodes at the time $t$ as shown below in Equation 5.37. where $E_{residual_a}$ is the residual energy of anchor node $a$.

$$Energy_{residual} = \frac{\sum_{a\in D} \; E_{residual_a}}{|D|} \tag{5.37}$$

Figure 5.6(a) represents a network scenario at time $t$ in an area of $100m \times 100m$ comprising of anchor nodes (represented as black triangles) and the unknown nodes (represented as black circles). The green solid lines represent the one hop neighbourhood between an anchor node and an unknown node. The solid blue lines represent the overall connection among the unknown nodes. Applying the proposed algorithm, we estimated the location of the unknown nodes (represented by red circle) as shown in Figure 5.6(b) The deviation from the actual position is marked with blue lines from the black circle to the red circle.

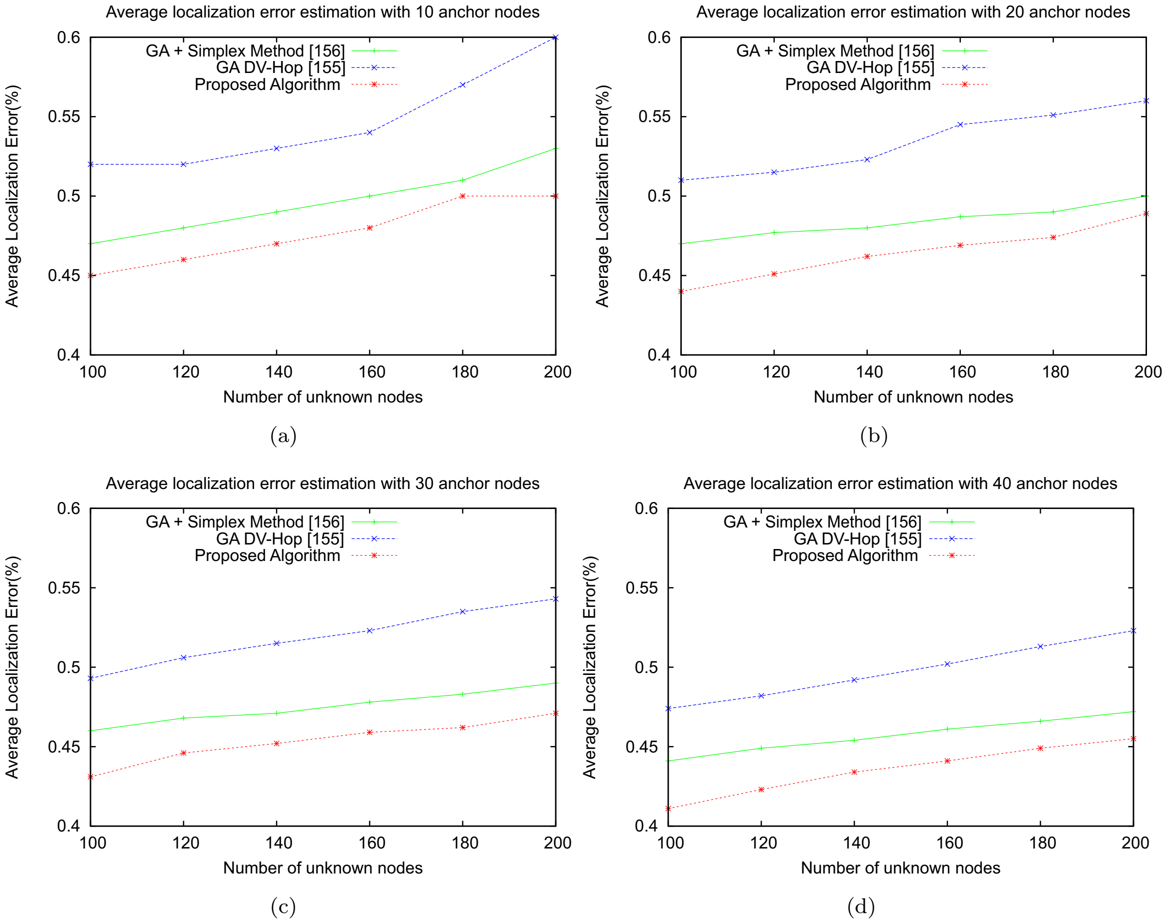
The statistical values of results are shown in the Table 5.2. Results are shown

Table 5.2: *Performance under different parameters*

| Parameters | | Performance | | |
|---|---|---|---|---|
| No. of Anchors | No. of Unknown Nodes | Average Localization Error | No. of anchor nodes in optimized dominating set | Computational time (seconds) |
| 10 | 100 | 0.0450 | 5 | 10.3686 |
| 10 | 120 | 0.0461 | 5 | 14.3458 |
| 10 | 140 | 0.0472 | 6 | 15.9872 |
| 10 | 160 | 0.0481 | 7 | 17.1232 |
| 10 | 180 | 0.0500 | 7 | 19.3258 |
| 10 | 200 | 0.0511 | 8 | 21.3211 |
| 20 | 100 | 0.0443 | 8 | 12.2132 |
| 20 | 120 | 0.0451 | 8 | 15.6453 |
| 20 | 140 | 0.0462 | 11 | 17.5623 |
| 20 | 160 | 0.0469 | 12 | 18.3122 |
| 20 | 180 | 0.0474 | 13 | 21.3116 |
| 20 | 200 | 0.0489 | 13 | 22.9789 |
| 30 | 100 | 0.0431 | 11 | 13.7893 |
| 30 | 120 | 0.0466 | 13 | 17.2965 |
| 30 | 140 | 0.0520 | 14 | 19.3879 |
| 30 | 160 | 0.0459 | 14 | 22.0107 |
| 30 | 180 | 0.0462 | 15 | 24.3213 |
| 30 | 200 | 0.0471 | 16 | 25.2312 |
| 40 | 100 | 0.0411 | 12 | 15.3541 |
| 40 | 120 | 0.0423 | 14 | 19.0113 |
| 40 | 140 | 0.0434 | 17 | 21.0121 |
| 40 | 160 | 0.0441 | 17 | 24.6354 |
| 40 | 180 | 0.0449 | 21 | 25.7987 |
| 40 | 200 | 0.0455 | 23 | 27.8673 |

for the variable number of anchor nodes ranging from 10 to 40 with unknown nodes ranging from 100 to 200. The table also represents the number of anchor nodes utilized in the optimized CDS backbone through which the given number of unknown nodes has been localized. The data confirms the fact that even though there are numbers of anchor nodes present in the scenario, the optimized CDS backbone utilizes a very few number of anchor nodes to locate the unknown nodes.

The average localization error is shown in the Table 5.2. The results are also compared with the two existing algorithm [155][156] as shown in Fig. 5.7. We have simulated all the three algorithms with different number of anchor nodes and different number of unknown nodes. The results show that the proposed algorithm is having better accuracy of the location estimation as compared to the other two algorithms. Figure 5.8 describes the result for network lifetime comparison. The Three Dimensional (3D) representation of the data considers x-axis as no. of anchor nodes, y-axis as residual energy percentage and z-axis as no. of unknown nodes. The red surface in the 3D representation shows the overall residual energy surface level of the proposed algorithm which is considerable higher than the other algorithms in comparison. This signifies to the fact that, as the anchor nodes are mostly responsible for the location estimation process and the backbone is generated with load distributed optimized allocation, the residual energy for the nodes increases the overall network lifetime. In our case, the network lifetime increased by 60%.



(a)

(b)

(c)

(d)

FIGURE 5.7: *Average Localization Error(%) vs No. of Unknown Nodes*

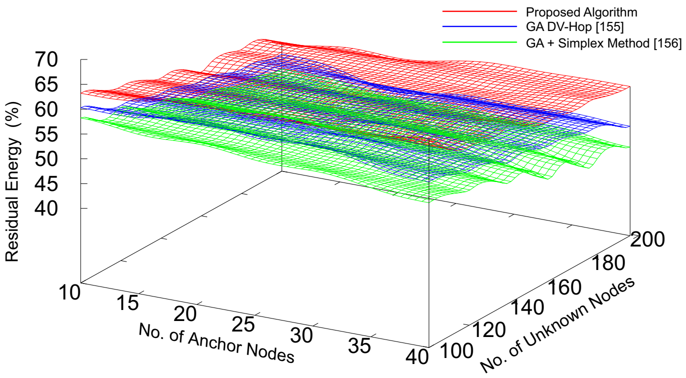


FIGURE 5.8: *Network Lifetime comparison based on residual energy*

## 5.4 Conclusion

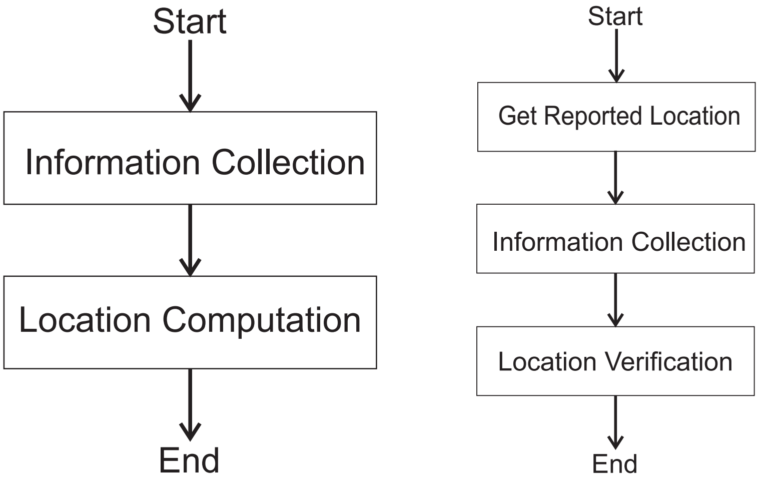
In this chapter, we have proposed a novel algorithm of optimizing a CDS which is based upon anchor nodes. Another major consideration is, the proposed algorithm applies random mobility for both the anchor nodes and the unknown nodes. The optimization process uses the genetic algorithm with elitism strategy so that the fittest solution can be retained accordingly for a fast convergence of the global solution. Obtaining the optimized CDS, the localization process executed that depends upon proximity matrices and transformation function.Finally, standard least square method is applied to get the estimated location of the unknown nodes. As the major calculations are taken care by the anchor nodes, the network lifetime increases in the proposed algorithm. Furthermore, we have compared our simulated results with other two recent algorithms and the analysis shows that the proposed algorithm is better in terms of accuracy of the localization error and network lifetime. In addition, the proposed algorithm is scalable and works with different network sizes.

# CHAPTER 6

# A secure localization approach using mutual authentication and insider node validation

## 6.1 Introduction

Localization [47] defines the calculation of the location or position of sensor nodes in Wireless Sensor Networks (WSNs). The dynamic need of the applications has made the deployment of WSNs extended from static to mobile. Such networks are dynamic and therefore the localization of nodes is also changeable and thus makes the process a critical factor in WSNs. The knowledge of the physical location of a network entity helps in different applications and services [196][197][198]. The main consideration of location discovery is a set of special nodes known as anchor nodes, which are resource privileged having more storage and computational capacity. Using the location of anchor nodes, other unknown nodes compute their location in different ways. Therefore, it is critical that malicious anchor nodes need to be prevented from



(a) Location Estimation

(b) Location Verification

FIGURE 6.1: *Localization System*

providing false location information as the unknown nodes completely depend on the anchor nodes for computing their own location.

WSNs attract the adversaries in a very general way. Attacks are executed by the internal nodes as well as external nodes. Therefore, it is compulsory that the localization techniques should be secured enough[199]. The secured localization process must prevent both malicious insider nodes from misrepresenting their location and outside entities from performing intrusion with the location determination process. The security requirements for localization techniques must include privacy of the location information, authorization for legitimate nodes and the integrity to identify any kind of deviation from true location. Further, information availability to compute proper location is also required for a secured localization process.

The accuracy of nodes' locations can be considered on the basis of two aspects. On one hand, nodes (anchor or unknown) need to calculate their correct position depending upon some references, which is called localization estimation (Figure 6.1(a)). On the other hand, the Base Station ($BS$) also needs to ensure that the location estimations it has received are correct. Thus, we need to verify the locations received from the nodes. This is called as location verification (Figure 6.1(b)).

## 6.2 Attack Model

Many attacks [199] have been studied on localization system. Attacks are executed in the information collection process in localization estimation phase as well as location verification phase. There are several types of elementary and combinational attacks that can be executed in localization systems. Table 6.1 summarizes the layer wise attacks in WSNs localization process[181].

TABLE 6.1: *Summarization of layer wise attacks on localization in WSNs [8].*

| **Layers** | **Attacks** | **Attack behaviour** | **Results** |
|---|---|---|---|
| Physical layer | Stealing | Signal eavesdropping and tampering | Packet error and packet loss |
| | Jamming | Sending jamming signal in the working frequency range | Packet loss |
| Data link layer | Collision | Repetition of messages | Packet loss |
| | Exhaustion | Sending of unnecessary message | Packet loss |
| | Unfairness | Explicitly take the control of the channel | Packet loss |
| Network layer | DoS Attacks | Exhaustion of energy of the unknown nodes | Packet loss |
| | Selective forwarding | Selectively forward packets | Packet loss |
| | Sybil | Possessing multiple identities | Packet error |
| | Sinkhole | Maliciously tamper with routing | Packet error |
| | Wormhole | Shortening the distance to make a fast routing path | Packet loss |
| Transport layer | Flooding | Establishing false connections | Packet loss |
| | Tampering | Tampering localization beacons | Packet error |

### 6.2.1 Elementary attacks

Elementary attacks are the prime attacks which have their own technical aspects of execution. Some of such attacks are discussed below.

**Range change attack** In this attack an attacker changes the range or Angle of Arrival (AoA) measurements among nodes. This attack affects on both localization estimation and location verification systems. For example, reducing or increasing the range measurement between node $A$ and $B$ will lead to malicious estimation of locations of $B$ shown by green dotted circles in the Figure 6.2.

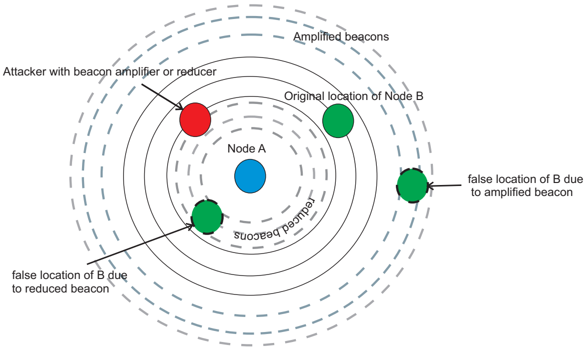
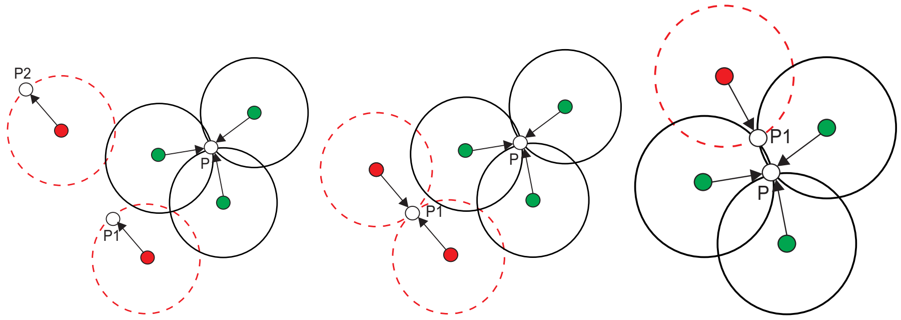

Amplified beacons
Attacker with beacon amplifier or reducer
Original location of Node B
Node A
false location of B due to amplified beacon
reduced beacons
false location of B due to reduced beacon

FIGURE 6.2: *Effects of range change*

**False beacon location attack** In this attack an attacker makes the victim node to receive false estimated locations. For example, an attacker gains control over a beacon or anchor node and then it make the node broadcasts false location.

**False reported location attack** This attack is generally executed in a location verification system where a malicious anchor node or unknown node reports false location.



(a) uncoordinated (b) collusion (c) pollution

FIGURE 6.3: *Location reference attack*

### 6.2.2 Combinational attacks

Combinational attacks are those who merge different technicalities of elementary attacks and create overall malicious affect. Some of the important combinational attacks are listed below.

**Impersonation** In this attack an attacker makes its identity to be as a legitimate node in the network. For example, in localization systems, an attacker spoofs the anchor nodes' identity and broadcasts false locations. This leads to erroneous range measurements. In location verification systems, an attacker impersonate a victim node to make verifiers believe that the original node is at the attacker's location.

**Sybil attack** In this attack a malicious node has the capability of presenting itself as different identities in a network to function as distinct nodes. These multiple identities are called Sybil nodes. It sends false information like position of beacon nodes and erroneous strength of signal. By masquerading and disguising as multiple identities, this type of malicious node gains control over the network.

**Location-reference attack** This attack is executed against the localization phase. Each common node gets a location-reference set $< loc_i, d_i >$ for localization where $loc_i$ is the location of beacon $i$ and $d_i$ is the distance between the beacon and the common node. In this attack the attacker makes the compromised beacons broadcast false locations and distorts the distance measurements between beacons and common nodes. The attack can be classified into three types: (a) uncoordinated attack, (b) collusion attack, and (c) pollution attack. Exemplary scenarios are shown in Figure 6.3(a), 6.3(b), and 6.3(c) respectively. Red nodes represent the attacker nodes, green nodes represent beacon nodes and the white nodes represent common nodes.

In uncoordinated attack, different false location references are provided to mislead the unknown node to different false locations, e.g., $P1$ and $P2$ in the Figure 6.3(a). In collusion attack, all false location references mislead the common node to the same randomly chosen false location, say $P1$ in Figure 6.3(b). In pollution attack, all false location references misguide the unknown node, to a specially chosen false location $P1$, as in Figure 6.3(c), which still conforms to some normal location references. This attack succeeds even when normal location references are in the majority. In all the categories as shown in Figure 6.3 , P is the original location.

## 6.3 Proposed Algorithm

Our proposed algorithm considers only the anchor nodes, unknown nodes and Base Station($BS$) where anchor nodes and unknown nodes are deployed randomly. The anchors are having a variable range of transmission with an average transmission range $R_{avg}$ given as:

$$R_{avg} = \frac{min \sum_{e \in E} \psi(|e|)}{m} \tag{6.1}$$

Where $m$ is the number of anchor nodes in the network,$e$ is an edge between two nodes, $E$ is the set of the edges in the network, $\psi(|e|)$ is the weighing function of a connection between an anchor node and an unknown node and interpreted as: $\psi(|e|) \ \sim |e|^{\alpha} \ where \ 2 \leq \alpha \leq 4$

The algorithm starts with an initialization phase that deals with distribution of certificates by the $BS$. After the distribution of the certificates, distance estimation phase starts among the anchor nodes and the unknown nodes. Once the distances are estimated, the BS is able to localize the unknown nodes applying Minimum Mean Square Error (MMSE) method. The algorithm is summarized in Algorithm 8.

**Algorithm 8** Distance estimation by Anchor nodes

```
Input:- Anchor node set $A$, unknown node set $U$
$BS$ creates identities $ID_{aj}$ for all anchor nodes and identities $ID_{ui}$ for all unknown nodes
$BS$ provides certificates: $Cert_{aj}$ , $Cert_{ui}$
$\forall$ $a_j \in A$ do
        $a_j$ sends $u_i$ random nonce $\chi$, $Cert_{aj}$; for $i = 1, 2, ..., m$
        $a_j$ waits for a threshold time $t_{retransmit}$ to retransmit the message
$\forall$ $u_i$ under $R_{avg}$ for any $a_j \in A$
        $u_i$ sends $a_j$ : $[\chi, time_{proc}]_{K_{a_j}+}$ , $Cert_{uj}$
Calculate $time_{prop}$
$d_{ui}^{aj} = c \times time_{prop}$
$a_j$ sends $d_{ui}^{aj}$ to the Base Station (BS)
end loop
Apply MMSE
```

As we have used the speed of light, $c$, to estimate the distance, the process shown above will prevent the generation of high speed link required to execute wormhole attack because there cannot be any high speed link in which the transmission speed will be more than that of the light. The utilization of mutual authentication with certificates provided by the BS will help to avoid or prevent any kind of authentication attack such as sybil attack, impersonation attack executed by the outsider nodes. The encryption method will help to securely transmit the estimated distance to the BS. The $t_{retransmit}$ value will help to detect the jamming attack so that further the avoidance and detection process can be applied following the methods as shown in the paper [201]. But it can be a fact that, the insider nodes are compromised and can generate distance reduction or enlargement attacks. To prevent these attacks, we have to follow the further process.

Let's assume that the deviation of the true position of the unknown node due to measurement error and/or malicious distance estimates is $\delta$ which is tolerable for the system. We know that the unknown node $(x_{u_i}, y_{u_i})$ must be in the intersection region

**Algorithm 9** Validation of distance estimation and detection of malicious anchors by BS

```
1: Input:- Set of anchor nodes $A$ with locations $(x_{a_j}, y_{a_j})$ location estimate of an unknown node $(x_{u_i}, y_{u_i})$, error parameter $\delta$
2: $\forall\ a_j \in A,\ j = 1, 2, ..., m$
3: if $\left(true_{d_{u_i}^{a_j}} - \delta\right)^2 \leq \left(x_{u_i} - x_{a_j}\right)^2 + \left(y_{u_i} - y_{a_j}\right)^2 \leq \left(true_{d_{u_i}^{a_j}} + \delta\right)^2$ then
4:     Exit
5: else
6:     Go to Step 8
7: end if
8: Calculate the algebraic centre $x^*$ of intersection region $R$
9: Initialize $r^* = 0$                         ▷ radius of the intersection region $R$ as
10: $\forall\ v$ inside the region $R$ do
11: if $||v_d - r^*|| > r^*$ then
12:     $r^* \longleftarrow ||v_d - r^*||$
13: end if
14: $\forall\ a_j \in A,\ j = 1, 2, ..., m$
15: $\overline{\overline{true^{a_j}_{d_{u_i}}}} = \frac{true^{a_j}_{d_{u_i}}}{1+\varepsilon_{max}}$
16: if $\overline{\overline{true^{a_j}_{d_{u_i}}}} > ||x^* - a_j|| + r^*$ then
17:     Anchor node $a_j$ is malicious
18: else
19:     $a_j$ is not malicious
20: end if
```

of the anchor nodes' bound circles in the range. Therefore, following the Algorithm 9 we can validate the distance estimation provided by the anchor nodes.

## 6.4 Network Model and Assumptions

The network model is considered to be self-organizing having no central control of deploying the sensor nodes in the network. For the ease of presentation, the wireless sensor network model $\mathcal{N}$ is considered to be in 2-D and represented by a graph $G(V, E)$ consists of $V$, a set of vertices and $E$ a set of edges. The size of the network can be given as:

$$|\mathcal{N}| = |A| + |U| \tag{6.2}$$

Where, $|A|$ is the size of anchor node set $A$, $|U|$ is the size of the unknown node set $U$ and $A, U \subseteq V$.

In the proposed algorithm, we have divided the network nodes in two categories. First, the anchor nodes, $a_j \in A$ , which are privileged in their storage capacity and computational capacity with additional energy resources. Second, the unknown nodes, $u_i \in U$, which are not privileged like the anchor nodes and are able to perform minimum computational tasks. Both types of nodes are randomly deployed in the network environment. The location estimation of an unknown node is calculated by using the location information of the anchor nodes in a WSN. Therefore, the integrity of location messages as well as the reliability of message origin is very important during the localization process. Confidentiality of estimated location is also required in some applications, to protect the privacy of the corresponding sensors. In this paper, an appropriate cryptographic scheme is presented to provide the security services. The assumptions for our proposed approach have been listed below.

- The unknown nodes and anchor nodes are mobile.
- Base station is assumed to be trusted and is considered to be key distributor and certificate authority.
- Anchor nodes and unknown nodes are deployed with their private keys
- Base Station shares the public key only to the legitimate unknown nodes and anchor nodes predefined.

**Initialization Phase:** Base station($BS$) provides the identity for all anchor nodes and unknown nodes as $ID_{a_j}$ and $ID_{u_i}$ where $a_j$ is an anchor node and $u_i$ is an unknown node. $BS$ also provides certificates for each anchor node and unknown node as $Cert_{a_j}$ and $Cert_{u_i}$.

$$BS \to Cert_{a_j} = [ID_{a_j}, K_{a_j+}, t, e_t]BS_{K-} \tag{6.3}$$

Where, $ID_{a_j}$ is the identity of an anchor node $a_j$, $K_{a_{j+}}$ is the public key of that anchor node, $t$ is the timestamp when the certificate was created and $e_t$ is the expiry time of the certificate. This total certificate is digitally signed by $BS_{K-}$ which is the private key of the base station. All anchor nodes must make them updated by having a fresh certificate as required. For an legitimate unknown node $u_i$ , we can rewrite the above format in the following way.

$$BS \rightarrow Cert_{u_i} = [ID_{u_i}, K_{u_{i+}}, t, e_t]BS_{K-} \tag{6.4}$$

Where, $ID_{u_i}$ is the identity of an unknown node $u_i$, $K_{u_{i+}}$ is the public key of that unknown node, and $e_t$ is the expiry time of the certificate.

**Distance Estimation phase:** The anchor node $a_j$ sends a random nonce $x$ , along with the certificate $Cert_{a_j}$ to all the one-hop neighbourhood unknown nodes $u_i$ in the range $R_{avg}$ and starts the timer on. The unknown nodes receive the message and verify the certificate using the public key $BS_{K+}$ given by $BS$. As only legitimate anchor nodes are having the certificate to provide, by verifying the certificates, the authentication of the anchor nodes can be proved. Then, the unknown nodes $u_i$ response back to the anchor node $a_j$ with the same nonce $x$ , time duration between receiving the last bit of message sent by anchor node and transmitting the first bit of message to the anchor node, given as $time_{proc_u}$ encrypted with anchor node's public key $K_{a_{j+}}$ along with its own certificate.

$$a_j \rightarrow u_i : x, Cert_{u_i} \tag{6.5}$$

$$u_i \rightarrow a_j : [x,\ time_{proc\_u}]_{K_{a_{j+}}},\ Cert_{u_i} \tag{6.6}$$

When $a_j$ sends message to $u_i$ , it waits for a bounded time value $t_{retransmit}$ to retransmit the message if no response starts arriving to the anchor in that bounded time. This value is precomputed at the starting of the network deployment assuming all the favourable conditions of the network environment with a noise effect of $\triangle t$ and given as:

$$t_{retransmit} = t_{normal} + \ \triangle t \tag{6.7}$$

where, $t_{normal}$ is the normal time duration of getting a response back from the unknown node.

When the anchor node receives the response back from the unknown nodes, it decrypts the message using its own private key $K_{a_{j-}}$, verifies the certificate of the unknown nodes, stops the timer and calculates the signal propagation time as:

$$time_{prop} = \frac{(time_j - time_{proc_u} - time_{proc_a})}{2} \tag{6.8}$$

Where $time_{prop}$ is the signal propagation time, $time_j$ is the timer interval at the anchor side and $time_{proc_a}$ is the time duration between receiving the first bit of the response and last bit of the response. The interaction between unknown node and anchor node is shown in Figure 6.4. Once the propagation time is calculated, the estimated distance between anchor node $a_j$ and unknown node $u_i$ is calculated as:

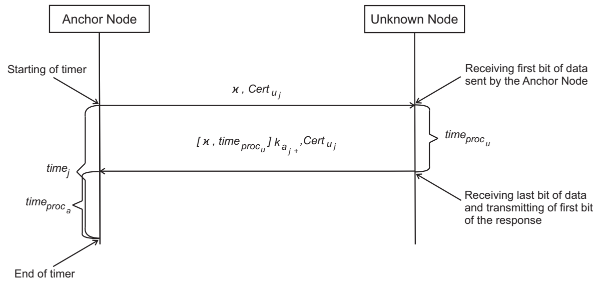

Anchor Node
Unknown Node
Starting of timer
Receiving first bit of data sent by the Anchor Node
ϰ , Cert $u_j$
[ ϰ , time $_{proc_u}$ ] k $_{a_{j+}}$ ,Cert $u_j$
time$_{proc_u}$
time$_j$
time$_{proc_a}$
Receiving last bit of data and transmitting of first bit of the response
End of timer

FIGURE 6.4: *Propagation time estimation process*

$$d_{u_i}^{a_j} = c \times time_{prop}, \quad where\ c\ is\ the\ speed\ of\ light \tag{6.9}$$

Once the anchor node calculates this estimated distance, it is then forwarded to the $BS$ encrypted with the public key of $BS$ and along with the anchor node's certificate.

$$a_j \rightarrow BS : [d_{u_i}^{a_j}]_{BS_{K+}}, \quad Cert_{a_j} \tag{6.10}$$

After receiving the messages from the anchor nodes, $BS$ decrypts the message with its own private key and gets the estimated distances. Finally, it uses MMSE [170] to estimate the location of an unknown node $(x_{u_i}, y_{u_i})$. One thing need to remember is that, we need atleast three non-collinear anchor nodes to apply MMSE. Another important attribute of our proposed algorithm deals with the mobility of the nodes. We consider that the nodes (whether the anchor or the unknown) are mobile. The relative mobility between an unknown node $u_i$ with respect to anchor node $a_j$ at a given time $t$ is given by

$$RM_t^{a,u} = d_{a,u_t} - d_{a,u_{t-1}} \tag{6.11}$$

$RM_t^{a,u}$ is positive if node $u_i$ is moving away from $a_j$ and negative if $u_i$ is coming closer to $a_j$.

Though the mobility is incorporated in the algorithm, nodes ( both the anchor nodes and the unknown nodes) are assumed to be pseudo static i.e. they are static for a very short time interval for the localization process and this does not incorporate any significant error in the estimation.

**Handling distance estimation error** Distance estimations in a wireless environment are very common to have error due to noise or delay in the medium. The estimation error is $\epsilon \in [-\epsilon_{max}, \epsilon_{max}]$ where $\epsilon_{max}$ is a system parameter and given as: $0 \leq \epsilon_{max} \leq 1$. Therefore, the estimated distance can be given as:

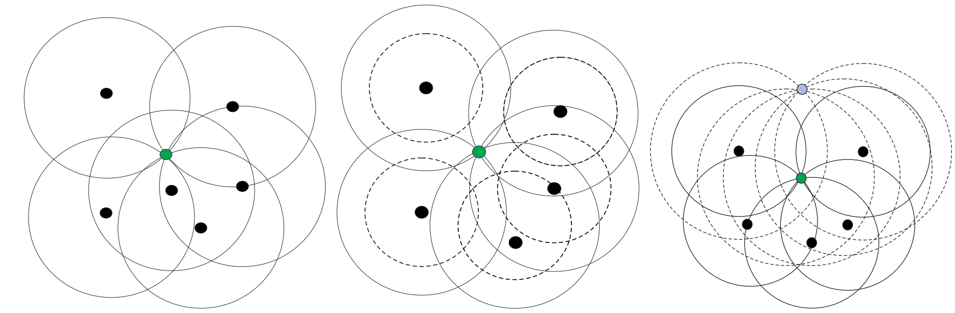
$$d_{u_i}^{a_j} \in [true_{d_{u_i}}^{a_j} \times (1 - \epsilon_{max}), true_{d_{u_i}}^{a_j} \times (1 + \epsilon_{max})] \tag{6.12}$$

where $true_{d_{u_i}}^{a_j}$ is the true distance between $a_j$ and $u_i$ and can be calculated by applying Euclidean method.

Further, the presence of compromised insider anchor nodes can create an error factor $\theta$. Following this, the estimated distance between $a_j$ and $u_i$ in presence of malicious anchor node can be given as:

$$d_{u_i}^{a_j} = true_{d_{u_i}}^{a_j} \times (1 + \epsilon_{max}) \times (1 + \theta) \;\; where\ \theta > 0 \tag{6.13}$$

As we know that $\epsilon \in [-\epsilon_{max}, \epsilon_{max}]$ , the value of $\epsilon$ can create both the positive estimation error and negative estimation error. Positive estimation error will create



(a) Truthful estimation (b) Distance reduction (c) Distance enlargement

Figure 6.5: *Distance manipulation attack*

multiple intersection points of the convex region of the anchor nodes' ranges leading to the distance enlargement attacks. On the other hand, negative estimation error creates an empty intersection region assuming that the location of the unknown node is in the intersection of bounds of anchors leading to the distance reduction attack. This concept is shown in the Figure 6.5. The black solid circles are anchor nodes and green circle is the original estimated location. If the anchor nodes are compromised and provide reduced distance estimations, the intersection will be empty and if the malicious anchor nodes provide enlarged distance estimations, the position of the unknown node deviates from the original position shown as light blue circle.

Distance reduction is not a severe in localization. If we find the empty intersection region $\mathcal{R}$, the distance estimates can be increased with a factor of $\frac{1}{1-\epsilon_{max}}$ to get a non empty intersection region $\mathcal{R}'$, where the unknown node must exist.

To prevent distance enlargement situation, the $BS$ need to follow the process summarized in Algorithm 9. The tolerable error parameter $\delta$ can be derived from the following equation as:

$$\delta = w_1\epsilon + w_2\theta \tag{6.14}$$

where $\epsilon$ is the system measurement error due to noise and $\theta$ is the error included by malicious anchor nodes. We assume that the unknown nodes are error free and do not provide any false distance estimation. $w_1$,$w_2$ are used as weighing values for the errors depending upon the network conditions. This $\delta$ will provide an upper bound and lower bound of the estimated distance in presence of error given as:

$$(true^{a_j}_{d_{u_i}} - \delta)^2 \leq (x_{u_i} - x_{a_j})^2 + (y_{u_i} - y_{a_j})^2 \leq (true^{a_j}_{d_{u_i}} + \delta)^2 \tag{6.15}$$

and

$$true^{a_j}_{d_{u_i}} = \sqrt{(x_{u_i} - x_{a_j})^2 + (y_{u_i} - y_{a_j})^2} \tag{6.16}$$

The algebraic centre $x^*$ in Algorithm 9, can be calculated using barrier method on the unconstrained optimization problem given as:

$$min(x, \delta) - \lambda.\delta - \sum_{j=1}^{m} log[(\overline{true^{a_j}_{d_{u_i}}}.(1-\delta))^2 - ||x - a_j||^2] - log(\delta) \tag{6.17}$$

where $\lambda$ is the Lagrangian multiplier and $\overline{true^{a_j}_{d_{u_i}}}$ is given by: $\overline{true^{a_j}_{d_{u_i}}} = \frac{true^{a_j}_{d_{u_i}}}{1-\epsilon_{max}}$ i.e. the increased distance estimation in case of negative

The radius of the intersection region $\mathcal{R}$ is initialized to zero with an assumption that the unknown node is positioned at the intersection point itself and no convex region has been generated by the intersection. Moreover, the radius of the intersection region can be updated by verifying the distance between any point inside the region and the algebraic centre $x^*$. Finally, we can detect the malicious insider anchor nodes depending upon the increased estimated distance.

So, the attacks those are identified in localization process as shown in Table 6.1, is addressed well in the proposed model. The summarization of countermeasures by the proposed model has been shown in Table 6.2.

Table 6.2: *The summarization of countermeasures by the proposed algorithm*

| Attacks | Attack behaviour | Prevention by our proposed model |
|---|---|---|
| Stealing | Signal eavesdropping and tampering | Our proposed model uses encryption to prevent such attacks |
| Jamming | Sending jamming signal in the working frequency range | Detection is addressed in the proposed algorithm by using bounded time |

| | | |
|---|---|---|
| Collision | Repetition of messages | Not applicable in the proposed model, as the maximum calculation is done by BS and anchor node with minimum message controls. |
| Exhaustion | Sending of unnecessary message | No scope to provide unnecessary message as transmission range is limited and the distance estimation process is secured. |
| Unfairness | Explicitly take the control of the channel | Not possible due to the minimum size of the packets. |
| DoS Attacks | Exhaustion of energy of the unknown nodes | Can be monitored directly by the base station. |
| Selective forwarding | Selectively forward packets | Using the approach of one hop neighborhood forwarding is not necessary. |
| Sybil | Possessing multiple identities | Mutual authentication is used. |
| Sinkhole | Maliciously tamper with routing | Mutual authentication is used with the certificates. |
| Wormhole | Shortening the distance to make a fast routing path | The distance estimation is done based upon the speed of light which is the maximum speed of transmission and therefore no faster link can be created between an anchor and an unknown node. |
| Flooding | Establishing false connections | Broadcasting is limited by the anchor nodes within a limited range of $R_{avg}$ |
| Tampering | Tampering localization beacons | Both encryption and mutual authentication is used. |

| | | |
|---|---|---|
| Insider attack | Compromised anchor nodes may provide false information | Both the distance reduction and distance enlargement attack have been addressed. |
| Range change attack | Changes the range or angle of arrival (AoA) | Our proposed model does not incorporate the mechanism of AoA as it works on time interval to calculate the distance and therefore can easily avoid such attacks. |
| False beacon location attack | Compromises a beacon and then he can make the beacon broadcast false location | Authentication, limited range and validation of distance estimation in the proposed approach will help to avoid such attacks. |
| False reported location attack | malicious node reports false | Verification is done at the BS, so there is less chance to report falsified verification. |

## 6.5 Results and Discussion

In this section, we have evaluated the proposed algorithm based on the parameters as shown in Table 6.3.

Table 6.3: *Simulation parameters and rules*

| Parameters | Values |
|---|---|
| Simulation Area | $500m \times 500m$ |
| No. of Unknown Nodes | 500 |
| Communication range | 120 m |
| Node placement | Random |
| Mobility | Random Way Point model |

We have compared the simulated results with the three recent algorithms: 1) Collaborative Secure Localization algorithm based on Trust model (CSLT) proposed by Han et. al. [181], 2) Multilateral Privacy Algorithm for secured Localization proposed by Shu et. al. [186] and 3) Authenticated weight-based secured DV-hop proposed by Liu et. al.[194]. The performances of the algorithms are measured on the following three parameters: simulation time, localization efficiency and localization accuracy. The attacks described in Table 6.2 are also simulated to show the efficiency of the proposed algorithm.

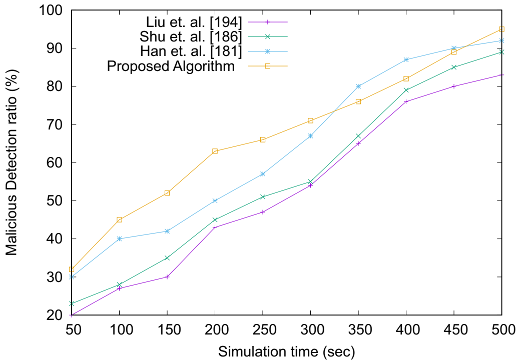
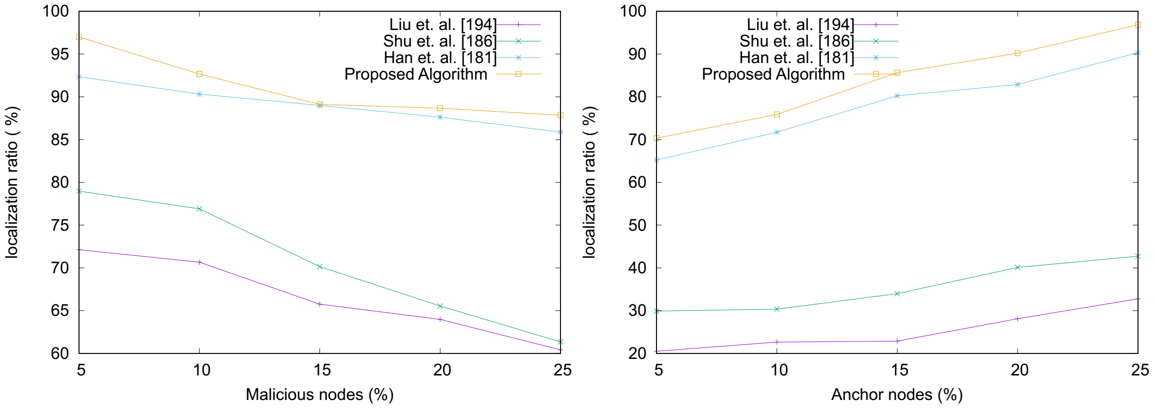


FIGURE 6.6: *Comparison of malicious detection ratio*

Simulation time is defined as the time taken for the algorithms to detect a particular malicious attack. The result in Figure 6.6 shows that the proposed algorithm is efficient in detecting 90% of the malicious attack with less time as compared to the other algorithms in comparison.

The localization ratio is defined as the percentage of successful location estimation of unknown nodes. The result in Figure 6.7(a) shows that, with the increasing malicious nodes' percentage, every algorithm in our comparison faces a significant decrease in successful localization of unknown nodes. However, the proposed algorithm still performs better as compared to others. Figure 6.7(b) shows that the proposed algorithm out performs the other algorithms in the successful localization of unknown nodes with the increasing percentage of anchor nodes.

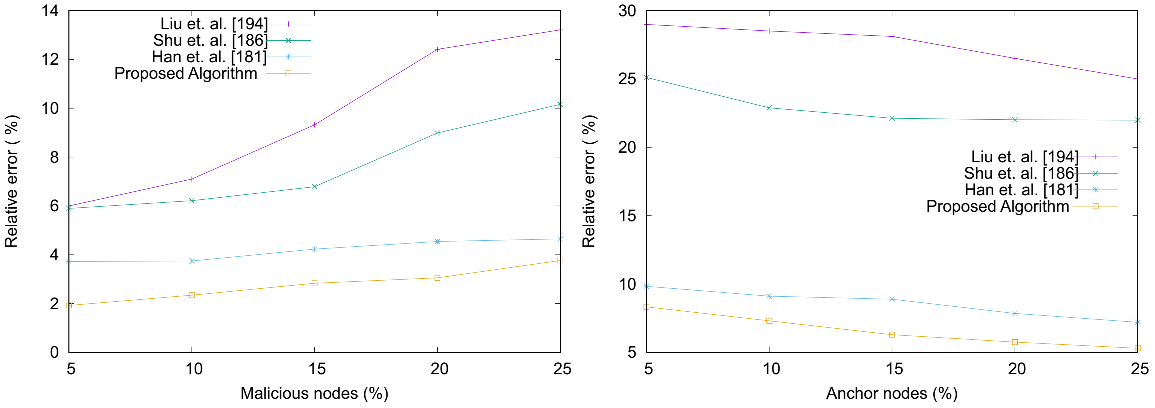


(a)

(b)

FIGURE 6.7: *Comparison of localization ratio: (a) Impact of malicious nodes (b) Impact of anchor nodes*

Localization accuracy is a valuable metric for evaluating the efficiency of localization algorithms. In the proposed work, the localization accuracy is defined by the relative error between the actual location and the calculated node position.



(a)

(b)

FIGURE 6.8: *Comparison of localization accuracy: (a) Impact of malicious nodes (b) Impact of anchor nodes*

In our simulation, we have varied the ratio of malicious nodes from 5% to 30% with increments of 5%. Simulation result, shown in Figure 6.8(a), shows that the relative error percentage of location estimation increases with the increasing number of malicious nodes. However, the proposed algorithm proves its efficiency in location estimation accuracy. Similarly, location accuracy is also tested by varying the anchor nodes' percentage. Result shown in Figure 6.8(b), signifies to the fact that the proposed algorithm significantly reduces the relative error percentage with the increasing number of anchor nodes. It is also seen in the result that, the other algorithms also decrease the relative error with the increasing number anchor nodes, but the percentage of relative error is less in our proposed algorithm.

## 6.6 Conclusion

Security in localization has always been a vital part of localization algorithms. Though, there are a number of algorithms are introduced with security aspects, but the algorithm designers have somehow overlooked the complexity issue of the algorithms in the resource constrained WSNs. In this chapter, we have addressed this problem and provided a solution with our proposed algorithm. The proposed algorithm not only prevents a number of outsider attacks , it also provides a check on the insider nodes. Moreover, the algorithm provides low overhead and major functionality is on Base Station. The simulation results also prove the efficiency of the proposed algorithm in terms of localization accuracy, simulation time and localization ratio. The most important feature of our algorithm is that it supports mobility of the nodes and therefore it is suitable for dynamic network environments.

# BIBLIOGRAPHY

[1] John Ross, ”Introduction to Wireless Networks,” in The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless, 2nd Edition, No Starch Press, 2008, pp. 11-28.

[2] I. Marsic, Wireless Networks Local and Ad Hoc Networks. Rutgers University, 2013.

[3] R. Di Pietro, S. Guarino, N. V Verde, and J. Domingo-ferrer, ”Security in Wireless Ad-Hoc Networks A Survey,” Journal of Computer Communications, vol. 51, pp. 1-20, 2014.

[4] Peter Kampstra. Evolutionary Computing in Telecommunications A likely EC success story. Masters thesis, Vrije University, Amsterdam, August 2005. BMI Paper, Supervisors: Rob D. van der Mei and Gusz Eiben Online available at http://www.few.vu.nl/stagebureau/werkstuk/werkstukken/werkstuk-kampstra.pdf

[5] W. Baluja, T. O. Ledesma, and L. Coya, New Solution For The Creation Of MANETs Based On Personal Devices, IEEE Latin America Trans., vol. 14, no. 3, pp. 1480-1487, 2016.

[6] P. Rawat, K. Deep, H. Chaouchi, and J. Marie, "Wireless sensor networks: a survey on recent developments and potential synergies," Journal of Supercomputing, vol. 68, no. 1, pp. 1-48, 2014.

[7] T. Z. C.S. Raghavendra, Krishna M. Sivalingam, Wireless Sensor Networks, 2004, Springer.

[8] U. M. Peovi, J. J. Mohorko, K. Benki, and F. . arko, "Single-hop vs. Multi-hop Energy efficiency analysis in wireless sensor networks," in 18th Telecommunications Forum,TELFOR, 2010.

[9] T. Arampatzis, J. Lygeros, S. Member, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," in proceedings of IEEE International Symposium on Intelligent Control, Mediterrean Conference on Control and Automation, pp. 719-724, 2005.

[10] P. Gupta, and P. R. Kumar, "The Capacity of Wireless Networks," IEEE Trans. on Info. Theory, vol. 46, no. 2, pp. 388-404, 2000.

[11] Ko R-S, "A load-balancing routing algorithm for wireless sensor networks based on domain decomposition.," Ad Hoc Networks 30:63-83. doi: 10.1016/j.adhoc.2015.03.003, 2015

[12] Dietrich I, Dressler F, "On the Lifetime of Wireless Sensor Networks,", ACM Trans Sens Networks. 5:139, 2009.

[13] M. Grossglauser, P. Avenue, F. P. Nj, and D. Tse, "Mobility Increases the Capacity of Ad-hoc Wireless Networks." IEEE/ACM trans. on Networking, vol. 10, no. 4, pp. 477-486, 2002.

[14] J. Li, D. S. J. De Couto, D. R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," in proceedings of the 6th annual international conference on mobile computing and networking, 2002, pp. 120-130.

[15] K. N. Amouris and L. A. C-d, " A position-based multi-zone routing protocol for wide area mobile ad-hoc networks," IEEE 49th Vehicular Technology Conference, 1999, pp. 1365-1369.

[16] M. Mauve and H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," IEEE network, vol. 15, no. 6, pp. 30-39, 2001.

[17] M. Srivastava,R. Muntz, M. Potkonjak, "Smart Kindergarten: Sensor-based Wireless Networks for Smart Developmental Problem-solving Environments," in proceedings of 7th annual international conference on mobile computing and network, pp. 132-138, 2001.

[18] B. Das and V. Bharghavan, "Routing in ad-hoc networks using minimum connected dominating sets," Communications, 1997. ICC '97 Montreal, Towards the Knowledge Millennium. 1997 IEEE International Conference on, Montreal, Que., 1997, pp. 376-380.

[19] S. Butenko,D-Z Du, P. M. pardalos and X. Cheng, "On the construction of virtual backbone for ad hoc wireless network," in Cooperative control: Models, Applications and Algorithms, vol. 1. pp. 43-54, 2003.

[20] K. M. Alzoubi and O. Frieder, "Distributed construction of connected dominating set in wireless ad hoc networks," in Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 2002, vol. 3, pp. 1597-1604.

[21] J. Wu and H. Li, "On calculating Connected Dominating Set for efficient Routing in ad hoc Wireless Networks" in proceedings of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pp. 7-14, 1999.

[22] D. S. Johnson, "Computers and Intractability; A Guide to the Theory of NP - Completeness," W.H. Freeman and Company( New York), 1990.

[23] I. Stojmenovic, M. Seddigh, and J. Zunic, "Dominating Sets and Neighbor Elimination-Based Broadcasting Algorithms in Wireless Networks," IEEE Trans. on Parallel and Dist. Systems, vol. 13, no. 1, pp. 14-25, 2002.

[24] R. Xie, D. qi, Y. Li, J. Z. Wan "A novel distributed MCDS approximation algorithm for wireless sensor networks," Wireless Communications and Mobile Computing , Vol. 9, no. 3, pp. 427437, 2009.

[25] M. Rai, S. Verma, and S. Tapaswi, "A power aware minimum connected dominating set for wireless sensor networks," J. Networks, vol. 4, no. 6, pp. 511-519, 2009.

[26] G. Han, H. Xu, T. Q. Duong, J. Jiang, and T. Hara, "Localization algorithms of Wireless Sensor Networks: A survey," Telecommun. Syst., vol. 52, no. 4, pp. 2419-2436, 2013.

[27] Jeril Kuriakose , Sandeep Joshi, R. Vikram Raju, Aravind Kilaru, "A Review on Localization in Wireless Sensor Networks", Advances in Signal Processing and Intelligent Recognition Systems, Volume 264 of the series Advances in Intelligent Systems and Computing, pp 599-610

[28] F. Cadger, K. Curran, J. Santos, and S. Moffett, "A survey of geographical routing in wireless Ad-Hoc networks," IEEE Commun. Surv. Tutorials, vol. 15, no. 2, pp. 621-653, 2013.

[29] Y. B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," Wirel. Networks, vol. 6, no. 4, pp. 307-321, 2000.

[30] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for wireless networks," ACM MobiCom, no. MobiCom, pp. 243-254, 2000.

[31] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (DREAM)," Proc. 4th Annu. ACM/IEEE Int. Conf. Mob. Comput. Netw., pp. 76-84, 1998.

[32] S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker, "GHT: A Geographic Hash Table for Data-Centric Storage," Proc. 1st ACM Int. Work. Wirel. Sens. networks Appl. - WSNA 02, p. 78, 2002.

[33] Sasha Slijepcevic Seapahn Megerian Miodrag Potkonjak , "Characterization of Location Error in Wireless Sensor Networks: Analysis and Applications, Information Processing in Sensor Networks," Volume 2634 of the series Lecture Notes in Computer Science pp 593-608, 2003

[34] A. Savvides, W. L. Garber, R. L. Moses, and M. B. Srivastava. "Analysis of Error Inducing Parameters in Multihop Sensor Node Localization," IEEE Transactions on Mobile Computing, vol. 4, no. 6, November/December 2005

[35] Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, "Secure localization and location verification in wireless sensor networks: A survey," J. Supercomput., vol. 64, no. 3, pp. 685-701, 2013.

[36] G. Mao and B. Fidan, "Localization Algorithms and Strategies for Wireless Sensor Networks," Information Science Reference, 2009.

[37] Long Cheng, Chengdong Wu, Yunzhou Zhang, Hao Wu, Mengxin Li, Carsten Maple, "A Survey of Localization in Wireless Sensor Network." International Journal of Distributed Sensor Networks, Vol. 8, no. 12, 2012.

[38] E. Niewiadomska-Szynkiewicz, "Localization in wireless sensor networks: Classification and evaluation of techniques," Int. J. Appl. Math. Comput. Sci., vol. 22, no. 2, pp. 281-297, 2012.

[39] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," Comput. Networks, vol. 51, no. 10, pp. 2529-2553, 2007.

[40] G. M. Gandhi and P. Rama, "GPS based Multi-hop Communication with Localization in Subterranean Wireless Sensor Networks," in Procedia Computer Science, 2015, vol. 57, pp. 1189-1198.

[41] B. Cheng, R. Du, B. Yang, W. Yu, C. Chen and X. Guan, "An Accurate GPS-Based Localization in Wireless Sensor Networks: A GM-WLS Method," 40th International Conference on Parallel Processing Workshops, Taipei City, 2011, pp. 33-41.doi: 10.1109/ICPPW.2011.32, 2011

[42] B. Dil, S. Dulman, and P. Havinga, "Range-based localization in mobile sensor networks," Wirel. Sens. Networks, vol. 3868, p. 164, 2006.

[43] P. B. and V. N. Padmanabhan,"RADAR: An in-building RF based user location and tracking system," Proc. IEEE INFOCOM 2000. Conf. Comput. Commun. Ninet. Annu. Jt. Conf. IEEE Comput. Commun. Soc. (Cat. No.00CH37064), vol. 2, pp. 775-784, 2000.

[44] J. Hightower, G. Borriello, and R. Want, "SpotON: An indoor 3D location sensing technology based on RF signal strength," UW CSE 00-02-02, p. 16, 2000.

[45] B. J. Dil and P. J. M. Havinga, "A feasibility study of RIP using 2.4 GHz 802.15.4 radios," in 2010 IEEE 7th International Conference on Mobile Adhoc and Sensor Systems, MASS 2010, 2010, pp. 690-696.

[46] A. Nasipuri, K. Li, B. H. P. Analysis, and D. Aids, "A Directionality based Location Discovery Scheme for Wireless Sensor Networks," Proc. 1st ACM Int. Work. Wirel. Sens. networks Appl., pp. 105-111, 2002.

[47] D. Niculescu and B. Nath, "Ad-hoc positioning system (APS) using AOA," Int. Conf. Comput. Commun., pp. 1734-1743, 2003.

[48] A. Savvides, C.-C. Han, and M. Strivastava, "Dynamic fine-grained localization in Ad-Hoc networks of sensors," Proceeding MobiCom 01 Proc. 7th Annu. Int. Conf. Mob. Comput. Netw., pp. 166-179, 2001.

[49] A. Savvides, H. Park, and M. Srivastava, "The bits and flops of the n-hop multilateration primitive for node localization problems," In Proceedings of ACM-WSNA '02, September 2002.

[50] T. He, C. Huang, B. M. Blum, J. a Stankovic, and T. Abdelzaher, ”Range-free localization schemes for large scale sensor networks,” Proc. 9th Annu. Int. Conf. Mob. Comput. Netw. (MobiCom ’03), p. 81, 2003.

[51] Y. Liu, X. Yi, and Y. He, ”A novel centroid localization for wireless sensor networks,” Int. J. Distrib. Sens. Networks, vol. 2012, 2012.

[52] Y. Zhou, X. Ao, and S. Xia, ”An improved APIT node self-localization algorithm in WSN,” in Proceedings of the World Congress on Intelligent Control and Automation (WCICA), 2008, pp. 7576-7581.

[53] D. Niculescu and B. Nath, ”DV Based Positioning in Ad Hoc Networks,” Telecommun. Syst., vol. 22, no. 1-4, pp. 267-280, 2003.

[54] S. Nath, V. N. Ekambaram, A. Kumar, and P. V. Kumar, ”Theory and algorithms for hop-count-based localization with random geometric graph models of dense sensor networks,” ACM Trans. Sens. Networks, vol. 8, no. 4, pp. 1-38, 2012.

[55] Xueyong Xu, Liusheng Huang, Jun He, He Huang, Guohua Jiang, ”A Fine-grained Hop-count Based Localization Algorithm for Wireless Sensor Networks,” Journal of Computers, Vol. 8, No. 3, 2013

[56] N. A. Alrajeh, M. Bashir, and B. Shams, ”Localization techniques in wireless sensor networks,” Int. J. Distrib. Sens. Networks, vol. 2013, 2013.

[57] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero III, R. L. Moses, and N. S. Correal, ”Locating the nodes: cooperative localization in wireless sensor networks,” Signal Process. Mag. IEEE, vol. 22, no. 4, pp. 54-69, 2005.

[58] J. P. Sheu, P. C. Chen, and C. S. Hsu, ”A distributed localization scheme for wireless sensor networks with improved grid-scan and vector-based refinement,” IEEE Trans. Mob. Comput., vol. 7, no. 9, pp. 1110-1123, 2008.

[59] Rastko R. Selmic, Vir V. Phoha, Abdul Serwadda, ”Wireless Sensor Networks: Security, Coverage, and Localization,” Springer, 2016.

[60] M.-S. Huang and R. M. Narayanan, ”Trilateration-Based Localization Algorithm Using the Lemoine Point Formulation,” IETE J. Res., vol. 60, no. 1, pp. 60-73, 2014.

[61] N. F. Danial and T. Krauthammer, ”Trilateration adjustment by finite elements,” J. Surv. Mapp. Div. Am. Soc. Civ. Eng., vol. 106, no. SU1, pp. 73-93, 1980.

[62] W. Navidi, W. S. Murphy, and W. Hereman, ”Statistical methods in surveying by trilateration,” Comput. Stat. Data Anal., vol. 27, no. 2, pp. 209-227, 1998.

[63] K. W. Cheung, H. C. So, W. K. Ma, and Y. T. Chan, ”Least Squares Algorithms for Time-of-Arrival-Based Mobile Location,” IEEE Trans. Signal Process., vol. 52, no. 4, pp. 1121-1128, 2004.

[64] K. Madsen, H.B. Nielsen, O. Tingleff, Methods for non-linear least squares problems, Informatics and Mathematical Modelling, Technical University of Denmark 2nd Edition, 2004

[65] M. Karagiannis, L. Chatzigiannakis and J. Rolim, ”Multilateration: Methods for Clustering Intersection Points for Wireless Sensor Networks Localization with Distance Estimation Error,” Arxiv preprint arXiv:1203.3704, 2012

[66] Cota-Ruiz, J., Rosiles, J.-G., Sifuentes, E., Rivas-Perea, P. , ”A Low-Complexity Geometric Bilateration Method for Localization in Wireless Sensor Networks and Its Comparison with Least-Squares Methods,” Sensors (Basel, Switzerland), 12(1), 839-862. http://doi.org/10.3390/s120100839, 2012.

[67] S. Misra and G. Xue, ”CluRoL: Clustering based Robust Localization in Wireless Sensor Networks,” MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, pp. 1-7. doi: 10.1109/MILCOM.2007.4454815, 2007

[68] O. Tekdas and V. Isler, ”Sensor Placement for Triangulation-Based Localization,” in IEEE Transactions on Automation Science and Engineering, vol. 7, no. 3, pp. 681-685, July 2010, doi: 10.1109/TASE.2009.2037135

[69] V. Pierlot and M. Van Droogenbroeck, ”A New Three Object Triangulation Algorithm for Mobile Robot Positioning,” in IEEE Transactions on Robotics, vol. 30, no. 3, pp. 566-577, June 2014, doi: 10.1109/TRO.2013.2294061

[70] F. Zeng, M. Yu, C. Zou and J. Gong, ”An Improved Point-in-Triangulation Localization Algorithm Based on Cosine Theorem,” 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 2012, pp. 1-4, doi: 10.1109/WiCOM.2012.6478419

[71] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, ”Wireless sensor networks: a survey on recent developments and potential synergies,” J. Supercomput., vol. 68, no. 1, pp. 1-48, 2014.

[72] Harrop P, Das R (2012) Wireless sensor networks 2012-2022. IDTechEx

[73] Harrop P (2012) Wireless sensor networks and the new Internet of things. Energy Harvest J. Available at http://www.energyharvestingjournal.com

[74] J. Yick, B. Mukherjee, and D. Ghosal, ”Wireless sensor network survey,” Comput. Networks, vol. 52, no. 12, pp. 2292-2330, 2008.

[75] K. W. Michael Winkler, Michael Street, Klaus-Dieter Tuchs, ”Wireless Sensor Networks for Military Purposes,” Auton. Sens. Networks, vol. 13, pp. 365-394, 2012.

[76] M. P. Durisic, Z. Tafa, G. Dimic, and V. Milutinovic, ”A survey of military applications of wireless sensor networks,” Mediterr. Conf. Embed. Comput. 2012, pp. 196-199, 2012.

[77] J. Agre and L. Clare, ”An integrated architecture for cooperative sensing networks,” Computer (Long. Beach. Calif)., vol. 33, no. 5, pp. 106-108, 2000.

[78] M. Bhardwaj, T. Garnett, and A. P. Chandrakasan, ”Upper bounds on the lifetime of sensor networks,” ICC 2001. IEEE Int. Conf. Commun. Conf. Rec. (Cat. No.01CH37240), vol. 3, pp. 1-37, 2001.

[79] P. Bonnet, J. Gehrke, and P. Seshadri, ”Querying the physical world,” IEEE Pers. Commun., vol. 7, no. 5, pp. 10-15, 2000.

[80] N. Bulusu, D. Estrin, and L. Girod, ”Scalable coordination for wireless sensor networks: self-configuring localization systems,” Proc. 6th Int. Symp. Commun. Theory Appl. A 01), Ambleside, UK, no. July, pp. 1-6, 2001.

[81] B. Warneke, M. Last, B. Liebowitz, and K. S. J. Pister, ”Smart dust: communicating with a cubic-millimeter computer,” Computer (Long. Beach. Calif.), vol. 34, no. 1, pp. 44-51, 2001.

[82] http://www.fao.org/sd/EIdirect/EIre0074.htm.

[83] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, ”Habitat monitoring: Application driver for wireless communications technology,” ACM SIGCOMM Comput. Commun. Rev., vol. 31, no. 2 supplement, pp. 20-41, 2001.

[84] N. Noury, T. Herv, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, and T. Porcheron, ”Monitoring behavior in home using a smart fall sensor and position sensors,” in 1st Annual International IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology - Proceedings, 2000, pp. 607-610.

[85] M. Ogawa, T. Tamura, M. Yoda, and T. Togawa, ”Fully automated biosignal acquisition system for home health monitoring, ” Eng. Med. Biol. Soc. 1997. Proc. 19th Annu. Int. Conf. IEEE, vol. 6, no. C, pp. 2403-2405 vol.6, 1997.

[86] T. Botsis, G. Demiris, S. Pedersen, and G. Hartvigsen, ”Home telecare technologies for the elderly.,” J. Telemed. Telecare, vol. 14, no. 7, pp. 333-7, 2008.

[87] B. G. Celler, T. Hesketh, W. Earnshaw, and E. Ilsar, ”An instrumentation system for the remote monitoring of changes in functional health status of the elderly at home,” in Engineering in Medicine and Biology Society, 1994. Engineering Advances: New Opportunities for Biomedical Engineers. Proceedings of the 16th Annual International Conference of the IEEE, 1994, pp. 908-909 vol.2.

[88] E. M. Petriu, N. D. Georganas, D. C. Petriu, D. Makrakis, and V. Z. Groza, ”Sensor-based information appliances,” IEEE Instrum. Meas. Mag., vol. 3, no. 4, pp. 31-35, 2000.

[89] C. Herring and S. Kaplan, ”Component-based software systems for smart environments,” IEEE Pers. Commun., vol. 7, no. 5, pp. 60-61, 2000.

[90] I. A. Essa, ”Ubiquitous sensing for smart and aware environments,” IEEE Pers. Commun., vol. 7, no. 5, pp. 47-49, 2000.

[91] J. Kahn, R. Katz, and K. Pister, ”Next century challenges: Mobile networking for “Smart Dust”,” Proc. 5th Annu. ACM/IEEE Int. Conf. Mob. Comput. Netw., pp. 271-278, 1999.

[92] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, ”The Cricket location-support system,” Proc. 6th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom 00, pp. 32-43, 2000.

[93] G. J. Pottie and W. J. Kaiser, ”Wireless integrated network sensors,” Commun. ACM, vol. 43, no. 5, pp. 51-58, 2000.

[94] J. M. M. Rabaey, M. J. J. Ammer, J. L. J. Da Silva, D. Patel, S. Roundy, J. L. da Silva, D. Patel, and S. Roundy, ”PicoRadio supports ad hoc ultra-low power wireless networking,” Computer (Long. Beach. Calif.), vol. 33, no. 7, pp. 42-48, 2000.

[95] E. Shih, S.-H. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan, ”Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks,” Proc. 7th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom 01, pp. 272-287, 2001.

[96] G. Hoblos, M. Staroswiecki, and A. Aitouche, ”Optimal design of fault tolerant sensor networks,” IEEE Int. Conf. Control Appl., pp. 467-472, 2000.

[97] L. Paradis and Q. Han, ”A survey of fault management in wireless sensor networks,” J. Netw. Syst. Manag., vol. 15, no. 2, pp. 171-190, 2007.

[98] A. Munir, J. Antoon, and A. Gordon-Ross, ”Modeling and Analysis of Fault Detection and Fault Tolerance in Wireless Sensor Networks,” ACM Trans. Embed. Comput. Syst., vol. 14, no. 1, pp. 1-43, 2015.

[99] K. K. Rachuri and C. S. R. Murthy, ”On the scalability of expanding ring search for dense wireless sensor networks,” J. Parallel Distrib. Comput., vol. 70, no. 9, pp. 917-929, 2010.

[100] I. Snigdh and D. Gosain, ”Analysis of scalability for routing protocols in wireless sensor networks,” Opt. - Int. J. Light Electron Opt., vol. 127, no. 5, pp. 2535-2538, 2016.

[101] V. K. Verma, S. Singh, and N. P. Pathak, ”Analysis of scalability for AODV routing protocol in wireless sensor networks,” Opt. - Int. J. Light Electron Opt., vol. 125, no. 2, pp. 748-750, 2014.

[102] https://www.ecnmag.com/article/2012/08/designing-low-cost-wireless-sensor-networks-real-world-applications

[103] J. Polo, G. Hornero, C. Duijneveld, A. Garcia, and O. Casas, ”Design of a low-cost Wireless Sensor Network with UAV mobile node for agricultural applications,” Comput. Electron. Agric., vol. 119, pp. 19-32, 2015.

[104] E. Unsal, ”Low Cost Wireless Sensor Networks for Environment,” The online Journal of Science and Technology, vol. 6, no. 2, pp. 61-67, 2016.

[105] M. Hempstead, M. J. Lyons, D. Brooks, and G.-Y. Wei, ”Survey of hardware systems for wireless sensor networks,” J. Low Power Electron., vol. 4, no. 1, pp. 11-20, 2008.

[106] A. Engel, A. Friedmann, M. Koch, J. Rohlfing, T. Siebel, D. Mayer, and A. Koch, ”Hardware-accelerated Wireless Sensor Network for Distributed Structural Health Monitoring,” Procedia Technol., vol. 15, no. 6151, pp. 737-746, 2014.

[107] Chun Kit Ng, Chun Ho Wu, W. H. Ip, J. Zhan, G. T. S. Ho, C. Y. Chan, Network Topology Management Optimization of Wireless Sensor Network (WSN),

Intelligent Computing Theories and Application, Volume 9772 of the series Lecture Notes in Computer Science pp 850-859, Date: 12 July 2016.

[108] ] K. Hari Krishna, Y. Suresh Babu, Tapas Kumar, Wireless Network Topological Routing in Wireless Sensor Networks, Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) 2016, Volume 79, 2016, Pages 817-826.

[109] Y. Zhang, Q. Chen, G. Liu, W. Shen, and G. Wang, "Environment Parameters Control Based on Wireless Sensor Network in Livestock Buildings," Int. J. Distrib. Sens. Networks, vol. 2016, 2016.

[110] R. Marfievici, A. L. Murphy, G. Pietro Picco, F. Ossi, and F. Cagnacci, "How Environmental Factors Impact Outdoor Wireless Sensor Networks: A Case Study," Proc. IEEE 10th Int. Conf. Mob. Ad-Hoc Sens. Syst. (MASS 13), pp. 565-573, 2013.

[111] S. Sivathasan and D. OBrien, "Hybrid Radio and Optical Communications for Energy-efficient Wireless Sensor Networks.," IETE J. Res., vol. 57, no. 5, pp. 399-406, 2011.

[112] D. Anguita, D. Brizzolara, and G. Parodi, "Optical wireless communication for underwater Wireless Sensor Networks: Hardware modules and circuits design and implementation," Ocean. 2010 Mts/Ieee Seattle, no. July 2016, pp. 1-8, 2010.

[113] Antonio Moschitta and Igor Neri "Power consumption Assessment in Wireless Sensor Networks," ICT - Energy - Concepts Towards Zero - Power Information and Communication Technology, Dr. Giorgos Fagas (Ed.), InTech, DOI: 10.5772/57201. 2014.

[114] S. Chen, J. Yao, and Y. Wu, "Analysis of the power consumption for wireless sensor network node based on ZigBee," in International Workshop on Information and Electronics Engineering (IWIEE), 2012, vol. 29, pp. 1994-1998.

[115] A. Damaso, D. Freitas, N. Rosa, B. Silva, and P. Maciel, "Evaluating the power consumption of wireless sensor network applications using models.," Sensors (Basel)., vol. 13, no. 3, pp. 3473-500, 2013.

[116] X. Wang, D. Le, H. Cheng, and C. Xie, "All-IP wireless sensor networks for real-time patient monitoring," J. Biomed. Inform., vol. 52, pp. 406-417, 2014.

[117] Snigdh , D. Gosain , N. Gupta, "Optimal sink placement in backbone assisted wireless sensor networks," Egyptian Informatics Journal, vol. 17, pp. 217-225, 2016.

[118] Reza Azarderakhsh, Amir H. Jahangir, Manijeh Keshtgary. "A New Virtual Backbone for Wireless Ad-Hoc Sensor Networks with Connected Dominating Set," WONS 2006 : Third Annual Conference on Wireless On-demand Network Systems and Services, Jan 2006, Les Menuires (France), pp.191-195, 2006.

[119] S. M. N. Z. J. H. Alam, Ḧierarchical and Nonhierarchical Three-Dimensional Underwater Wireless Sensor Networks," Arxiv, pp. 21, 2010.

[120] Miriam Carlos-Mancilla, Ernesto Lpez-Mellado, and Mario Siller, "Wireless Sensor Networks Formation:Approaches and Techniques," Journal of Sensors, vol. 2016, 2016.

[121] P. S. Vinayagam, "A Survey of Connected Dominating Set Algorithms for Virtual Backbone Construction in Ad Hoc Networks," International Journal of Computer Applications, Vol. 143, No.9, 2016.

[122] S. Ren, P. Yi, D. Hong, Y. Wu, and T. Zhu, "Distributed construction of connected dominating sets optimized by minimum-weight spanning tree in wireless ad-hoc sensor networks," in Proceedings - 17th IEEE International Conference on Computational Science and Engineering, CSE 2014, Jointly with 13th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2014, 13th International Symposium on Pervasive Systems, Algorithms, and Networks, I-SPAN 2014 and 8th International Conference on Frontier of Computer Science and Technology, FCST 2014, 2015, pp. 901-908.

[123] A. V. . Sutagundar and S. S. . Manvi, ”Fish bone structure based data aggregation and routing in wireless sensor network: Multi-agent based approach,” Telecommun. Syst., vol. 56, no. 4, pp. 493-508, 2014.

[124] X. Kui, Y. Sheng, H. Du, and J. Liang, ”Constructing a CDS-based network backbone for data collection in wireless sensor networks,” Int. J. Distrib. Sens. Networks, vol. 2013, 2013.

[125] Lifford McLauchlan, Soumya Saha and Rajab Challoo, ”Comparative Study of SWST (Simple Weighted Spanning Tree) and EAST (Energy Aware Spanning Tree),” International Journal of Networked and Distributed Computing, Vol. 2, No. 3, 148-155, 2014.

[126] Ayegl Tysz Erman, Arta Dilo and Paul Havinga, ”A virtual infrastructure based on honeycomb tessellation for data dissemination in multi-sink mobile wireless sensor networks,” EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 17, 2012.

[127] J. Guadalupe Olascuaga-Cabrera, Ernesto Lpez-Mellado, Andres Mendez-Vazquez, and Flix Francisco Ramos-Corchado, ”A Self-Organization Algorithm for Robust Networking of Wireless Devices,” IEEE Sensors Journal, Vol. 11, No. 3, 2011.

[128] Mohamed Lehsaini and Herv Guyennet, ”An efficient cluster-based self-organisation algorithm for wireless sensor networks,” Int. J. Sensor Networks, Vol. 7, No, 1/2, 2010.

[129] M. Khan, G. Pandurangan, and V. S. A. Kumar, ”Distributed Algorithms for Constructing Approximate Minimum Spanning Trees in Wireless Sensor Networks,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 1, pp. 124-139, 2009.

[130] Jun Xiao and Xiaochuan Zheng,”Research of three-dimensional localization algorithm based on DV-Hop AC-PSO” The 26th Chinese Control and Decision Conference (CCDC-2014), doi:10.1109/CCDC.2014.6852225, 2014.

[131] S. Kumar and D. K. Lobiyal, "Power efficient range-free localization algorithm for wireless sensor networks," Wirel. Networks, vol. 20, no. 4, pp. 681-694, 2014.

[132] S. Kumar and D. K. Lobiyal, "An advanced DV-Hop localization algorithm for wireless sensor networks," Wirel. Pers. Commun., vol. 71, no. 2, pp. 1365-1385, 2013.

[133] Jicheng Liu, Wenxiu Wang, Yintong Shang, "An improving Localization algorithm for wireless sensor networks based on DV-Hop" International Conference on Measurement, Information and Control (MIC), pp. 511-515, doi: 10.1109/MIC.2012.6273353, 2012.

[134] Dai Ying, Wang Jianping, Zhang Chongwei, "Improvement of DV-Hop Localization Algorithms for Wireless Sensor Networks," 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), pp. 23-25,doi: 10.1109/WICOM.2010.5601372, 2010.

[135] G. Han, H. Xu, J. Jiang, L. Shu, T. Hara, and S. Nishio, "Path planning using a mobile anchor node based on trilateration in wireless sensor networks," Wirel. Commun. Mob. Comput., vol. 13, no. 14, pp. 1324-1336, 2013.

[136] G. Han, C. Zhang, J. Lloret, L. Shu, and J. J. P. C. Rodrigues, "A mobile anchor assisted localization algorithm based on regular hexagon in wireless sensor networks," Sci. World J., vol. 2014, 2014.

[137] Zhen Hu, Dongbing Gu , Zhengxun Song, Hongzuo Li "Localization in wireless sensor networks using a mobile anchor node," International Conference on Advanced Intelligent Mechatronics AIM,2008.

[138] Qiang Tang, Kun Yang, Ping Li, Jianming Zhang, Yuansheng Luo and Bing Xiong "An energy efficient MCDS construction algorithm for wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, Vol. 83, pp. 1-15, 2012.

[139] Yu Hu , Xuemei Li, ”An improvement of DV-Hop localization algorithm for wireless sensor networks”, Telecommun Syst, Vol. 53, Issue 1, pp. 13-18, 2013.

[140] Dengyi Zhang, Feng Liu, Lei Wang, Yuanxiu Xing, ”DV-Hop localization algorithms based on centroid in wireless sensor networks,” 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 3216-3219, 2012.

[141] Xiao Chen and Benliang Zhang, ”Improved DV-Hop Node Localization Algorithm in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, Vol. 2012, Article ID 213980, doi:10.1155/2012/213980, 2012.

[142] Ahmad El Assaf, Slim Zaidi, So FeneAffes, Nahi Kandil, ”Hop-Count Based Localization Algorithm for Wireless Sensor Networks.” 13th Mediterranean Microwave Symposium (MMS), Vol. 1, Issue. 6, pp. 2-5, 2013.

[143] R. M. Curry and J. Cole Smith, ”A Survey of Optimization Algorithms for Wireless Sensor Network Lifetime Maximization,” Comput. Ind. Eng., vol. 101, pp. 145166, 2016.

[144] P. Kuila and P. K. Jana, ”Energy Efficient Load-Balanced Clustering Algorithm for Wireless Sensor Networks,” Procedia Technol., vol. 6, pp. 771-777, 2012.

[145] Y. Liao, H. Qi, and W. Li, ”Load-balanced clustering algorithm with distributed self-organization for wireless sensor networks,” IEEE Sens. J., vol. 13, no. 5, pp. 1498-1506, 2013.

[146] J. He, S. Ji, Y. Pan, and Z. Cai, ”Approximation algorithms for load-balanced virtual backbone construction in wireless sensor networks,” Theor. Comput. Sci., vol. 507, pp. 2-16, 2013.

[147] J. He, S. Ji, M. Yan, Y. Pan, and Y. Li, ”Genetic-algorithm-based construction of load-balanced CDSs in wireless sensor networks,” in Proceedings - IEEE Military Communications Conference MILCOM, 2011, pp. 667-672.

[148] J. S. He, S. Ji, R. Beyah, Y. Xie, and Y. Li, "Constructing load-balanced virtual backbones in probabilistic wireless sensor networks via multi-objective genetic algorithm, Trans. Emerg. Telecommun. Technol., vol. 26, no. 2, pp. 147-163, 2015.

[149] A. Raha, M. K. Naskar, and A. Paul, "A Genetic Algorithm Inspired Load Balancing Protocol for Congestion Control in Wireless Sensor Networks using Trust Based Routing Framework ( GACCTR )," I. J. Comput. Netw. Inf. Secur., no. July, pp. 9-20, 2013.

[150] S. L. N. Sayali M.Wani, "Identification of Balanced Node for Data Aggregation in Wireless Sensor Network," in International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016, 2016, no. May, pp. 2344-2348.

[151] P. Wan, K. Alzoubi, and O. Frieder, "Distributed construction of connected dominating set in wireless ad hoc networks," INFOCOM 2002. Twenty-First , vol. 0, no. c, pp. 1597-1604, 2002.

[152] M. Kalantari, M. Haghpanahi, and M. Shayman, "A p-norm flow optimization problem in dense wireless sensor networks," in Proceedings of the 27th Conference on Computer Communications (IEEE INFOCOM 2008), 2008, pp. 341-345.

[153] D. F. Larios, J. Barbancho, F. J. Molina, and C. Len, "LIS: Localization based on an intelligent distributed fuzzy system applied to a WSN," Ad Hoc Networks, vol. 10, no. 3, pp. 604-622, 2012.

[154] V. K. Singh and V. Sharma, "Elitist Genetic Algorithm Based Energy Balanced Routing Strategy to Prolong Lifetime of Wireless Sensor Networks," Chinese J. Eng., vol. 2014, pp. 1-6, 2014.

[155] B. Peng and L. Li, "An improved localization algorithm based on genetic algorithm in wireless sensor networks," Cogn. Neurodyn., vol. 9, no. 2, pp. 249-256, 2015.

[156] F. Wang, C. Wang, Z. Wang, and X. Zhang, "A Hybrid Algorithm of GA + Simplex Method in the WSN Localization," Int. J. Distrib. Sens. Networks, vol. 2015, pp. 1-9, 2015.

[157] S. Li and F. Qin, "A dynamic neural network approach for solving nonlinear inequalities defined on a graph and its application to distributed, routing-free, range-free localization of WSNs," Neurocomputing, vol. 117, pp. 72-80, 2013.

[158] P. Cottone, S. Gaglio, G. Lo Re, and M. Ortolani, "A machine learning approach for user localization exploiting connectivity data," Eng. Appl. Artif. Intell., vol. 50, pp. 125-134, 2016.

[159] A. Cspedes-mota, G. Castan, A. F. Martnez-herrera, and L. E. Crdenas-barrn, "Optimization of the Distribution and Localization of Wireless Sensor Networks Based on Differential Evolution Approach," vol. 2016, 2016.

[160] L. W. Chen, "Cooperative energy-efficient localization with node lifetime extension in mobile long-thin networks," J. Netw. Comput. Appl., vol. 64, pp. 89-97, 2016.

[161] A. O. De S, N. Nedjah, and L. D. M. Mourelle, "Distributed efficient localization in swarm robotics using Min-Max and Particle Swarm Optimization," Expert Syst. Appl., vol. 50, pp. 55-65, 2016.

[162] V. Sharma and A. Grover, "A modified ant colony optimization algorithm (mACO) for energy efficient wireless sensor networks," Optik (Stuttg)., vol. 127, no. 4, pp. 2169-2172, 2016.

[163] H. Shakibian and N. Moghadam Charkari, "In-cluster vector evaluated particle swarm optimization for distributed regression in WSNs," J. Netw. Comput. Appl., vol. 42, pp. 80-91, 2014.

[164] T. Bhatia, S. Kansal, S. Goel, and A. K. Verma, "A genetic algorithm based distance-aware routing protocol for wireless sensor networks," Comput. Electr. Eng., vol. 56, no. c, pp. 441-455, 2016.

[165] M. Khalily-Dermany, M. Shamsi, and M. J. Nadjafi-Arani, "A convex optimization model for topology control in network-coding-based-wireless-sensor networks," Ad Hoc Networks, 2017.

[166] Y. E. E. Ahmed, K. H. Adjallah, R. Stock, and S. F. Babikier, "Wireless Sensor Network Lifespan Optimization with Simple, Rotated, Order and Modified Partially Matched Crossover Genetic Algorithms," IFAC-PapersOnLine, vol. 49, no. 25, pp. 182-187, 2016.

[167] A. Srinivasan and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks," Encycl. Wirel. Mob. Commun., pp. 1-26, 2007.

[168] L. Lazos and R. Poovendran, "HiRLoc: high-resolution robust localization for wireless sensor networks," Sel. Areas Commun. IEEE J., vol. 24, no. 2, pp. 233-246, 2006.

[169] 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.

[170] L. Lazos, R. Poovendran, and S. apkun, "ROPE: robust position estimation in wireless sensor networks," in Proceedings of the 4th international symposium on Information processing in sensor networks, 2005, p. 43.

[171] S. Capkun and J. Hubaux, "Secure Positioning in Wireless Networks," vol. 24, no. 2, pp. 221-232, 2006.

[172] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," in Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on, 2006, pp. 277-283.

[173] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization in sensor networks using transmission range variation," in Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, 2005.

[174] Y. Liao, H. Qi, and W. Li, W. Du, L. Fang, and P. Ning, ”LAD: Localization anomaly detection forwireless sensor networks,” in Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, 2005, p. 41a–41a.

[175] C. Wang and L. Xiao, ”Sensor localization in concave environments,” ACM Trans. Sens. Networks, vol. 4, no. 1, pp. 3, 2008.

[176] F. Anjum, S. Pandey, and P. Agrawal, ”Secure Localization in Sensor Networks using Transmission Range Variation,” in Proceedings of the IEEE international conference on mobile ad hoc and sensor systems, 2005, pp. 9-203.

[177] Y. Zhang, W. Liu, Y. Fang, and D. Wu, ”Secure localization and authentication in ultra-wideband sensor networks,” Sel. Areas Commun. IEEE J., vol. 24, no. 4, pp. 829-835, 2006.

[178] N. Sastry, U. Shankar, and D. Wagner, ”Secure verification of location claims,” in Proceedings of the 2nd ACM workshop on Wireless security, 2003, pp. 1-10.

[179] S. apkun, L. Buttyn, and J.-P. Hubaux, ”SECTOR: secure tracking of node encounters in multi-hop wireless networks,” in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, pp. 21-32.

[180] K. B. Rasmussen and S. apkun, ”Location privacy of distance bounding protocols,” in Proceedings of the 15th ACM conference on Computer and communications security, 2008, pp. 149-160.

[181] G. Han, L. Liu, J. Jiang, L. Shu, and J. Rodrigues, ”A Collaborative Secure Localization Algorithm Based on Trust Model in Underwater Wireless Sensor Networks,” Sensors, vol. 16, no. 2, p. 229, 2016.

[182] T. Zhang, J. He, X. Li, and Q. Wei, ”A Signcryption-based Secure Localization Scheme in Wireless Sensor Networks,” Phys. Procedia, vol. 33, pp. 258-264, 2012.

[183] R. Garg, A. Varna, and M. Wu, ”An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks,” Inf. Forensics Secur. IEEE Trans., vol. 7, no. 2, pp. 717-730, 2012.

[184] M. Jadliwala, S. Zhong, S. Upadhyaya, C. Qiao, and J.-P. Hubaux, ”Secure distance-based localization in the presence of cheating beacon nodes,” Mob. Comput. IEEE Trans., vol. 9, no. 6, pp. 810-823, 2010.

[185] Q. Mi, J. A. Stankovic, and R. Stoleru, ”Practical and secure localization and key distribution for wireless sensor networks,” Ad Hoc Networks, vol. 10, no. 6, pp. 946-961, 2012.

[186] T. Shu, Y. Chen, and J. Yang, ”Protecting multi-lateral localization privacy in pervasive environments,” IEEE/ACM Trans. Netw., vol. 23, no. 5, pp. 1688-1701, 2015.

[187] A. Srinivasan, ”SecLoc–secure localization in WSNs using CDS,” Secur. Commun. Networks, vol. 4, no. 7, pp. 763-770, 2011.

[188] Zhu, W.T., Xiang, Y., Zhou, J., Deng, R.H., Bao, F. ”Secure localization with attack detection in wireless sensor networks,” Int. J. Inf. Secur. 10, 155-171, 2011.

[189] S. Jha, S. Tripakis, S. A. Seshia, and K. Chatterjee, ”Game theoretic secure localization in wireless sensor networks,” in Internet of Things (IOT), 2014 International Conference on the, 2014, pp. 85-90.

[190] Z. Merhi, A. Haj-Ali, S. Abdul-Nabi, and M. Bayoumi, ”Secure localization for wireless sensor networks using decentralized dynamic key generation,” in Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, 2012, pp. 543-548.

[191] C.-C. Chang, W.-Y. Hsueh, and T.-F. Cheng, ”A Dynamic User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks,” Wirel. Pers. Commun., vol. 89, no. 2, pp. 447-465, 2016.

[192] C.-H. Lin, Y.-H. Huang, A. D. Yein, W.-S. Hsieh, C.-N. Lee, and P.-C. Kuo, ”Mutual trust method for forwarding information in wireless sensor networks using random secret pre-distribution,” Adv. Mech. Eng., vol. 8, no. 4, 2016.

[193] A. Rasheed and R. N. Mahapatra, "The three-tier security scheme in wireless sensor networks with mobile sinks," Parallel Distrib. Syst. IEEE Trans., vol. 23, no. 5, pp. 958-965, 2012.

[194] Liu, X., Yang, R., Cui, Q. "An Efficient Secure DV-Hop Localization for Wireless Sensor Network," Intl. J. Sec. Appl., vol. 9,no. 7, 2015.

[195] www.isi.edu/nsnam/ns-doc/node217.html

[196] Perkins, D.D., Tumati, R., Wu, H., Ajbar, I. "Localization in Wireless Ad Hoc Networks," Resource Management in Wireless Networking. pp. 507-542. Kluwer Academic Publishers, 2005.

[197] Boukerche, A., Oliveira, H.A.B.F., Nakamura, E.F., Loureiro, A.A.F. "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems," Comput. Commun., vol, 31,no. 12, pp. 2838-2849, 2008.

[198] Chintalapudi, K.K. "On the Feasibility of Ad-Hoc Localization Systems," Tech. Rep., Comput. Sci. Dep. Univ. South. California, vol. 117, 2003.

[199] Cao Xiao-mei , Yu Bo , Chen Gui-hai, R.F. "Security Analysis on Node Localization Systems of Wireless Sensor Networks," J. Softw.,vol. 19, pp. 879-887, 2008.

[200] Jiang, J., Han, G., Zhu, C., Dong, Y., Zhang, N." Secure Localization in Wireless Sensor Networks: A Survey (In- vited Paper)," J. Commun., vol. 6,no. 123, 2011.

[201] Xu, W., Ma, K., Trappe, W., Zhang, Y. "Jamming sensor networks: attack and defense strategies," IEEE Network, vol. 20,no. 3, pp. 41-47, 2006.

# Publications

[1] Gulshan Kumar, Mritunjay Kumar Rai, "An energy efficient and optimized load balanced localization method using CDS with one-hop neighbourhood and genetic algorithm in WSNs," J. Netw. Comput. Appl. 78, C (January 2017), 73-82. DOI: https://doi.org/10.1016/j.jnca.2016.11.013 (SCI/SCIE Indexed with Impact Factor 2.33)

[2] Gulshan Kumar, Mritunjay Kumar Rai, Hye jin Kim, Rahul Saha "A secure localization approach using mutual authentication and insider node validation in wireless sensor networks," Mobile Information System. (Accepted, SCI/SCIE Indexed with Impact Factor 1.4).

[3] Gulshan Kumar, Mritunjay Kumar Rai "An Improved DV-Hop Algorithm with Minimum Connected Dominating Set for Mobile Nodes in Wireless Sensor Networks," Engineering Letters. (Accepted, Scopus Indexed).

[4] Gulshan Kumar, Mritunjay Kumar Rai, Rahul Saha "Improvement of Trust and Reputation using Intrusion Detection and Authentication in Ad Hoc Networks," International Journal of Security and Its Applications, Vol. 10, No. 4, pp.63-70, 2016. (Scopus indexed)

[5] Gulshan Kumar, Mritunjay Kumar Rai, Rahul Saha ”SeLHOC: Secured Location Estimation With One Hop Clusters In Wireless Sensor Networks,” International Journal of Applied Engineering Vol. 10, No. 5, 2015. (Scopus Indexed)

[6] Gulshan Kumar, Mritunjay Kumar Rai Enhancement of Security in MAODV using SHA-512 , Information, Vol 17, pp: 1857-1864, May 2014. (Scopus, SCIE Indexed)

[7] Gulshan Kumar, Mritunjay Kumar Rai, ”Performance analysis of M-Confidant protocol (Multicast based co-operation of nodes fairness in dynamic ad hoc network”, 2nd International Conference on Computing Science - Wilkes100, 2014.

[8] Gulshan Kumar, Mritunjay Kumar Rai, ”Securing Range Free Localization against Wormhole Attack using Distance Estimation and Maximum Likelihood Estimation in Wireless Sensor Networks,” Journal of Network and Computer Applications (Elsevier). (Communicated)