AN INTELLIGENT ALGORITHM FOR ENERGY EFFICIENT AND SECURE LOCALIZATION IN WIRELESS SENSOR NETWORKS

A
Thesis
submitted to

For the award of

DOCTOR OF PHILOSOPHY (Ph.D)

in

ELECTRONICS AND COMMUNICATION ENGINEERING

By
Rekha
(Registration No. 11512763)

Supervised By
Dr. Gulshan Kumar
Associate Professor, School of Computer Science Engineering

LOVELY FACULTY OF TECHNOLOGY AND SCIENCES

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

August 30, 2020

DECLARATION

I declare that the thesis entitled "An Intelligent Algorithm for Energy Efficient and Secure Localization in Wireless Sensor Networks" has been prepared by me under the guidance of Dr. Gulshan Kumar, Associate Professor, School of Computer Science and Engineering, Lovely Professional University, India. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Rekha
School of Electronics and Electrical Engineering
Lovely Professional University
Jalandhar, Delhi G.T.Road (NH-1)
Phagwara, Punjab-144411, India
Date: August 30, 2020

CERTIFICATE

This is to certify that the thesis entitled "An Intelligent Algorithm for Energy Efficient and Secure Localization in Wireless Sensor Networks", which is being submitted by Ms. Rekha for the award of the degree of Doctor of Philosophy in Electronics and Communication Engineering from the Lovely Faculty of Technology and Sciences, Lovely Professional University, Punjab, India, is entirely based on the work carried out by her 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. Gulshan Kumar
Associate Professor
School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab-144411, India
Date: August 30, 2020

DEDICATION

"I would like to dedicate my thesis to Late Dr. Mritunjay Kumar Rai for his teaching, guidance, encouragement and invaluable suggestions, which i still miss everyday. "

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to my supervisor, Dr. Gulshan Kumar, 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 very much grateful to Late Dr. Mritunjay Kumar Rai, for his supervision from the initial stage of my research work, motivation, enthusiasm and immense knowledge.

I want to express my gratitude towards my loving husband for his constant care and support as he always encouraged me to never ever give up. I would like to show my gratitude to Dr. Rahul Saha and Dr. Reji Thomas for their valuable suggestions and support during my research.

I am also grateful to the friends and fellow researchers, particularly Sandeep Kaur, Romaan Nazir, Ankita Soni, Kajal Katoch and Kaya Puri for their constructive criticism and suggestions. I would like to show my gratitude to the entire family of Lovely Professional University and School of Electronics and Electrical Engineering for providing me a suitable research atmosphere to carry out my work in proper time.

I am also very much grateful to my parents, 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: August 30, 2020 Rekha

Abbreviations

Abbreviations	Description
OSI	Open Systems Interconnection
WPAN	Wireless Personal Area Networks
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Networks
WWAN	Wireless Wide Area Networks
IR	Infra-Red
WIMAX	Worldwide Interoperability for Microwave Access
AP	Access Point
WSNs	Wireless Sensor Networks
MANETs	Mobile Ad hoc Networks
MEMS	Micro-Electro-Mechanical Systems
VLSI	Very Large Scale Integration
CPU	Central Processing Unit
BS	Base Station
MINA	Multi-hop Infrastructure Network Architecture
PDA	Personal Digital Assistant
UNPF	Unified Network Protocol Framework
ADC	Analog-to-Digital Converter
RF	Radio Frequency
IA	Industrial Automation
ECG	Electrocardiogram

EMG	Electromyogram
DV-Hop	Distance Vector-Hop
GPS	Global Positioning System
UTM	Universal Transverse Mercator
ToA	Time of Arrival
TDoA	Time Difference of Arrival
AoA	Angle of Arrival
RSSI	Received Signal Strength Indicator
APIT	Approximate Point in Triangle
PIT	Point in Triangulation
SNSB	Static Node Static Beacon
MNSB	Mobile Node Static Beacon
ADC	Analog-to-Digital Convertor
SNMB	Static Node Mobile Beacon
MNMB	Mobile Node Mobile Beacon
PERLA	Power-Efficient Range-free Localization Algorithm
HCQ	Hop-Count Quantization
MDS	Multi-Dimensional Scaling
PSO	Particle Swarm Optimization
NDV-Hop	Novel Distance Vector-Hop
EM-Hop	Error Correction and Multi-Hop
IBDV-Hop	Improved Bat-based Distance Vector-Hop
TLBO	Teaching Learning Based Optimization
EWCL	Enhanced Weighted Centroid Localization algorithm
LWC	Linear Weighting Centroid
NWC	Neighbor Weighting Centroid
HTCRL	Homothetic Triangle Cyclic Refinement Location
AOD	Angle of Departure
DCRL	Distributed cooperative Range-free Localization
CDS	Connected Dominating Set
UDG	Unit Disk Graph
MCDS	Minimum Connected Dominating Set
SCDS	Strongly Connected Dominating Set
AORED	Algorithm on Optimized Region Efficient Data
LNSM	Log-Normal Shadowing Model
PSO-ANN	Particle Swarm Optimization-Artificial Neural Network

GWOLN	Golf wolf Optimization for Localization Node
OCS	Orient Cuckoo Search
SFLA	Shuffled-Frog Leaping Algorithm
GA	Genetic Algorithm
EPSOCEO	Enhanced PSO-based Clustering Energy Optimization
ELM	Extreme Learning Machine
SLFN	Single-hidden Layer Feed-forward Network
NLOS	Non-Line-of Sight
VPSO	Vector Particle Swarm Optimization
LNNE	Localization using Neural Network Ensembles
EMSO	Enhanced Mass Spring Optimization
LNSM	Log-Normal Shadowing Model
LSE	Least Square Estimation
FSO	Fish Swarm Optimization
MAP-M& N	Mobile Anchor Positioning-Mobile Anchor& Neighbor
CH	Cluster Head
SSLA	Salp Swarm Localization Algorithm
LU	Localized Unit
P2P	Peer to Peer
T2FL	Type-2 Fuzzy Logic
AWGN	Additive White Gaussian Noise
SERENE	SElecting REpresentatives in sensor NEetworks
CPS	Colored Petri Nets
DCMAC	Distributed Cross-layer cooperative MAC
ODS-MAC	On-demand Scheduling Cooperative MAC
EACCMAC	Energy-Aware Cross-layer Cooperative MAC
BRSL	BRS-based Robust algorithm for Secure Localization
SSLS	Signcryption-based Secure Localization Scheme
RTT	Round Trip Time
MAAKA	Mutual Authentication And Key Agreement
AFTNS	Activation Function-based Trusted Neighbor Selection
VANETs	Vehicular Ad hoc NETworks
BARS	Blockchain-based Anonymous Reputation System
RSUs	Road Side Units
PoW	Proof of Work
PoS	Proof of Stake

IoTs	Internet of Things
DMTR	Distributed Management Trust model and Reward
CRL	Certificate Revocation List
MOFBC	Memory-Optimized and Flexible BlockChain
GV	Generator Verifier
EECDS	Energy-Efficient Connected Dominating Set
DCL	Degree of Collinearity
RM	Relative Mobility
LE	Localization Error
RMSE	Root Mean Square Error
ALE	Average Localization Error
NNL	Neighbor Node List
RTS	Request-to-Send
CTS	Clear-to-Send
ACK	Acknowledgment
CCTS	Cooperative-CTS
HTS	Helper-to-Send
DIFS	Distributed Interframe Space
PLSN	Proportion of Localized Sensor Node
PUSN	Proportion of Unlocalized Sensor Node
LEV	Localization Error Variance

ABSTRACT

Due to advancement in technology and increasing demands of users, wireless telecommunications have grown rapidly over the past decades. It incorporates different types of fixed, mobile devices, portable two-way radios, cellular telephones, notebook computers, Personal Digital Assistants (PDAs), and wireless networking. The emergences of MicroElectroMechanical Systems (MEMSs) and wireless communications have facilitated the interaction of researchers with physical environments to communication networks. Wireless communications instigate different devices equipped with advanced systems such as Global Positioning Systems (GPS), PDAs, two-way radios, etc. without wire interface which facilitates the communication to users in different environmental conditions. The major concerns of wireless networks are limited resources, bandwidth, dynamic topology, availability of the network, different propagation properties, etc.

Recent developments introduce the new kind of networks termed as Wireless Sensor Networks (WSNs) which encompasses a broad spectrum of ideas to fulfill various desires of human. The growing usage of data from a set of sensor nodes, rise the demand of networks from static to mobile and freedom from different restriction. The main focus of the thesis is on WSNs which consists of a large number of sensor nodes for observing the physical phenomenas in various environmental conditions. These sensor nodes are small in size, low-cost and autonomous in nature. These autonomous sensor nodes observe the physical activities and atmospheric occurrences and forward

the collected data to Base-Station (BS) over a wireless link. The gathered information from tiny sensor nodes is processed by BS to perform controlling actions. The features like self-organization and rapid developments facilities WSNs as auspicious for various applications such as military applications, industrial automation, smart homes, habitat monitoring, environment monitoring, healthcare, inventory control, and surveillance, etc.

However, WSNs have various challenges and issues of concerns for the researchers such as localization, resource-constrained, bandwidth, computational power, communicational capability, storage, and network lifetime. Localization is the most challenging concern as various applications of WSNs depends upon the precise locations of sensor nodes. The localization process can discover and track the sensor nodes using different localization approaches. Range-free approaches are mostly implemented in the recent past due to ease of applicability and low-cost hardware. Therefore, it is ensured by the localization algorithm that the location estimation process should be completed by utilizing minimum resources to prolong the network lifetime. It should be capable to locate the sensor nodes precisely which improve the localization accuracy. Further, the resources at Media Access Control (MAC) should be utilized properly which ensures the improvements in network lifetime. Moreover, the security of the localization algorithm is another issue of concern. The security of location information is ensured by the localization process by using adequate security approaches.

This thesis is structured into three key sections which cover three major objectives of the research. These objectives are presented with validated results that are obtained after simulation. The first objective improves the localization accuracy with precise locations of nodes. The second objective is based on an energy-efficient approach which prolongs the network lifetime significantly. The security of localization process is ensured by third objective. The three objectives of this thesis are explained as follows:

- *An advanced DV-Hop localization algorithm* is introduced for energy-efficient and more precise localization in WSNs. A virtual backbone as Energy-Efficient Connected Dominating Set(EECDS) is constructed by using degree of connectivity and residual energy of beacon nodes. Further, to reduce the localization

error, a correction factor is also introduced. The concept of collinearity is also considered which improve the performance of localization process.

- *An energy-efficient localization algorithm at Media Access Control layer* is designed for efficient and effective localization. To accomplish better localization, the concept of cooperative communication among beacon nodes at MAC which maximize the residual energy of beacon nodes. An energy factor is also introduced which helps to reduce the energy consumption of beacon nodes. The the location information of beacon nodes are broadcasted using cooperative nodes. The cooperative beacon nodes are selected on the basis of least energy consumption using an effective and efficient scheme. Furthermore, the localization accuracy of the proposed algorithm is minimized by using correction factor for localization at BS.

- *A range-free localization algorithm powered by Blockchain technology* is presented for secure localization in WSNs. The lack of trust between nodes can be detrimental to the localization process. Various attacks and malicious activities can be executed internally or externally by the attacker to interrupt the functioning of the localization process. To address such issues, the trust values of beacon nodes are evaluated using various metrics such as reputation, mobility, residual energy, and one-hop neighbor nodes list. Further, the trust values are shared among the network for blockchain generation. The most trusty beacon nodes are selected as a miner which adds the block to the blockchain. Further, the process of localization is performed by highly trusty beacon nodes to accomplish the locations of unknown nodes.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Wireless Sensor Networks

1.1 Introduction

Wireless networks are emerging and fast technology with lots of exciting actions and communication technologies [1]. Firstly, the wireless networks are designed by the University of Hawaii under the brand ALOHAnet in 1969 and became operational in 1971. WaveLAN was the first commercial wireless network that is developed by National Cash Register (NCR) systems in 1986. Wireless networks become a significant part of the communication in which information is transmitted without any physical connection or wires [2]. The information broadcasted through a wireless network includes three different elements i.e. radio signals, the data formats, and the network structure. All three essentials are self-regulating and during a network construction, all these elements must be defined. Wireless networks are generally executed with radio frequency communication and the information is transmitted from one-point to another by radio waves. Implementation of wireless networks for radio signals is done on physical layer of Open Systems Interconnection (OSI) model [3] and data formats are controlled by higher layers. Network structure includes the adapters and base

station for transmitting, receiving and controlling of radio signals [4]. Wireless networks can be classified on the basis of network architecture and transmission coverage area as shown in Figure 1.1. The wireless networks can be further classified based

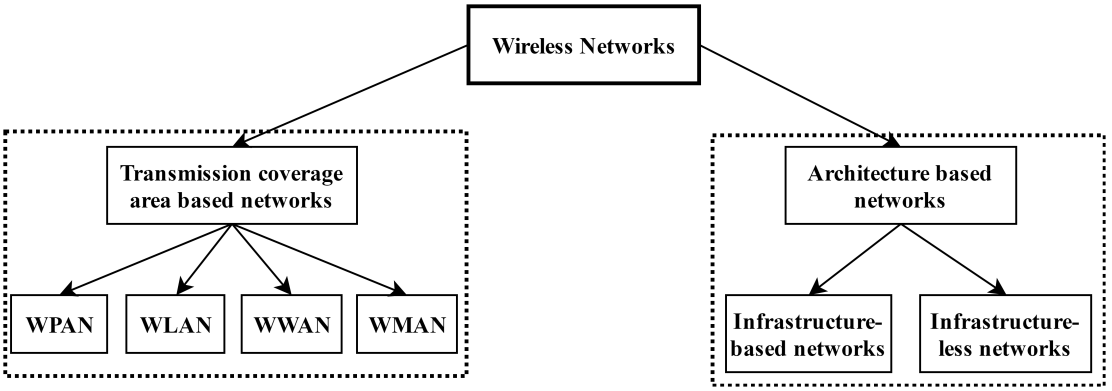

FIGURE 1.1: *Classification of wireless networks.*

on transmission coverage area into various types such as Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Wide Area Network (WWAN) and Wireless Metropolitan Area Networks (WMAN).

Two technologies such as Infra-Red (IR) and Bluetooth come in WPAN networks. In WPAN, the range of connectivity of personal systems is within 10 meters. However, a direct line of sight is required in IR [5]. In WLAN networks, the users can communicate with each other to form a network in a local area. A network can be created temporary with a few users without using Access Point (AP) [6]. In WWAN networks, the information can be transmitted, covering large areas such as cities and countries. In WMAN networks, the connection can be established between multiple networks in metropolitan areas such as large buildings in a city. A different standard body such as 802.16 and Worldwide Interoperability for Microwave Access (WiMAX) is primarily responsible for implementing WMAN [7]. On the basis of infrastructure, wireless networks are divided into two different types such as infrastructure-based and infrastructure-less networks. Infrastructure-based networks utilized AP for communication. The wireless communication can be controlled by AP, which provide faster data transmission speed with more security. The networks with predefined infrastructure are called infrastructure-based networks. In infrastructure-less networks, the infrastructure changes dynamically over time. All the devices communicate with

each other directly without a central AP device. In this type of networks, every node can take its own decision based on network requirement. Wireless Sensor Networks (WSNs) and Mobile Ad hoc Networks (MANETs) [7] are examples of infrastructure-less networks.

1.1.1 Wireless Sensor Networks

WSNs are regarded as enabling technology of an emerging field which is envisaged to solve the different problems, thus facilitating the accommodation of new advanced services and providing efficient solution to the ever-increasing user demands. The WSNs makes the association with the the physical globe and the digital world by seizing and exposing the phenomena of the real world. These phenomena can be converted into a form that can be easily assessable, storable and actable. The integration of sensor devices with various machines, devices, and atmospheres afford incredible remunerations to society. These networks can support to evade terrible infrastructures failures, conserve exquisite natural resources, improve productivity, provide more secure communication, and also enable various smart applications such as smart home technologies. The astonishing development in technologies such as Micro-Electro Mechanical System (MEMS), Very Large Scale Integration (VLSI), and wireless communications also gives more contribution to the pervasive usage of sensor networks.

WSNs are self-organized and infrastructure-less network, in which a number of small and lightweight sensor nodes are installed in the surroundings to monitor various physical phenomena and activities [8]. In traditional WSNs, one sink node was utilized for communication and these types of networks have the problem of lack of scalability when the number of sensor nodes increased in the network and size of data gathered by sink nodes increased. Moreover, the performance of the network cannot be computed without including the size of network. A general scenario of WSNs include multiple sinks for communicating information between nodes. Multiple sink nodes will diminish the probability of isolated clusters of sensor nodes that cannot distribute their

information to unfortunate environment conditions. These types of networks are more flexible and scalable as large number of sensor nodes improve performance. However, multiple sinks network scenario does not represent the trivial extension of single sink network scenarios. Sometimes, the sensor nodes forward the gathered information to a single sink node selected among multiple, and further data is transmitted to the gateway towards the final users. A suitable sink node can be selected among multiple for data transmission. In various situations, sensor nodes forward the data to the selected sink node among several sink nodes, and the sink node further broadcasts the information to the final user.

The structure of WSNs is shown in Figure 1.2 and it consists of various components

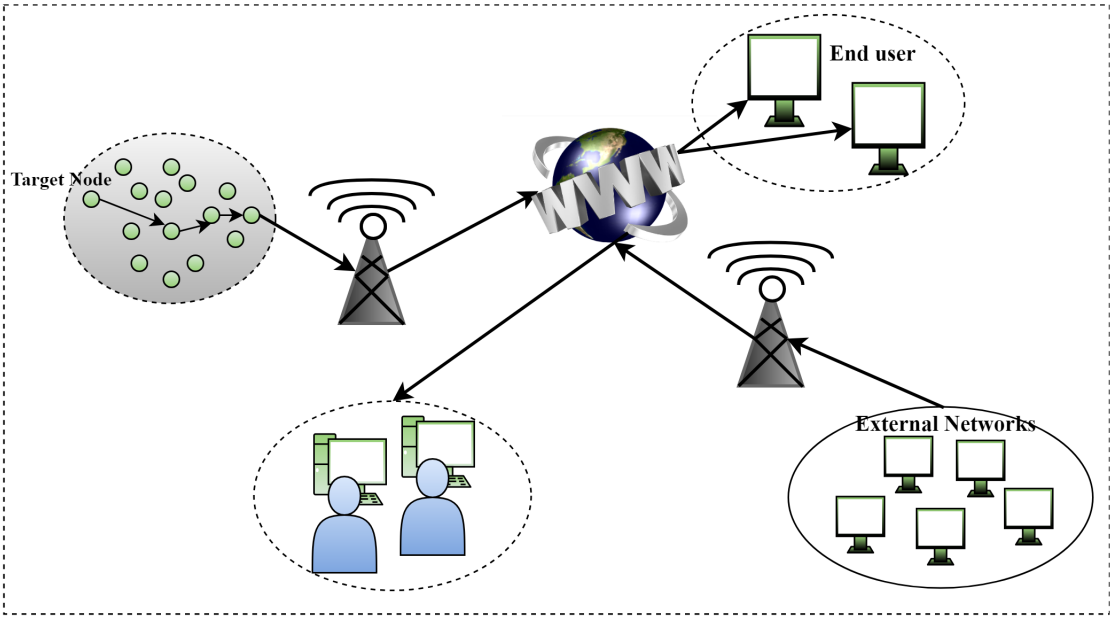

FIGURE 1.2: *Wireless Sensor Networks.*

like sensor nodes, a sink node, one or several base stations, internet or satellite for wireless communication, manager node and users.

1.1.2 Architecture of WSNs

The architecture of WSNs are classified into two categories: (1) layered architecture, and (2) clustered architecture. The detailed description about architectures

are discussed as follows:

1. Layered Architecture

The layered architecture consists of a single Base Station (BS) with various level of sensor nodes around it that corresponds to the one-hop or multi-hop to the BS depicted in Figure 1.3. Layered architectures are used in various applications within a building as a backbone, sensor-based infrastructure in the military [9]. In smart home communication, BS work as an access point to wired networks and tiny sensor nodes provide network connectivity by creating a backbone wirelessly. Personal Digital Assistant (PDA) devices are utilized by the users to communicate BS using small sensor devices. Unified Network Protocol Framework (UNPF) has a set of protocols and procedures to complete the enactment of layered architecture in WSNs [9].

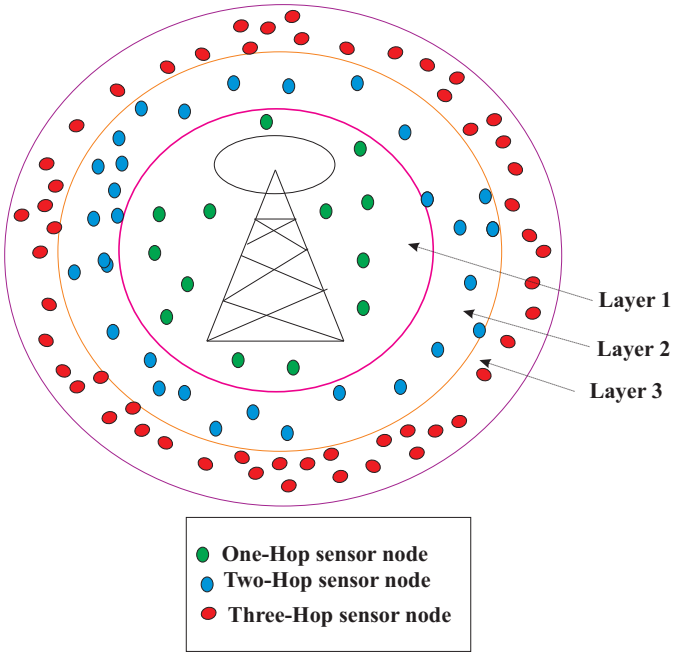

FIGURE 1.3: *Layered architecture of WSNs*

2. Clustered Architecture

The clustered architecture is established by using the perception that, sensor nodes with higher energy are utilized for data transmission of information from one point to another while sensor nodes with lowest energy perform the sensing task in specific field. The sensor nodes are organized into clusters in this type of architecture. Each cluster has a cluster head which control the operations of all cluster members. On the basis of energy some of the nodes are elected as cluster head and remaining nodes in the cluster becomes the member of that cluster [10]. After sensing the target of interest, each member transmits the gathered data to the cluster head. Further, cluster heads broadcast the information to BS. To establish the clusters and providing special tasks to cluster heads can prominently expand the lifetime, scalability and energy efficiency of WSNs. The clustered architecture of networks is depicted in Figure 1.4. It reveals that the sensed information reaches at BS with two hops communication. For more effective communication, the clustering can be extended in more depth hierarchically. The clustering architecture is generally convenient to sensor networks because of its essential suitability for data fusion. Cluster heads collect the data from all cluster participants and only essential data are extracted. After that, the information is transmitted to BS. Base stations can be either movable or stationary and these are placed successively with the network. Sensor nodes obtain environmental data and transmit data via adjacent servers to the sink node. These tiny sensor comprise of the actuator, energy unit, storage, transceiver, and CPU. Sensor nodes have restricted energy, storage and computer capacity due to resources constraints [11]. The distribution of sensor nodes are random in the environment to sense any physical activity such as light, humidity, pressure, temperature, velocity, and sound, etc.

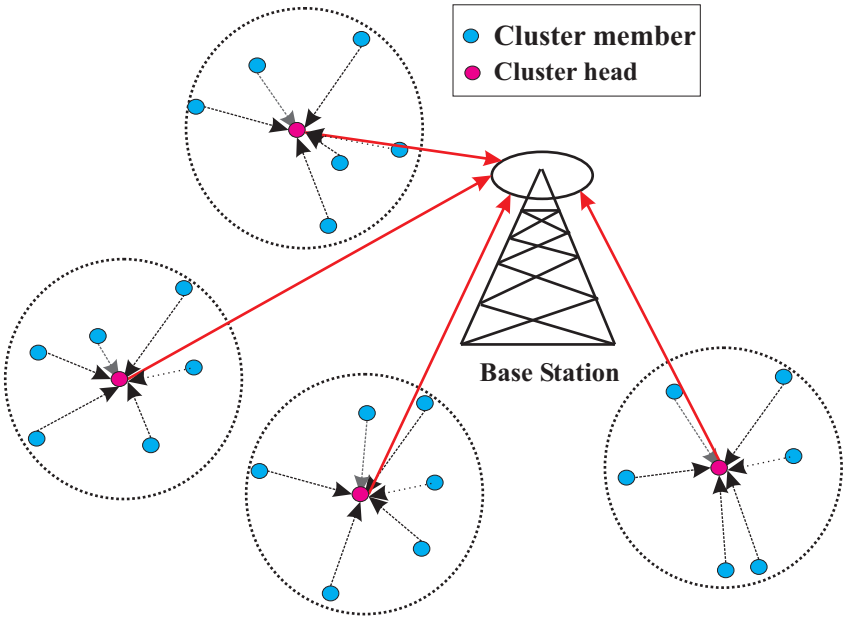

FIGURE 1.4: *Clustering in WSNs.*

1.1.3 Components of Sensor node

WSN is an array of sensor nodes that are spatially dispersed and are able to communicate via a wireless channel. The growth of microsensors has been resulted by recent developments in microelectro-mechanical devices, small energy devices and extremely embedded digital electronics [12]. Each sensor node of WSNs has different components like memory, communication device, controller, sensor or actuator and power supply as shown in Figure 1.5[13].

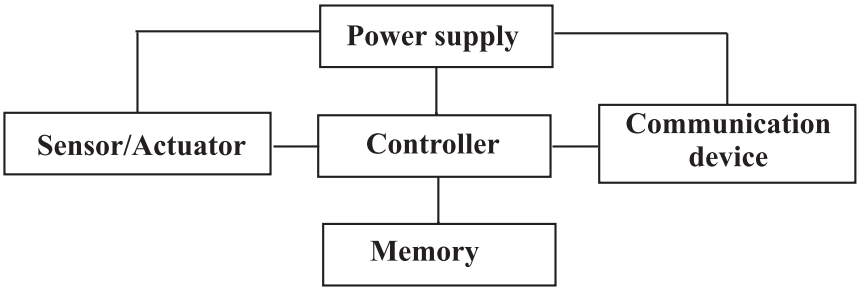

FIGURE 1.5: *Sensor node components*

- **Memory Unit:**

  Memory unit stores the sensed data of sensor nodes. WSNs network has limited memory because of small size of sensors node.

- **Power Unit:**

  The power system is the critical part of sensor node that store the energy to perform various tasks. The power in node batteries that can be rechargeable or no rechargeable. Natural resources such as solar energy are used in form of photovoltaic panels and cells for additional battery storage, wind turbine power, kinetic air power, etc.

- **Controller:**

  The microcontroller unit is responsible for various tasks, such as data processing and other node components control. This device is the primary component of the device that controls and manages all the parts of node. A small storage device built on an embedded panel or a built-on memory can be used for the controller device. A computer controls the sensor unit, cooperates with other devices through the cellular connection.

- **Sensor unit:**

  This unit is also primary component of sensor node that separates it with communication capacity from all other embedded systems. It usually comprises of several sensors that collect information from various environmental and physical circumstances. The process of sensing physical activity such as temperature, pressure, heat, sound, and light is achieved by a sensor unit. Sensor unit mainly consists of two subunits: a sensor and Analog-to-Digital Converter (ADC). The sensor input is transformed by the ADC into a digital signal, that is further transmitted to the handling device.

- **Communication device:**

  Generally a communication device is used to transfer information from sensor node to sink node during communication process. Due to the technological advancement, the reduced size and cost of devices stimulated curiosity in potential use of a big number of unattended disposable devices. Sensor node can communicates bidirectionally [14].

1.1.4 Types of WSNs

WSNs can be deployed in different areas for monitoring particular activities. Based on the environment and conditions, the WSNs can be classified as follows:

1. Multimedia WSNs
2. Underground WSNs
3. Underwater WSNs
4. Terrestrial WSNs
5. Mobile WSNs

In Multimedia WSNs, the information can be collected in the form of video, audio images, and messages. A large number of cameras and microphones are utilized for the association between all sensor nodes. The sensor nodes can sense and monitor various activities that happen in a specific time and the visual records can be preserved by nodes. All the sensor nodes are connected through wireless connection to perform different tasks such as compression, retrieval, and correlation of information [15]. Underground WSNs are very expensive and scarcely deployable as compared to terrestrial networks. The components of these types of networks are costly and required special maintenance regularly. All the sensor nodes are deployed underground for observing the activities, but the collected information is broadcasted to the base station that is deployed above the ground [16][17]. Underwater WSNs system consist of various tiny sensor nodes which are deployed underwater for monitoring purpose. The sensor nodes collect information after observing the activities and transmit that information to underwater vehicles. Underwater networks have various challenges such as propagation delay, failure of sensor nodes and lifetime of nodes [18].
WSNs are power restricted as nodes are battery powered. These sensor nodes are implemented in the hostile environment where human involvement can practically be avoided. It is almost impossible for one to replace or recharge the batteries of nodes [19]. Terrestrial WSNs consist of a large number of sensor nodes to perform various

tasks and the deployment of these nodes can be done in a structured or unstructured manner. In terrestrial WSNs, the sensor nodes are deployed above the ground and the energy for operations can be acquired using solar cells. The consumption of energy can be minimized by utilizing low duty cycles [20]. Mobile WSNs have a large number of sensor nodes that can be moved in a fixed area or dynamic area on their own. The mobile sensor nodes have the capability to sense happening physical activities and communicates the information to the base station through a wireless link. A base station can be fixed or movable in nature depends on the requirements of network scenarios. The mobile networks are more flexible than static networks but also have various challenges in terms of energy, topology, standards, routing, and validation of nodes [21].

1.2 Design challenges and applications of WSNs

WSNs are designed and deployed to perform different tasks related to object detection and tracking. The sensor nodes can be deployed in different remotes areas that are unreachable to wire and heavy devices. Sensor nodes in the network may be located many hops away from any other sensor nodes where direct communication required more power for communication. When all sensor nodes are large enough that sensor can transmit data directly to the base station using a single hop is called one-hop communication and the topology called star topology. In this type of topology, each sensor node directly communicates with the base station using the wireless link [22]. However, sensor networks often contain big geographical regions and hence radio transmitting capacity should be maintained at minimum to reduce energy consumption. Multi-hop communication is most preferable in WSNs and formed a mesh topology. Sensor nodes of this sort not only collect information, but also operate as a relay for other sensor nodes and operate together to spread sensor information to a base station. Single-hop and multi-hop communication are represented in Figure 1.6 [23].

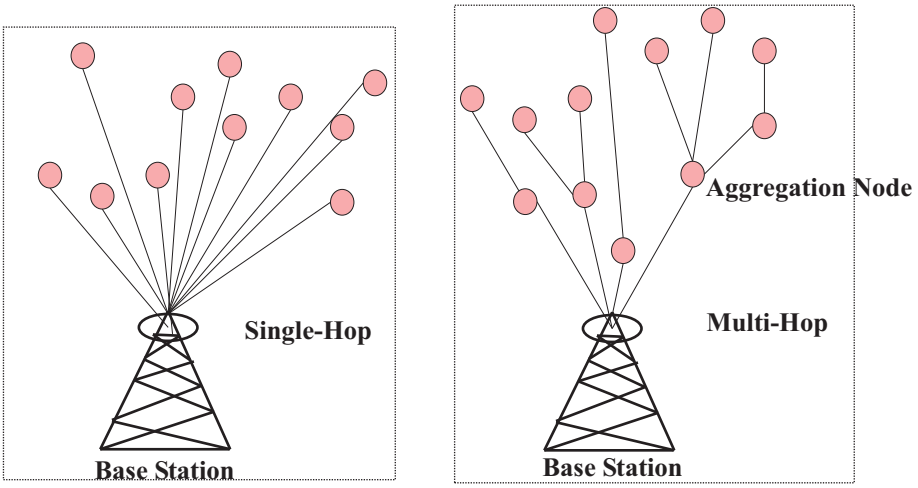

FIGURE 1.6: *WSNs communication with Single-Hop and Multi-Hop.*

1.2.1 WSNs design challenges

WSNs work as a bridge to fulfill the gap between the physical world of humans and the virtual world of technologies. WSNs provide a low-cost solution to various domain of technology. The rapid growth and development of WSNs enable its usage in a wide variety of application with variable properties. Due to emerging demand, it is very difficult to deliberate the essential hardware issues and software support. Initially, the WSNs were mainly discovered for military application with Defense Advanced Research Projects Agency (DARPA). However, various design-related issues and challenges are faced by researchers while setting up working sensor network scenarios. Different challenges and constraints of WSNs are as follows:

- **Energy**

  The intrinsic properties of each sensor node presents various challenges to the communication protocol primarily in terms of energy consumption. Each sensor node has limited energy and these nodes are powered by batteries which must be either recharged when depleted or replaced. For some particular node both options are inappropriate and simply discarded, once their energy goes down [24].

- **Self-management**

  WSNs should be able to perform the task without any human intervention after deployment. All the configuration, adaptation, repair, and maintenance should be done by WSNs itself [25].

- **Hardware and Software Issues**

  WSNs consist of a large number of sensor nodes for sensing purposes. These sensor nodes should be available at low cost and light in weight. The storage of sensor nodes is preferred inexpensive. Limited memory of each sensor node is also challenging [26]. The CPU regulates the computational capability and energy consumption of sensor nodes. Radio range of sensor nodes is also a critical issue in WSNs. Radio range ensures the network connectivity and data collection in the physical environment being monitored by sensor nodes. The software should be lightweight, low cost, less energy-consuming and hardware-independent [26].

- **Node deployment**

  Deployment of sensor nodes in developing protocols is another challenging factor and the position of sensor nodes need to be predetermined. Sensor nodes are randomly deployed in remote areas, terrain or disaster relief operations. The random deployment requires self-organizing protocols for communication protocol stack. Each node must handle itself in such a way that it is able to configure itself, cooperate with other nodes, adjust to loss, and handle itself without any human interference in changing environments. All of these characteristics must be intended to prevent unnecessary overhead energy.

- **Wireless medium**

  WSNs communication takes place via wireless media, and a sensor network developer has several problems by relying on wireless networks and communications. The Radio Frequency (RF) signals travel through a wireless medium which is affected by large and small scale. When the distance between sensor node and base station increases, the required power for transmission rapidly

increases. It is therefore power effective to separate a wide range into several smaller distances, thus promoting multi-hop transmission and tracking.

- **Network Lifetime**

  Network lifetime is also a critical issue of sensor nodes. To improve the lifetime of each sensor node without increasing power is a quite challenging. The period when the first network node does not have the power to transmit a signal is one of the most used network life expressions, since losing a node could results network losing some features.

- **Security**

  The security of WSNs is also challenging issue due to wireless medium used for transmission. In WSNs, communication is performed by open wireless channel, anyone can receives the data packets with the help of same frequency band wireless communication device. An attacker can destroy the wireless network by eavesdropping, spoofing and attacking the data packet. An attacker can modify the received data packets and re-inject these packets in the network.

- **Mobility**

  After the initial deployment of nodes, the position of nodes may change due to the requirement of environments. Mobility of nodes can result from environmental activities such as water, wind or other natural aspects, sensor nodes may be attached by moving objects and maybe possess by automation. In other words, we can say that mobility of sensor nodes may either be accidental effects or may the essential requirements of the system. Mobility may be introduced for all sensor nodes in the network or only to specified nodes. Therefore, mobility of nodes affects the performance of the networks.

- **Others challenges**

  From the above discussion, it is clear that various design factors in WSNs changes form the choices of other systems and networks. The difference between WSNs and traditional networks are tabulated in Table 1.1. There are various additional design factors which influence the design of nodes and WSNs.

For example, some sensor nodes may be attached on a moving item such as moving vehicles or robots, which continuously affects the network protocols or topologies that need repeated adaptations in routing, data aggregation, changing density and changing regions.

TABLE 1.1: *Comparisons of WSNs and traditional networks.*

Traditional wireless networks	**Wireless Sensor Networks**
These networks are designed for multiple purposes.	These types of networks are designed for the specific purpose
The prime design concerns of these networks are latencies and performance, energy conservation is not prime concern.	WSNs have limited resources such as memory, size, power and computational cost, etc.
Networks are designed according to special plans with a specific structure.	The nodes are deployed randomly with ad-hoc network structure.
The nodes or devices are functional in a controlled way.	Sensor networks are used in untrusted or hostile environments.
The devices are easily changeable and repairable for easy operation.	The physical change and repair is difficult due to the placement of nodes in remote areas.
The failure of devices are addressed through repair or maintenance	Devices failure is difficult to address by maintenance or repair.
The knowledge of network is feasible globally and utilized a centralized management.	Central management is not required and decisions are made through localization.

Various networks also require variable hardware capabilities, for example, sensor nodes may need more computation energy, storage and processing power for processing and collection of sensing data from neighbors nodes across the network. Also, some specific applications of WSNs may have certain quality and performance requirements in terms of latencies and throughput.

1.2.2 Applications of WSNs

With the advancement in communication and computation, technology get raise the necessity of distributed WSNs which have a large number of sensor nodes. Each sensor node should be able to monitor the physical activities continuously and communicate the collected information with other sensor nodes. Distributing the sensor nodes throughout the desired region is called the random deployment of nodes. There

are no specified protocols for such types of random deployment. These types of sensor networks are employed to perform various activities such as environmental monitoring, habitat monitoring to home networking and monitoring in the military. WSNs are also utilized for detection and alerting applications. It can send the signal to control room whenever a malfunction occurs in any industry. These networks are also usable for forest fire detection and the sensor broadcast an alarm signal to control room after detecting fire in the forest. On the other hand, WSNs are applicable to detect ground vibration and seismic activity by triggering an alarm. Various applications require low power, low-cost and precise algorithm for deployment. WSNs are applicable in a wide variety of applications depending upon specific requirements as shown in Figure 1.7 and these applications are as follows:

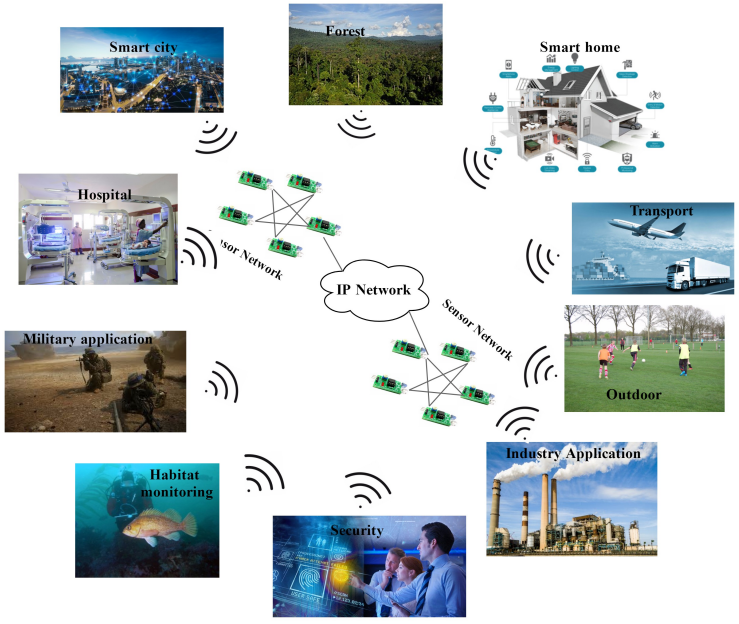

FIGURE 1.7: *Applications of WSNs.*

- Military applications
- Industrial applications
- Area monitoring
- Environmental/Earth monitoring
- Healthcare applications, and

- Commercial applications

1.2.2.1 Military applications

Due to emerging and advancement in technologies, WSNs act as a backbone for the military by conveying vital information rapidly form the area of interest and the networks are incorporated with defense applications due to its capability of sensing, reliability, fault-tolerance, and scalability. The enemies can destroy the deployed sensor networks, but these node are low-cost devices that dont affect a lot. WSNs are very beneficial for military application [28].

In the military, there is always a risk of being attacked by enemies. Therefore, the utilization of low-cost and tiny sensor nodes helps to diminish the loss. The suspicious activities by enemies such as armored vehicles, men in the foot, amount of weapon and its types can be detected, identified and classified in advance by deploying sensor nodes in available scenarios [29][30]. The networks provide reliable real-time images of war and better situational awareness. Sensing, monitoring, commanding, targeting and various tasks are performed by the deployed sensor nodes in the military. The small nodes are distributed with every troop, vehicles, critical missiles and equipments to report the current status of the suspicious activities. After collecting the reports, the information is forwarded to the base station mounted in a safe area and to the head of the troop who may further reports to the higher commanding authorities. The critical places and probable adversaries routes can be discovered by sensor nodes having a closure inspection on opposing forces activity. Intelligent missiles or shells also mounted with sensor nodes to attack the target properly [31].

1.2.2.2 Industrial applications

In industries, connected computers generate an ecosystem using WSNs that provides connection among devices in smart way[32]. Nowadays, the connected machines are built upon two approaches, one inside the factory where information regarding

the productivity of a machine collected by smart sensors has to be supplied to the key participants in the connected machine ecosystem. The other approach is much more macro level [33]. Sensors that assess a range of factors which would be useful in manufacturing applications, for example, visual strength or noise strength, voltage, current, strain, heat, XYZ position, quadrant direction, speed, positioning, liquid stream frequency, etc. are easily and cheaply produced [34]. The sensed information is further forwarded to control room with micro-controller where the information can be stored and analyzed by persons and decisions can be made, or some automation software that analyses the data and takes some action/decision. For example, if the water level goes down in some tank, which level is supposed to be maintained above a certain threshold, the decision to fill up tank can be triggered [35]. Sensors can be questioned using a micro-controller and information recorded on a storage board or transmitted via Bluetooth, Zigbee, Wi-Fi, Ethernet, cable, USB, infraround, etc. to other devices in real time. Therefore, WSNs are very essential for Industrial Automation (IA). The sensor networks provide a crucial association between the control system and the physical world. Various enlightened software and hardware are introduced for controlling systems which produce the prospects for automation in refineries, factories, sugar plants, rice plants and so many processing plants [36]. The utilization of WSNs in industrial automation affects various aspects of plant operations. The taxonomy of industrial automation is depicted in Figure 1.8.

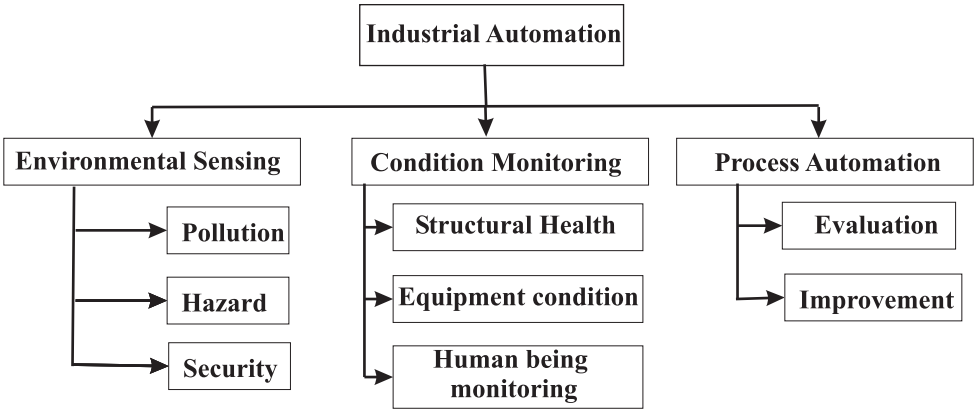

FIGURE 1.8: *Industrial automation taxonomy.*

1.2.2.3 Environmental/Earth monitoring

WSNs play significant role in different economic surveillance applications and usually these applications are separated into two categories i.e. outdoor and indoor surveillance. The indoor basically includes applications such as office and building monitoring and light, humidity, air quality and temperature are the physical aspects for sensing [37]. Outdoor monitoring includes various applications such as habitat monitoring, traffic controlling, earthquake detection, volcanoes eruption, hazardous detection, and weather forecasting, etc. The sensor nodes can be deployed, to monitor the concentration of dangerous gases in the air. WSNs are beneficial to monitor air pollution in various regions [38][39]. Wireless networks are more preferred rather than wired to make more reliable and systematic monitoring. WSNs are also applicable in forests for fire detection. Sensing nodes are distributed in forest and whenever a fire started, the sensor detects the fire. These nodes forward the sensed information towards control room to perform further controlled action. Sensing devices can helps to detect the affected fire area and firefighters can control the fire of forest. The early detection of activities is very beneficial for a successful action [40]. Further, the sensor nodes are also deployed to detect the land sliding in hilly areas. Sensor nodes enable the system to detect the slight changes in the movement of soil and small changes in different parameters that may happen during a landslide. With the help of data collection of land sliding, it may be possible to identify the future occurrence of landslides before it happens in actual. To monitor the quality of water in ocean, lakes, rivers, and dams, WSNs nodes are utilized. The sensor nodes enable to produce a more accurate map of status of water. Monitoring of water in remote areas can be possible by deploying sensor with the help of helicopters without any human intervention.

There are various example of different application like disaster relief operations, Biodiversity mapping and intelligent buildings (or bridges). In disaster relief operation sensors node are dropped from an aircraft over a wildfire, every node measures the temperature and derives a temperature map. Observing wildfire using sensors node is the example of biodiversity mapping. Reducing energy wastage by proper humidity,

ventilation, air conditioning control, measurement of room occupancy, temperature, airflow and measure mechanical stress after earthquakes [41]. Seismic activities in a large structure are detected by sensor nodes and these activities are transient in nature which have frequencies below 10 Hz. The response of the activities can be captured by deploying different physical properties sensors. However, to reduce the effects of noise and imperfect placement, sensor nodes should be oversampled at high frequency. WSNs are also very beneficial in traffic controlling to overcome the chances of jamming and accidents. Ground transportation is a crucial and complex socioeconomic key infrastructure for various operations. Operationally, the ground transport gives supports to various systems such as supply chain management, emergency response, and emergency healthcare. In urban areas, the more traffic results in prospective jamming or congestion. To build new road for all operations is neither feasible nor practicable due to lack of free space and wealth. To overcome the problems, distributed sensor systems can be placed in different areas to detect and reduce congestion. The sensor systems can collect information about the density of traffic, size, and speed of the vehicles and can suggest the new alternatives way to the drivers [42].

One more application area of WSNs is underground mining. Underground mining has the most crucial and dangerous atmosphere for the worker in the world. Various sensing tasks can be assigned to sensor nodes in WSNs for underground mining. Firstly, the sensor nodes can be deployed to discover individuals in normal or abnormal situations. Secondly, the sensor node can be utilized for detection of collapse holes in the mining [43]. Third, the nodes can be introduced to forecast and measure the seismic activities during the mining process. Finally, the sensor can monitor the number of gases including oxygen, carbon dioxide and methane inside the mine. Still, the WSNs faced various challenges during deployment of sensor nodes in underground mining such as the hostile or untrusted environment for communication. The line-of-sight communication link is not possible due to twists and turns of underground tunnels. Also, high amount of relative humidity, attenuation due to structure and signal absorption are key issues for WSNs [44].

Monitoring of active volcanoes continuously is another area of interest for WSNs.

Volcanoes take place when mantle melts, floats to the surface of Earth through the crust and release gases called volcanoes erupt. In general, the volcanoes of Earth are unseen to the vision and come on the seafloor with spreading ridges. The researchers collect the data to analyze the behavior of active volcanoes with the help of sensor nodes. Presently, active volcanoes are analyzed using highly expensive sensor nodes with additional external power. The maintenance and repairing of sensor nodes require helicopter for assistance. WSNs can be very useful for monitoring such active volcanoes by deploying a large number of tiny, low-cost and self-organizing sensor nodes to cover a large area. The deployment of WSNs is very economical as compared to presently expensive equipment's [45].

1.2.2.4 Healthcare applications

WSNs are very beneficial for healthcare-oriented application and proves its effectiveness in monitoring the patients with epilepsy, heart problem, heart attack or stroke patients, elderly patients, autism patients, and Parkinsons diseases. Healthcare applications do not work as stand-alone systems, rather they are integrated with complex health and rescue systems [46]. While preventive health care has encouraged diminishing the health spending and mortality rate, but the researches illustrate that the patients feel uncomfortable, inconvenient, complicated and interfere with their personal daily life. For example, numerous checkup visits or therapy sessions get miss due to clash of agenda with established living and working habits, transportation cost and overexertion [47]. To overcome these problems, intelligible solutions are provided by involving the following tasks:

- Sensor nodes develop extensive systems that offer analyzed data about the diseases and the prevention appliance to the patients.
- Sensor networks are integrated with health infrastructure in emergency and rescue operations with transportation.

- Sensor networks can be worn by patients to overcome the presence of a nurse or medical personnel medical.

Sensor network gives alert to the doctors or nurses about the health of patients and necessity the doctors involvement in it. Different sensors are available that can sense various functional activities of the human body such as hemoglobin, heart rate, blood pressure, Electrocardiogram (ECG), Electromyogram (EMG), blood flow, respiration, and the oxygen level in the blood, etc. Another area of WSNs applications is to monitor the pipelines of gas, water, and oil. To manage the pipelines is a challenging issue. The long length structure, high price, high risk, and various challenging conditions prerequisite continue and unobtrusive monitoring of the pipelines. Leakage in pipelines can happen due to extreme deformations caused by collisions, land sliding, earthquakes, corrosion, wear and tear, material flaws and intentional damage of the pipelines. To overcome these problems, sensor nodes are deployed to detect such types of happening [48][49].

1.2.2.5 Commercial application

WSNs are also applicable to various commercial applications. The exhaustion of material can be analyzed and monitored by deploying sensor nodes which detect the structural damage of materials. Virtual keyboards, an inspection of the quality of product and management of inventory are a good example of commercial applications of WSNs. Automated machines, theft detection, smart robotics, automated factories, automated vehicles and vehicles tracking are also some applications of WSNs [50][51].

1.3 Aim and objective of the Thesis

The overall motive of the presented thesis "An Intelligent Algorithm for Energy Efficient and Secure Localization in Wireless Sensor Networks" is to accomplish three

objectives which are specified as follows:

1. *To develop an optimized DV-Hop algorithm for minimizing the localization error.*
   The localization error in Distance Vector-Hop (DV-Hop) algorithm is the main issue of concern. DV-hop has attracted more attention due to its simplicity, cost, and stability but estimates the position of unknown nodes with the help of few beacon nodes which provide more localization error. Hence, an energy-efficient optimized DV-Hop algorithm is required which gives more precise localization with least energy consumption.

2. *To develop an energy-efficient framework for localization algorithm on the Media Access Control layer.*
   Network lifetime is also a major research concern in WSNs localization. The operable batteries of sensor nodes have limited energy and these batteries must be replaced or recharged once it depleted. The network lifetime of WSNs can be prolonged by either maximizing the energy of nodes or minimizing the energy consumption in the network. Also, strict timing is required to avoid a collision which reduces overall energy consumption. Therefore, an energy-efficient range-free localization algorithm is required which prolongs the network lifetime at the Media Access Control (MAC) layer.

3. *To address the security concerns in the localization algorithm under the presence of adversary nodes.*
   Security of localization algorithms is the most crucial aspects of WSNs. Localization errors can be produced by malicious or non-malicious nodes which greatly affect the performance of the localization process in WSN. The attacks on localization can be executed internally or externally by the nodes in WSNs. In the case of internal attacks, malicious nodes in network provide wrong location information, whereas different forms of intrusions can be executed with the localization process by external nodes. Sensor nodes cannot perform accurate and precise localization if the location information is bisected (de-routing) by

malicious nodes. To address the security concerns in localization, trust-based range-free secure localization algorithm is developed with blockchain technology.

1.4 Researcher's Contribution

The main contributions in this area of research are demonstrated in Figure 1.9 and the summary of the same in brief is specified as the following:

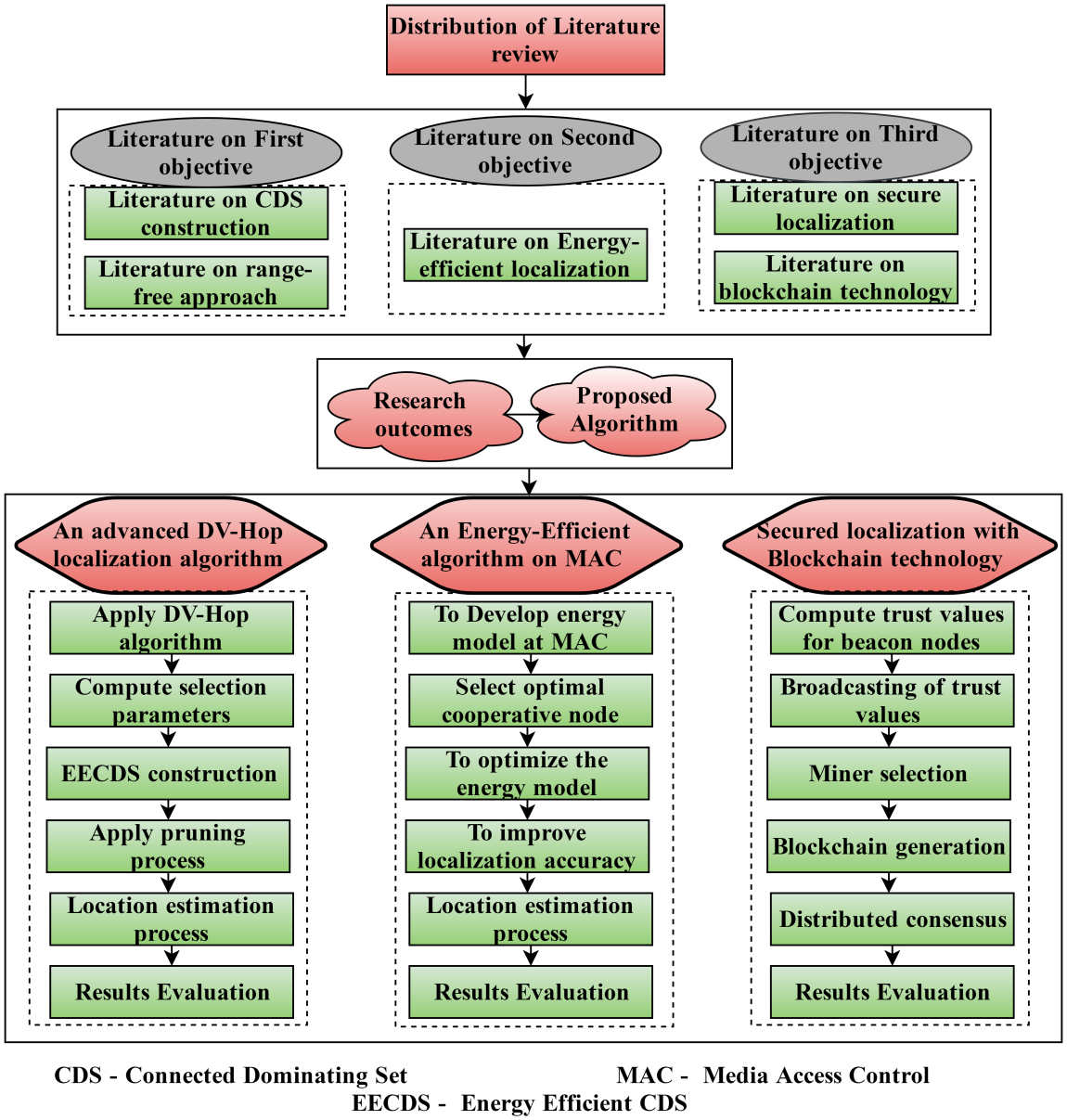

FIGURE 1.9: *Flowchart of the Research methodology.*

1.4.1 An Advanced DV-Hop based on Energy-Efficient Connected Dominating Set (EECDS)

The proposed algorithm employs the work [52] to construct EECDS which act as a backbone to the network. Initially, a virtual backbone is created by dominating set for energy-efficient localization. All the beacon nodes are selected on the basis of their residual energy and degree of connectivity with one-hop neighboured unknown nodes. The method proceeds until either the entire beacon nodes becomes an EECDS participant or the dominating set covers all the unknown nodes. After constructing EECDS, the pruning process is applied to accomplish MEECDS. Further, a correction factor is included to modify the hop-size of the beacon nodes. We also consider the concept of collinearity to reduce localization errors. Finally, the trilateration process is performed to achieve the positions of unknown nodes.

1.4.2 Energy Efficient localization algorithm at MAC

Network lifetime is a challenging concern which can be prolonged by integrating Cooperative MAC with localization algorithm. The communication among sensor nodes is achieved using cooperative communication. All the beacon nodes can broadcast the location information to unknown nodes either using direct communication or cooperative communication. A novel concept of cooperative communication in localization is introduced in place of direct communication. The positions of the beacon nodes is transferred to the base station with cooperative beacon nodes to improve network life. Co-operation is preferred using an efficient and effective system based on lower energy consumption. The accuracy of estimation is improved by incorporating a correction factor.

1.4.3 Secure Localization Algorithm

Security is a basic and crucial requisite for the localization process to improve accuracy and reliability. The lack of trust between nodes can be detrimental to the localization process. A number of attacks can be executed during localization by malicious nodes externally or internally. To address such issues, a novel trust-based secured localization algorithm has been developed. The trust values of each beacon node are evaluated considering various metrics such as reputation, mobility, residual energy, and one-hop neighbor nodes list. After trust value evaluation, the trust values are shared among beacon nodes using blockchain technology. The highly trustworthy beacon nodes are elected as a miner for mining of blocks so that unknown nodes select highly trusty beacon nodes to perform localization process.

CHAPTER 2

Localization in Wireless Sensor Networks

2.1 Localization

Sensor networks are closely connected with the surrounding physical activities in the environment. These nodes observe the happening events of surroundings and the collected information is generally important for sensor nodes. The data provided by sensor nodes is pointless if the place of the happening event is not recognized . WSNs are ad-hoc sensor networks and the locations of nodes may be not understood before the deployment. Localization is a process to assign the geographic position to each sensor nodes. For example, the sensing devices are organized in a forest to detect fire and raise alarms during an event. Whenever wildfires occur, these devices sense the fire and collect the data and forward information to end-users. If the locations of those particular sensor nodes give information about the fire, that are not known, further action cannot be taken by the control room. Therefore, accurate locations information of nodes is essential in various tasks such as habitat monitoring, battlefield,

surveillance, object tracking location-aware services and environmental information based routing.The physical position of sensing devices for further processing is the main concern for most WSN applications. Localization is a way to determine the position or fitness of sensor node locations.

In WSNs, there are various challenges faced during localization processes and various positioning technologies that have been investigated to resolve the issue of inadequate localization. There are several applications in WSNs that require accurate locations of nodes, otherwise it is irrelevant to have any sensory data (fire detection, location monitoring, recovery activities, etc.). The location of sensor clusters therefore performs an important role in WSNs and the knowledge about sensor nodes locations is always useful to process the new services and applications. Moreover, the accessibility of sensor nodes locations may facilitate myriad of applications such as road traffic controlling, health-care applications, intrusion detection, surveillance and inventory management [27]. Furthermore, different network facilities, location-oriented routing and information aggregation can be utilized excellently if sensor nodes have precise locations.

The concept of localization is essential when there is uncertainty about position of nodes. To compute the locations of these sensor nodes, effective localization algorithms are required [28]. When the collected information of sensor nodes is associated with the spatial information, the importance of information and proficiency of the process gathered increases substantially. For example, some sensor nodes are deployed for monitoring temperature of some particular regions. After collecting temperature reading without location information, the information is only useful to compute statistics such as mean, mode, and standard deviation. But, the collected information can be analyzed much more efficiently or meaningfully with location of nodes for different processes. Location information opens up a new paradigm to various application possibilities: an intelligent heat transfer model can be utilized to filter out noise and pinpoint the locations of heat sources.

The development from centralized wired applications to distributed wireless applications have a large amount of cost. These applications still have various challenges

during implementation such as complexity, protocols, and nature of the sensor nodes. In addition, much more details are required for distributing a large number of independent parts with new software version and highly energy devices. But, localization can make this effort to worthwhile and its ability to collect a large amount of data that could never be collected without sensor nodes. The significance of localization arises from various aspects and many of which are associated only with WSNs. These aspects comprise the identification and correlation of collected information, sensor nodes addressing, management in network and sensor nodes query in a specified area, coverage, object-tracking, geographic routing, nodes density and other properties of algorithms. All of these aspects make localization of sensor nodes a crucial technology for the growth and operation of WSNs. The process to discover the locations of sensor nodes can be divided into three steps (1) distance/angle estimation (2) position computation, and (3) localization algorithms. The main steps of the localization process are depicted in Figure 2.1.

1. *Distance/angle estimation:*

   In this phase, the distances between sensor nodes are discovered from each other. Distance estimation can be achieved by using received signal strength, angel information or hop count information. Further, the estimated distances are utilized for position computation of sensor nodes.

2. *Position computation:*

   In this phase, the position of sensor nodes are computed on the basis of available information received from neighbors nodes. Sensor nodes compute their coordinates in this phase of localization.

3. *Localization Approach:*

   Localization Approach: This phase plays a vital role in the localization process. It will decide how the information about sensor nodes is discovered and how that information is utilized for location computation.

All three components have their own importance and each component has its own method and solution for localization. The performance of the localization process

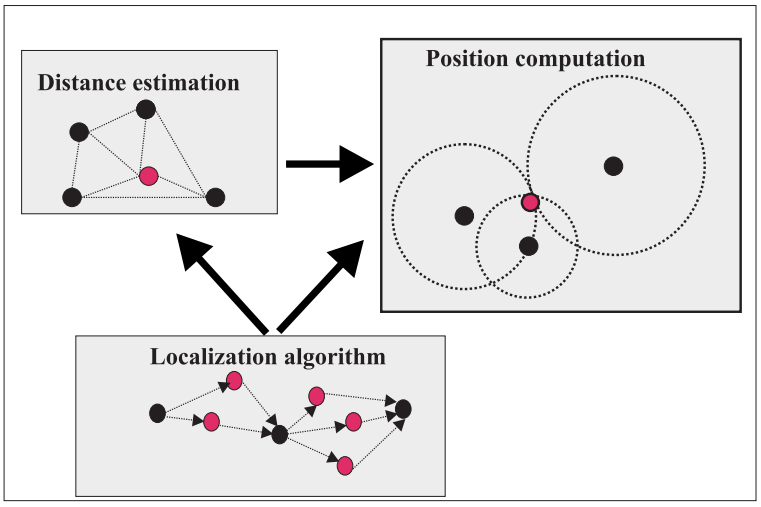

FIGURE 2.1: *Division of localization process.*

directly depends on each of these phases.

2.2 Key Aspects of Localization Algorithms

In this section, the crucial key aspects of the localization are discussed that must be considered during designing and selecting a localization approach. The key aspects affect the performance of the localization schemes significantly. These key aspects are discussed as follows:

2.2.1 Limited resources

The sensor node is generally composed of four parts: sensor, handling unit, transceiver (transmission and reception) and energy (batteries) to accomplish the task. Advancement in technology requires small size of existing sensing devices with low-cost and also have tiny space and computing skills. There are also restricted sensor node operating batteries, which must be substituted or re-charged once they have been exhausted [53]. But some sensor nodes that are deployed in unattended or remote areas, both options are not applicable. The sensor nodes are simply discarded from the networks once their battery depleted. Sensor nodes must function until its challenge

duration has either done or the battery can be altered for non-rechargeable batteries. The duration of the battery supply relies on the particular type of application [41]. For example, the sensor nodes in scientists monitoring can be work for several years while in a battlefield scenarios sensor nodes may only be required for a few hours or days. Therefore, localization scheme must consider all these constrained of the sensor nodes for good localization results [54].

2.2.2 Number and density of nodes

The performance of localization approaches is mostly affected by the density of sensor nodes. On one hand, some localization algorithms cannot work properly in low-density networks because of the performance depend on the distance measurement or hop count between nodes [55]. A low density of sensor nodes produces considerable localization error that affects the performance of the algorithms. On the other hand, for some algorithms, high density of nodes makes the localization process very costly. Furthermore, the high density of nodes gives more accurate localization with the high cost and more delay. It is a crucial concept to decide the number of nodes in the operation during a localization algorithm selection [56].

2.2.3 Network topology adaptability

Some methods to positioning to compute Euclidean distances among nodes by taking into account the smallest distance between sensor nodes. However, the concept works well the shortest path is identical to a straight line [57]. But, the WSNs are ad-hoc in nature, where the deployments of nodes are achieved randomly. For example, aircraft in the required regions could deploy sensor nodes in war or disaster areas. In random network scenarios, it is not possible to get the shortest path as a straight line which affects the results of localization [58].

2.2.4 Obstacles and irregularities

The Obstacles and irregularities in networks affects the performance of the localization algorithms. It may happen due to the presence of obstacles, which obstruct the line of sight between sensor nodes. Due to the presence of obstacles sensor nodes may not be able to send or receive the signal s properly from neighbor nodes causes localization unfeasible. The obstacles can cause signal reflections which give wrong distance estimations [59]. This type of problems occurs either in outdoor or indoor environments. Hence, the localization approaches must be able to manage all these situations for better performance [60].

2.2.5 Dynamics scenarios

An important assumption of various localization approaches is that the sufficient number of reference nodes should be available for the location estimation process. Generally, there must be a constraint path between unknown nodes to appropriate beacon nodes for localization of node [61]. This means that network should be sufficiently connected to perform localization of nodes. However, a large number of applications exist, where the sensor nodes are dynamic and connectivity of the network is random. In such types of networks, the sensor nodes may not be able to connect with neighbor nodes [21]. The dynamic nature of networks may become unacceptable for various sensor nodes. Therefore, sensor nodes must be able to operate in dynamic networks with accurate results [62].

2.2.6 Security

Security in localization is another area of concern in WSNs. To preserve the privacy and confidentiality of location information is an important issue in localization. In localization, errors can be produced by malicious or non-malicious nodes which greatly affect the performance of the localization process in untrusted environments

[63]. The attacks in localization can be executed internally or externally by the nodes in WSNs. Malicious nodes in the network provide wrong location information and different forms of intrusions can be executed with the localization process by external nodes. Sensor nodes cannot perform accurate and precise localization if the information of location is collected by malicious nodes [64]. Localization security has gained more attention from researchers with the rapid development of sensor localization technologies in WSNs. Therefore, the localization approach must be able to avoid or prevent such types of attacks. Security in localization is a basic and crucial requisite of nodes to improve the accuracy and reliability. The malicious sensor nodes cannot trust to other sensor nodes to perform the location estimation process in WSNs. The lack of trust between nodes can be detrimental to the localization process [65].

2.3 Classification of Localization

In WSNs, the positions of sensor nodes can be stated as a universal metric or relative metric. The universal metric represents the location of nodes within a general global reference frame. For example, the locations provided by the Global Positioning System (GPS) and the Universal Transverse Mercator (UTM) come under global metrics. In contrast, relative metrics depend on coordinates systems and reference frames. For example, the positions of sensor nodes are expressed in distances with respect to other nodes without association with global coordinates. Accuracy and precision are crucial factors for the localization process. Practically, it may be not possible for all sensor nodes to acquire global coordinates in WSNs because of resources constrained. Many sensor nodes in the networks compute their positions using a subset of nodes with global coordinates. The sensors nodes with prior known locations are called beacon nodes. The sensor nodes without knowledge of location information are called unknown nodes and their location is determined by using beacon nodes. Location of sensor nodes is determined by using distance and angle between nodes. There are various techniques employed in the localization of sensor nodes depicted in Figure 2.2. Basically, localization approaches are classified into two categories (1)

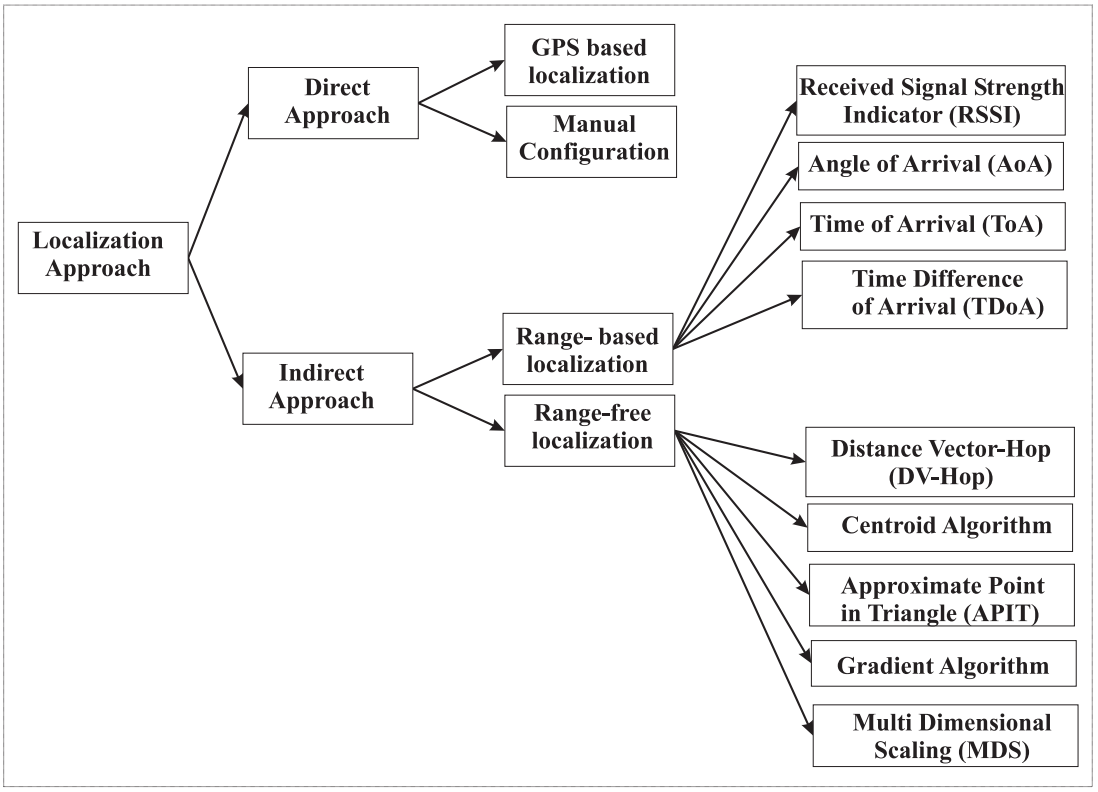

FIGURE 2.2: *Different types of localization techniques.*

Direct approach (2) Indirect approach. Further, direct approaches are categorized into manual configuration and GPS based localization. Indirect approaches are also categorized into range-based and range-free localization.

2.3.1 Direct approach

The manual configuration localization technique is most expensive and cumbersome and sensor nodes can not be manually deployed in remote areas which make it inaccessible for large WSNs and also not acceptable for mobile WSNs. In GPS based localization technique, every sensor node has installed GPS receiver in WSNs. This method is suitable for WSNs with the mobility of nodes. The location of the sensor is estimated with the help of GPS satellites. For finding the location with GPS, at least 4 GPS satellites must be in the line of sight with earth GPS receiver at any instant of time depicted in Figure 2.3. Each GPS satellites broadcast information about its coordinates and current time to earth GPS receiver. The information is

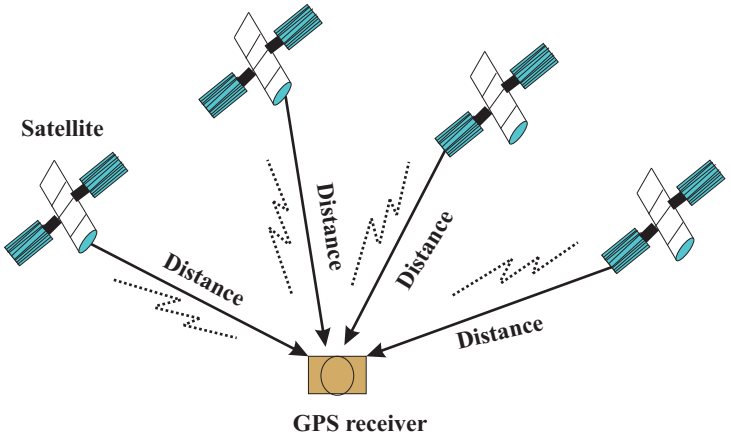

FIGURE 2.3: *Working principle of GPS.*

broadcasted with the speed of light and the distances between satellite transmitters to GPS receiver is computed by finding the time taken from transmitters to receiver. The GPS receiver computes its location by performing trilateration and at least 3 satellite transmitters require for 2-D localization [66]. These techniques improve the precision of location and provide less localization error. However, the costs of such localization methods are very high. It is very expensive and economically unrealistic for WSNs to equip each sensor node with GPS [67]. Also, the GPS system based localization methods are not energy efficient and require additional hardware [68].

2.3.2 Indirect approach

The indirect localization approaches are also called relative localization because the positions of nodes are related to other nodes in their locality. Indirect localization approaches were developed to overcome the drawbacks of the GPS based localization approach by reducing the computational cost of the localization process. In indirect approaches, GPS receivers are installed with some sensor nodes to compute their location called beacon nodes. With the help of beacon nodes, the location of remaining nodes called unknown nodes can be computed. Indirect approaches are explained as follows:

2.3.2.1 Range-based localization approach

In range-based approaches, the locations of unknown nodes are computed with respect to other nodes in its locality. Range-based methods are based on assumptions that one or more characteristics of the communication signals from sender to recipient can evaluate the complete range between sender and recipient. These techniques usually require complex hardware for the localization process which is not feasible because of high resource-constrained WSNs. Received Signal Strength Indication (RSSI), Time Difference of Arrival (TDoA), Angle of Arrival (AoA) and Time of Arrival (ToA) are important techniques of range-based localization.

- **Received Signal Strength Indication:**

In this type of technique, the distance between the sender and the recipient node is determined by evaluating the signal strength at the recipient [69]. RSSI is the measurement of the power of the received signal as shown in Figure 2.4. The size of signal attenuation is related to RSSI value and smaller value of RSSI represents the less attenuation. Generally, the RSSI measurement depends on the experience model. The communication frequency and transmit power are known by the transmitter. Therefore, strength of received power can be measured with the help of the above mentioned parameters. The loss due to propagation is also considered that is transformed into distance estimation [70]. Power of signal strength affect distance among transmitter and receiver in opposite way i.e. decreases and increases simultaneously and the RSSI is measured by the following equation:

$$P_r(d) = \frac{(P_t \times G_t \times G_r \times \lambda^2)}{4\pi^2 \times d^2} \tag{2.1}$$

where G_t represents the transmitting antenna and G_r represents the gain of receiving antenna, λ represents wavelength of the transmitted signal in meter. The signal strength of receiving nodes is computed as follows:

$$RSSI = P_t - P_L(d) \tag{2.2}$$

where P_t is the transmitted power and $P_L(d)$ represents the path loss at distance $'d'$ and both are measured in dBm.

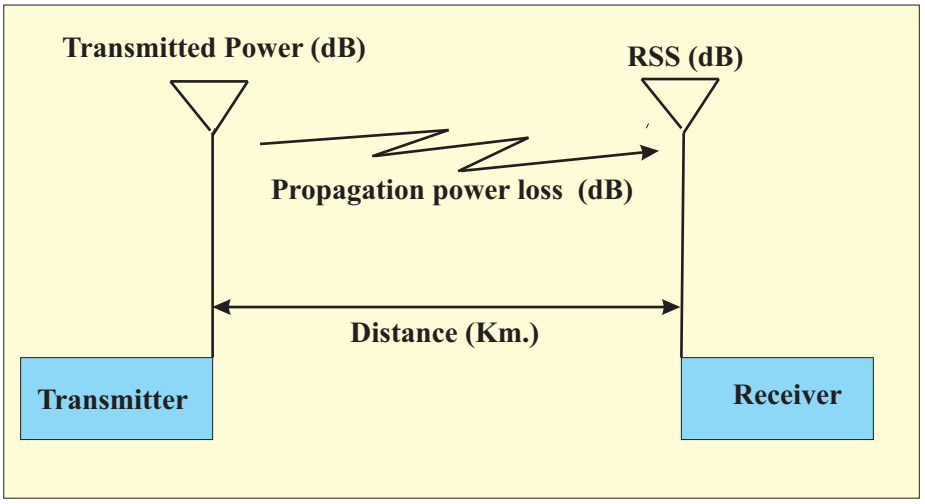

FIGURE 2.4: *Received Signal Strength Indication model.*

- **Angle of Arrival**

The location of an unknown node is calculated by two signal angles and AoA concept as shown in Figure 2.5. These angles are collected from the unknown nodes and the technique of triangulation is used by unknown nodes to predict their location. The direction of signal propagation is determined by using an array of microphones and antennas. In AoA localization, an array of antennas are used to compute the direction of arrival and at least two receivers required for localization [71]. The AoA localization consists of the angular separation between two beacons and a fixed axis. With the help of angle of arrival at a number of sensor nodes, angulations between nodes are used to locate unknown nodes. The AoA represents the angle between some reference direction known as orientation and propagation direction. Orientation indicates the way by which the signal angles are evaluated and the clockwise route from north is analyzed in degrees. The orientation with 0 value represents absolute AoA, otherwise it is relative.

In AoA scheme, the sensor nodes forward their bearings with respect to beacon nodes. In this scheme, strong cooperation requires between sensor nodes and they are able to tackle localization error. At least two non-collinear beacon nodes are required to

compute the location on unknown nodes when orientation is known in advance but, at least three beacon nodes required for locations as well as orientations. AoA is also affected by noise and additional problems. The locations cannot be computed if the unknown nodes cannot hear from enough beacon nodes. Also, AOA measurement requires heavily sized hardware for operation that adds up in the cost of system [72].

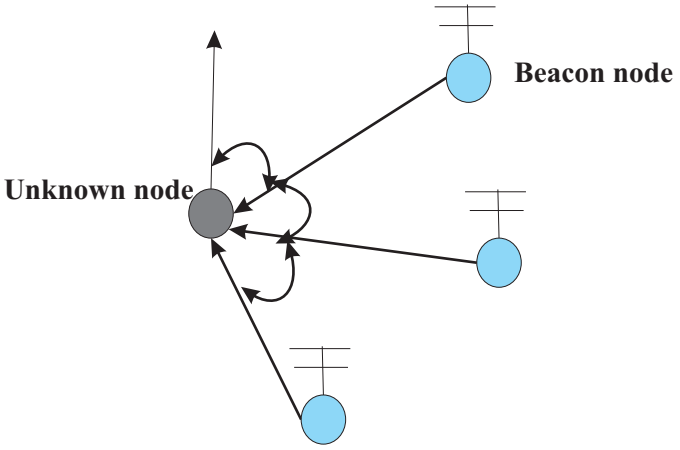

FIGURE 2.5: *Angel of Arrival localization scheme.*

- **Time of Arrival**

This method is also called time of flight. In this approach, time taken between beacon nodes radio signals and speed of traveling signal between beacon nodes to unknown nodes is measured. Further, the distances between nodes are computed to discover the position of unknown nodes [73]. Beacon nodes use GPS for high accuracy but it requires a high processing capability. Generally, ToA is classified into two types shown in Figure 2.6. One-way measurements of ToA is represented in Figure 2.6(a). The distance between two nodes is calculated using the following equation:

$$Distance_{ij} = (t_2 - t_1) \times v \tag{2.3}$$

where t_2 and t_1 are the sending and receiving times of the signal respectively and v is the velocity of the signal. Similarly, Figure 2.6(b) represents the two-way approach

and the distance is computed as follows:

$$Distance_{ij} = \frac{\{(t_4 - t_1) - (t_3 - t_2)\}}{2 \times v} \tag{2.4}$$

where t_3 and t_4 represent the sending and receiving time of the response signal respectively. The computed time of the arrival is then multiplied with speed of the signals. In one-way localization, the position of the receiver node is computed by itself. But, the location of the receiver is computed by the transmitter in the two-way approach [74]. The transmitter node and receiver node must be accurately synchronized to measure the TOA information in one-way propagation. But, synchronization is not required in case of two-way TOA.

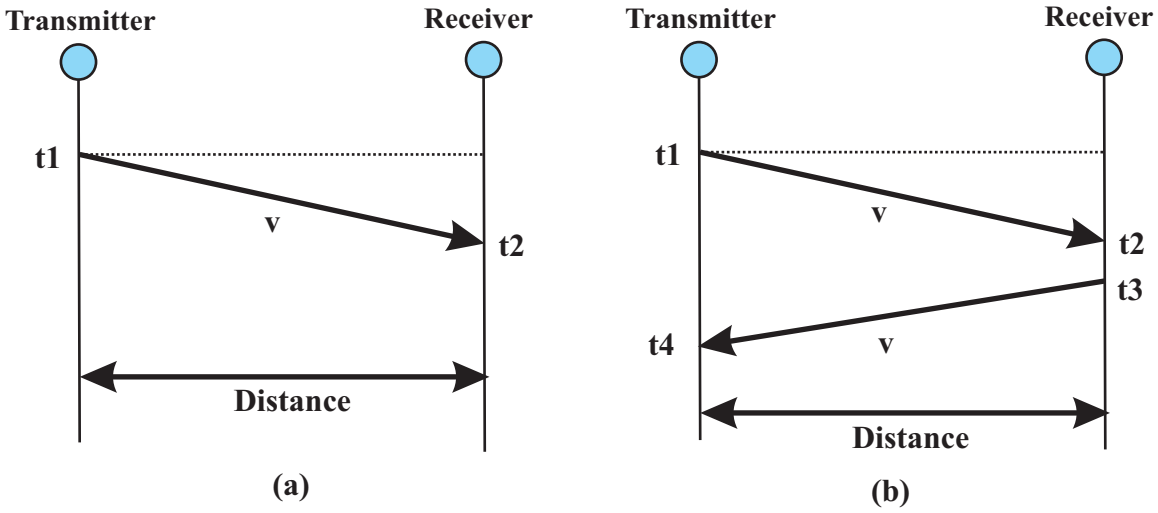

FIGURE 2.6: *(a) One-way ToA approach and,(b) Two-way ToA approach.*

- **Time Difference of Arrival**

In TDoA approach, the distances between sensor nodes are computed by emphasizing the difference of arrival times at receiver from transmitter sensor nodes shown in Figure 2.7. The received information is used by unknown nodes to calculate the distance between beacon nodes and itself [75]. For example, two signals such as radio signal and ultrasound sound signal with different velocities v_1 and v_2 are broadcasted from transmitter after t_{delay}. The difference between times of sending t_{delay} of both

signals is computed as follows:

$$t_{delay} = t_1 - t_3 \tag{2.5}$$

The broadcasted signals are received by the receiver node at time t_2 and t_4. Now, the node computes the distance as follows:

$$Distance = (v_1 - v_2) \times (t_4 - t_2 - t_{delay}) \tag{2.6}$$

In TDoA approach, time synchronization is not required between the transmitter and receiver node. Accurate and precise localization can be achieved without clock synchronization. But, the main drawback of approach is the requisite of special hardware for operation, for example, a speaker and microphone for the above example. These types of approaches do not require the synchronization clocks between sender and receiver and can give good accuracy in measurements. But its main drawbacks is that it requires additional hardware for operation like microphone and loudspeaker.

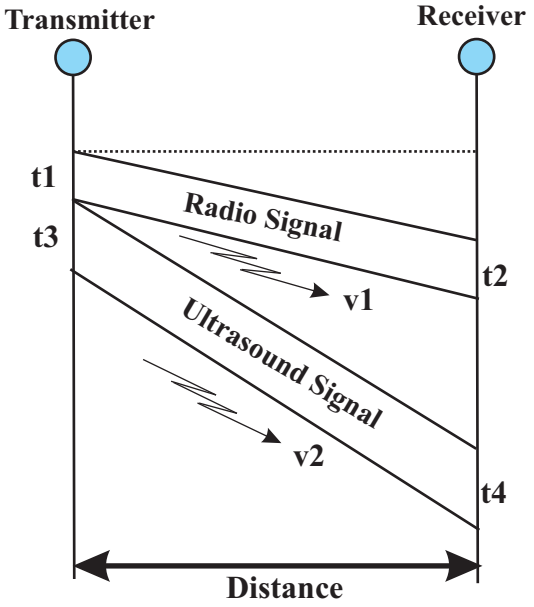

FIGURE 2.7: *TDoA localization approach.*

2.3.2.2 Range-free localization approach

Range-free localization approach does not require a point to point information and distance information for computing the locations of unknown nodes. These approaches require low-cost hardware to perform localization. The localization process is accomplished with the help of connectivity and hop count information. Approximate Point in Triangle (APIT), Centroid algorithm, Gradient algorithm, Multi-Dimensional Scaling (MDS) and Distance Vector-Hop (DV-Hop) are the example of range-free localization approaches. The descriptions of range-free approaches are as following:

- **Approximate Point in Triangle**

The APIT localization approach works based on area information for estimating the position of nodes. APIT approach depends on multiple beacon nodes to perform localization. At least three beacon nodes must be required for localization. Combination of three beacon nodes makes a triangle and an unknown node exist within or outside that triangle allows a node to discover its locations. In the triangular region, the possible area is narrow down depending on whether a node lies outside or inside the triangle. Repetition of the same procedure with a different possible combination of nodes can give more accurate localization in WSNs. The process of APIT is depicted in Figure 2.8. $B1, B2, B3, B4, B5$, and $B6$ are the beacon nodes and U represents the unknown nodes. When U has received location information from various beacon nodes, it assesses all possible triangle formed by beacon nodes. The unknown node discovers its presence inside or outside a triangle by applying Point in Triangulation (PIT) test. An unknown node U is considered outside the triangle formed by beacon nodes $B1, B2$ and $B3$, if there exists a direction such that a point adjacent to U either closer or further from all beacon nodes of triangle simultaneously. Otherwise unknown node U is considered inside the triangle and that particular triangle can be used for localization. APIT localization approach can be applied to such networks where node density is sufficient to perform localization in WSNs.

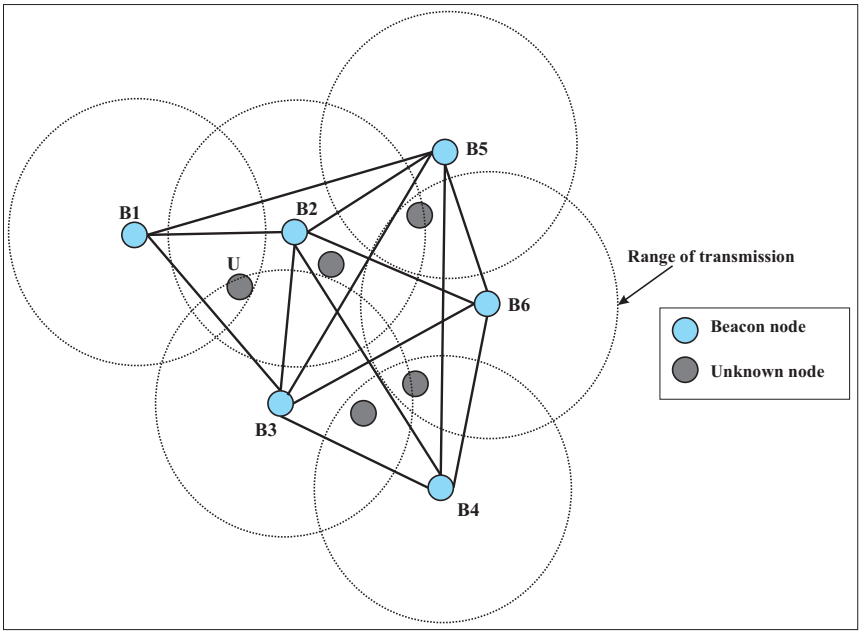

FIGURE 2.8: *APIT localization process.*

- Centroid Algorithm

Centroid approach is another popular approach of range-free localization and its process is explained in Figure 2.9. Generally, the basic idea for localization is that a set of beacon nodes are deployed with their coordinates (x_i, y_i). These beacon nodes continuously broadcast their location information in their neighborhood unknown nodes. The unknown nodes can compute their own position with the help of received information from beacon nodes. The positions of unknown nodes are evaluated as follows:

$$(x, y) = \left(\frac{\sum_{i=1}^{n} x_i}{n}, \frac{\sum_{i=1}^{n} y_i}{n} \right) \tag{2.7}$$

where (x, y) represents the coordinates of the unknown nodes and n is the total number of beacon nodes. Centroid algorithm has performs better against uncertainties of propagation, because the localization process depends only on beacon location information. Still, the number of nodes and deployment affects the performance of the centroid algorithm. Hence, the deployment of beacon nodes in an efficient way is very crucial.

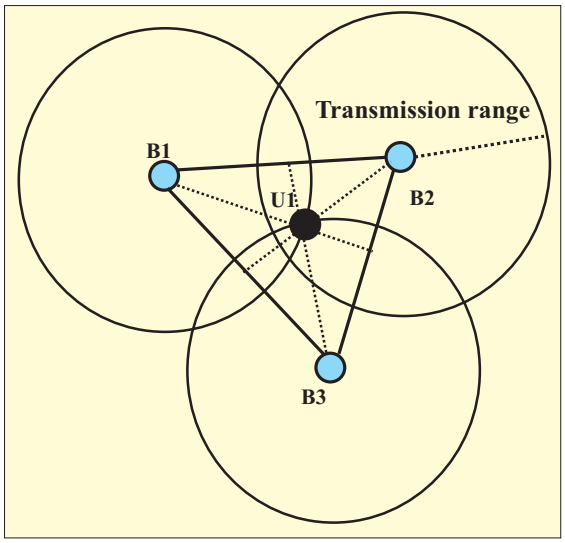

FIGURE 2.9: *Centroid localization in WSNs.*

- DV-hop localization algorithm

The basic DV-Hop localization algorithm has been investigated using the distance vector routing protocol [76]. Firstly, the beacon nodes broadcast its location information to unknown nodes across the networks. Further, the distances between unknown nodes and beacon nodes are computed by multiplying hop size and number of hop counts among nodes. Finally, the positions of unknown nodes are computed by applying the trilateration localization scheme. The positions of unknown nodes are computed in three steps in the DV-Hop algorithm depicted in Figure 2.10. In the first step, beacon nodes forward its location information $[ID_i, h_i, (x_i, y_i)]$ to unknown nodes across the network, where ID_i shows identification of beacon nodes, h_i define hop-count whose initial value is zero and (x_i, y_i) is the coordinates of the beacon nodes. In second stage, the hop-size distance of beacon nodes is computed as following Equation:

$$hops_i = \frac{\sum_{i \neq j} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{i \neq j} h_{ij}} \tag{2.8}$$

where (x_i, y_i) and (x_j, y_j) represents the coordinates of beacon node i and beacon node j respectively, h_{ij} defines the hop-count between node i and j. Every beacon node transmits the information to the network by using flooding after calculating hop-size. Even though numerous beacon nodes are present in the network, the unknown node

first receive data from the beacon node and then forward it to other neighboring nodes. The distances among beacon nodes and unknown nodes are computed as follows:

$$d_{it} = hops_i \times h_{it} \tag{2.9}$$

where d_{it} represents the expected or estimated distance between unknown node t and beacon node i, $hops_i$ is the hop-size distance of beacon nodes received by an unknown node from adjacent beacon node and h_{it} refers hop-count between beacon node and unknown nodes. At last with the help of trilateration method the position of all

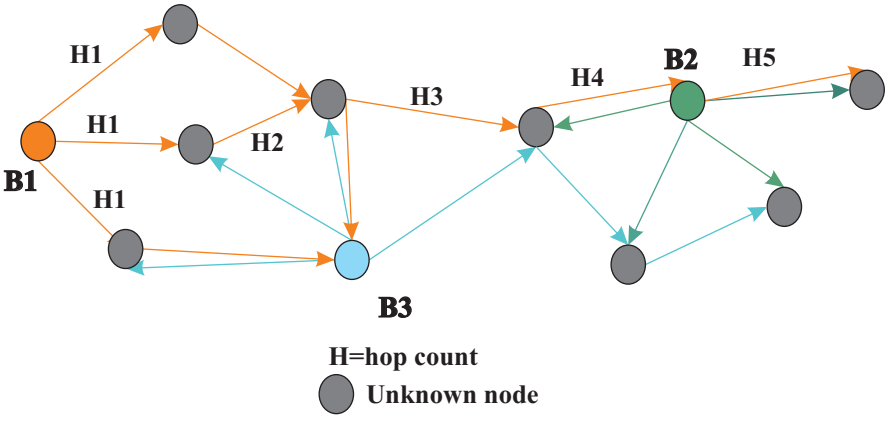

FIGURE 2.10: *DV-Hop localization algorithm.*

unknown nodes is calculated. In the traditional DV-Hop algorithm, the localization error is accumulated due to hop-count value and hop size distance. The working of DV-Hop can be understood with an example shown in Figure 2.11 and three beacon nodes are deployed with some unknown nodes. All beacon nodes compute their hop size distance using following equation:

$$A_1 \text{ or } hops_1 = ((50 + 45))/(3 + 4) = 13.57$$
$$A_2 \text{ or } hops_2 = ((50 + 37))/(4 + 3) = 12.43$$
$$A_3 \text{ or } hops_3 = ((37 + 45))/(3 + 3) = 13.67$$

After computing the hop size distance, each beacon node broadcast the information to all neighbor nodes. After receiving the hop size distance, unknown node U can compute approximated distances from all three beacon nodes as follows:

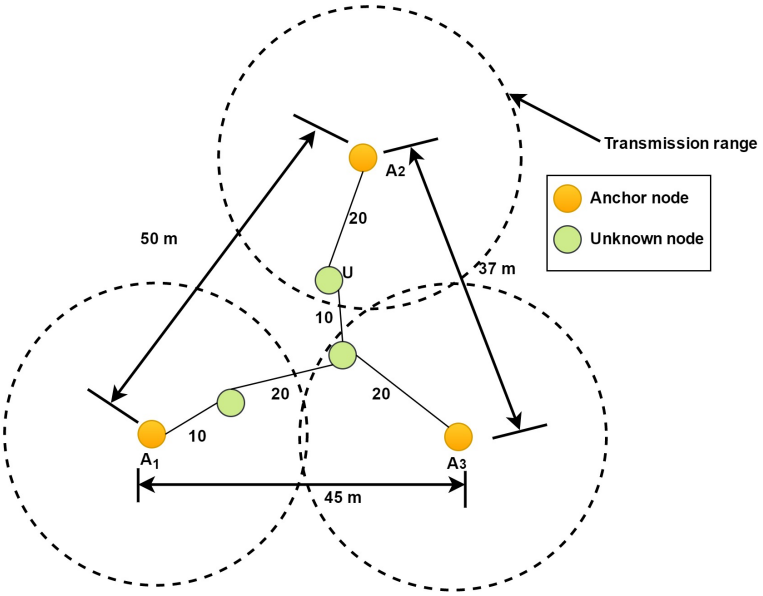

FIGURE 2.11: *An example of DV-Hop.*

$$d_{U1} = 13.57 \times 3 = 40.56$$
$$d_{U2} = 12.43 \times 1 = 12.43$$
$$d_{U3} = 13.67 \times 2 = 27.34$$

After getting the distances between nodes, the position of unknown nodes is computed by using trilateration method and least square method.

- **Multi-Dimensional Scaling**

MDS localization is a set of data analysis method that describes the organization of distance data as a geometrical representation. MDS approach can be used for centralized localization, where a central device collects the information from all nodes. The central device is more powerful as compared to all other nodes. In MDS, the distance matrix is generated by computing the distances between nodes. The MDS approach gives accurate localization if the correct distance matrix is provided. The distance matrix is established using Dijkstras or Floyd's algorithms for discovering the shortest path between nodes. The requirement of global location information and centralized management are the main shortcomings of the MDS approach.

- Gradient localization algorithm

In the gradient localization approach, the beacon nodes create a gradient that self-propagates across the network [77]. The gradient permits an unknown node to infer its distance from beacon nodes. After estimating the distances from at least three beacon odes, the unknown node compute its own location using trilateration or multilateration. The basics steps of the gradient localization approach are:

1. Each beacon nodes broadcast its location information into a packet across the network with a counter set to zero.

2. Each unknown node preserves the shortest path from all beacon nodes in the network from which it has received the location information. The estimated distance ($d_{iu)}$ between beacon nodes and unknown nodes are computed as follows:

$$d_{iu} = h_{iu} \times D_{hop} \tag{2.10}$$

   where D_{hop} represents the Euclidian distance of one hop and it is computed by the Kleinrock-Silvester method [78].

3. Finally, the coordinates of unknown nodes are computed with trilateration.

2.4 Computation

The discussion of the aforementioned localization algorithms illustrates that the positions of unknown nodes are computed by using computation methods at the last step. The computation process is performed either by unknown node or beacon nodes. Different types of computational methods are discussed as follows:

2.4.1 Trilateration computation

Trilateration is the process of computing coordinates of unknown node based on the measured distance between itself and neighbor beacon nodes. In the two-dimensional field, the measured distances between three non-collinear beacon nodes are required to perform accurate localization in WSNs. Trilateration method is the refined version of triangulation, but distance measurements are required to perform the process instead of angles measurements as shown in Figure 2.12. Generally, the information from a single beacon node gives an idea about the location of unknown node in a large circular area. Location information from another beacon node permits the unknown node to constrict the specific location in a region where two areas of beacon nodes overlap. Information coming from third beacon node gives an exact location of unknown node in a specified area. Information about more than three beacon nodes gives more precise location of unknown node. Let (x_t, y_t) is the coordinate

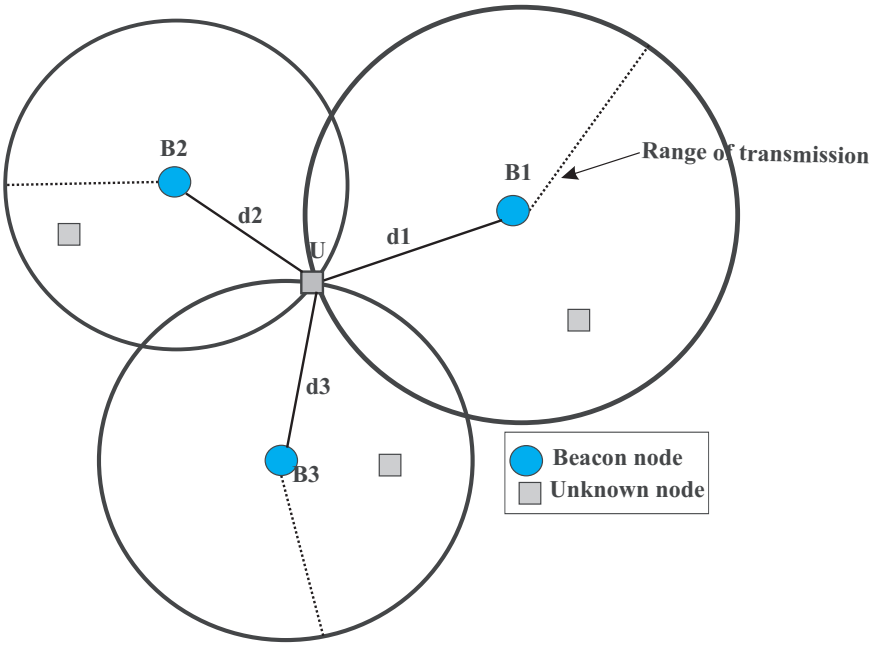

FIGURE 2.12: *Trilateration process.*

of the unknown nodes t and (x_i, y_i) refers to the coordinates of i^{th} beacon node where $[i = 1, 2, .., k]$ and d_{uk} is the distance from unknown node t to the beacon point i. The example of trilateration is considered for two-dimensional networks, but the same

matrix can be utilized for three-dimensional networks by increasing matrix elements. After arrangement and subtracting last equation from all previous one equation in the matrix, the equation becomes as follows:

$$\begin{cases} (x_t - x_1)^2 + (y_t - y_1)^2 = d_{t1}^2 \\ (x_t - x_2)^2 + (y_t - y_2)^2 = d_{t2}^2 \\ ... \\ (x_t - x_i)^2 + (y_t - y_i)^2 = d_{ti}^2 \end{cases} \tag{2.11}$$

The coordinates of t are calculated by using the formula:

$$A = -2 \times \begin{pmatrix} x_1 - x_i & y_1 - y_i \\ x_2 - x_i & y_2 - y_i \\ . & \\ . & \\ x_{i-1} - x_i & y_{i-1} - y_i \end{pmatrix} \tag{2.12}$$

$$B = \begin{pmatrix} d_{t1}^2 - d_{ti}^2 + x_1^2 + x_i^2 - y_1^2 + y_i^2 \\ d_{t2}^2 - d_{ti}^2 + x_2^2 + x_i^2 - y_2^2 + y_i^2 \\ .... \\ .... \\ d_{t(i-1)}^2 - d_{ti}^2 + x_{(i-1)}^2 + x_i^2 - y_{(i-1)}^2 + y_i^2 \end{pmatrix} \tag{2.13}$$

$$P_u = \begin{pmatrix} x_t \\ y_t \end{pmatrix} \tag{2.14}$$

At last, the position of the unknown nodes is obtained by applying least square method shown in equation 2.15.

$$P_t = (A^T A)^{-1} A^T B \tag{2.15}$$

2.4.2 Multilateration localization process

Trilateration localization approach depends on the presence of at least three non-collinear beacon nodes for computing the position of unknown node. The concept of trilateration approach is not suitable for such situations where three neighbor nodes with known locations are not available. For such cases, trilateration approach can be further extended for localization called multilateration. In multilateration, once unknown nodes discover its position using location information from neighbor nodes, it becomes a beacon node and broadcast its location to remaining unknown nodes in the networks. The process is repeated until all the unknown nodes have discovered their locations. The working of multilateration technique is explained with an example displayed in Figure 2.13. In this figure, all blue color nodes are beacon nodes whose locations are predetermined through either GPS or manually. At the first iteration, the red color node U is an unknown node and its location is estimated with the help of three beacon node $B1, B2$, and $B3$. After discovering the location, the red color node becomes reference nodes and helps other unknown nodes for estimating their positions. The position of unknown node $U1$ is discovered with the help of $B1, B4$, and U.

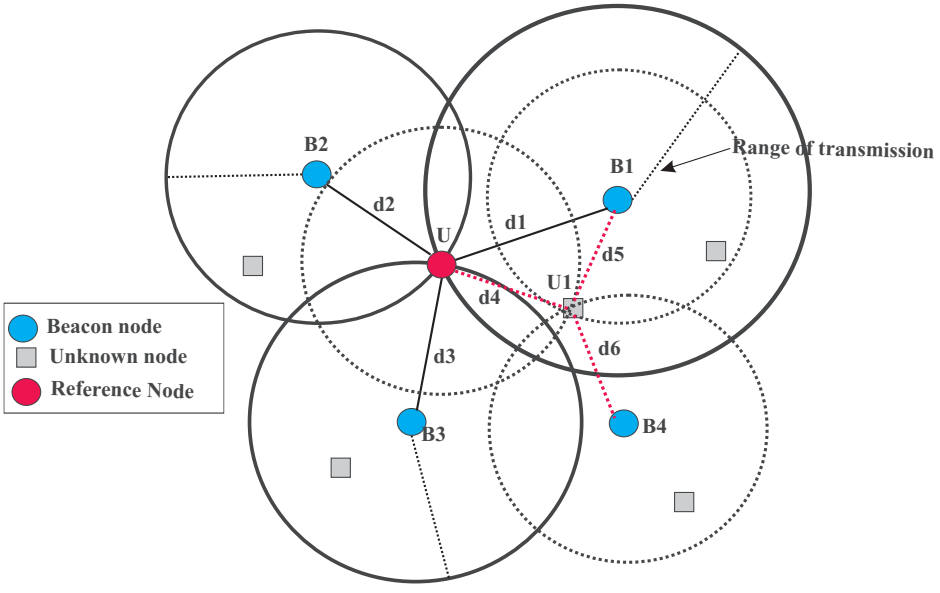

FIGURE 2.13: *Concept of multilateration.*

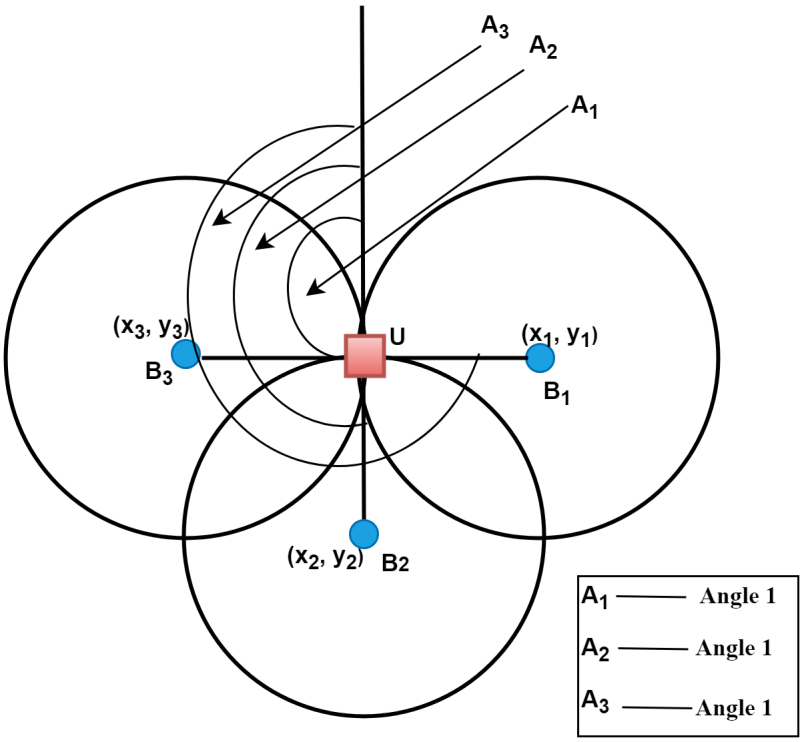

FIGURE 2.14: *Triangulation localization.*

2.4.3 Triangulation

The positions of unknown nodes are discovered with the help of trigonometry proposition or angular information in the triangulation localization process. If the two sides of the triangle are predetermined, the third unknown side can be computed using trigonometry property. Generally, the triangulation process depends on the angle information collected from different nodes in the networks. For determining the position of unknown nodes in two-dimensional WSNs, at least the locations of two beacon nodes and distances between them are necessary. The basic concept of triangulation is depicted in Figure 2.14 and it consists of three beacon nodes ($B1, B2$, and $B3$) with their position [$(x1, y1), (x2, y2)$, and $(x3, y3)$] and angles [$A1, A2$, and $A3$] relative to fixed baseline represented by vertical line in the figure. Assume that $(x_u, y_u)^T$ are the positions of unknown nodes, $(x_i, y_i)^T$ and the angle measurements from N beacon nodes are represented by $\beta = (\beta_1, \beta_2, ..., \beta_N)^T$. The measured angles do not provide actual angles due to atmospheric noise [79].

CHAPTER 3

Literature Survey

3.1 Introduction

As a result of advancement in Micro-ElectroMechanical Systems (MEMSs) and wireless technology, small, low-cost sensor nodes have emerged. Since the 1990s, due to its increasing demand, WSNs has attracted more attention to sectors and scholars. According to ONWORLD, the market for WSN devices and services is going to expand around 46 billion US dollars, which implies that the development is 500 million US dollars higher than the current industry level [80]. WSNs are the collection of a large number of sensor nodes used in the specified region to observe physical activities such as light, humidity, pressure, temperature, speed, and sound, etc. These nodes are used to determine the actual world environment's physical activity or behaviors and are dispersed in a broad region. After a specific event is detected, the sensed data is transmitted via a wireless connection to the base station. A set of sensor nodes is randomly implemented, forming a network called WSNs. Each sensor node has perception, communication and processing capabilities [81]. The sensor nodes have restricted resources such as executive power, low computational capacity, storage

memory and lifetime due to its small size and price. Due to resource constraints, the design and operation of nodes in WSNs have certain limitations. For example, sensor nodes should be small, long-life, low cost, robust and accessible in a network that can operable in remote and harsh environment [82]. A number of applications (fire detection, target tracking, rescue activities, etc.) in WSNs need the accurate position of nodes otherwise the sensed data is irrelevant. Thus, in WSNs, node localization plays an important role [83].

3.2 Categorization of the Literature Review

The contribution of our research highlights the process of localization in three objectives: 1) develop an improved localization algorithm, 2) develop an energy-efficient localization, and 3)contribute more secure localization. The classification of review of literature is shown in Figure 3.1. To achieve the above-mentioned objectives, the review of literature is categorized into different subsections as discussed below:

3.2.1 Literature-based on range-free localization algorithm

Y. Hu and X. Li [84] proposed an improved DV-Hop localization algorithm for WSNs. A threshold value M has introduced for hop count and the positions of unknown nodes are computed up to M hops using weighted average hop distances of beacon nodes. Once unknown nodes get localized, the unknown nodes become beacon nodes called reference nodes. Now the locations of all beacon nodes are computed with the help of reference nodes. In this way, more accurate and precise locations of nodes can be acquired. As compared to conventional DV-Hop algorithm improved algorithm enhances the positioning accuracy with low cost.

The Power-Efficient Range-free Localization Algorithm (PERLA) is introduced by S. Kumar and D. K. Lobiyal [85] for estimating the positions of the unknown nodes in

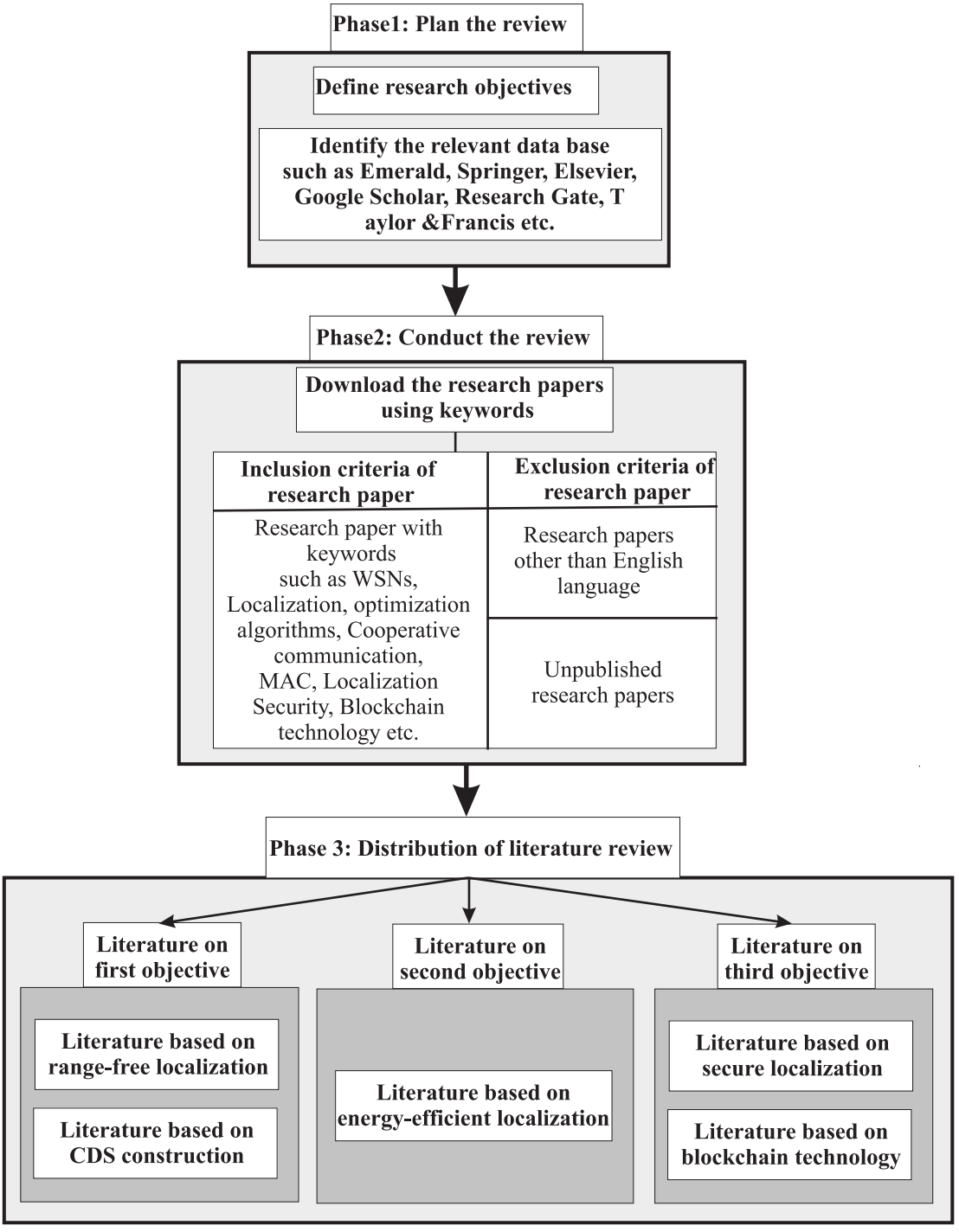

FIGURE 3.1: *Classification of Review of the Literature.*

WSNs. In this algorithm, the communication between beacon nodes and unknown nodes are limited to one way communication which reduced the overall energy consumption. Beacon nodes forward location information to unknown nodes with hop count initialized with zero. Once the location information is obtained by unknown

nodes, the hop size value of beacon nodes is computed by unknown nodes itself which reduces the one-way communication between nodes. For accurate localization of unknown nodes, hop size of beacon nodes are refined by introducing the average value of hop size of each beacon nodes. The refined hop size gives more accuracy of estimation in WSNs.

D. Ma et al. [86] introduced a range-free localization algorithm based on Hop Count Quantization (HCQ) for WSNs. In this algorithm, one-hop neighbor nodes are divided according to hop count value into three disjoint subsets. Further, the integer number of hop count is transformed into a real number hop count based on MDS (Multi-Dimensional Scaling) which resolves the localization problem of WSNs. The algorithm based on real hop count number gives a more accurate relative position as compared to integer value hop count based algorithm. Improvement in the proposed algorithm is independent of the numbers of anchors and proportional to node density.

S. Tomic et al. [87] proposed three new localization algorithm based on the improvement of DV-Hop localization for WSNs. These algorithms are iDV-Hop1, iDV-Hop2 and Quad DV-Hop proposed by authors. For an accurate localization, various steps based on geometry enhancement are followed in iDV-Hop1 and iDV-Hop2. With the help of quadratic programming in Quad DV-Hop bounded least square problem is resolved. Localization errors are diminished by iDV-Hop1 as compared to original DV-Hop and improved DV-Hop algorithm.

X. Chen et al. [88] have investigated improved DV-Hop localization algorithm to upgrade the localization performance of original DV-Hop algorithm. Some beacon nodes at the frontier are implemented to perceive the set border region in this algorithm. Further, the hop size of the beacon nodes is modified using least square error criterion. Moreover, two-dimensional hyperbolic localization algorithm is utilized instead of trilateration for accurate localization. The estimated locations of unknown nodes are optimized using Particle Swarm Optimization (PSO) algorithm.

S. Lee et al. [89] introduced approximate shortest path in irregular or anisotropic multihop range-free localization for WSNs. In this report, a new distance estimation technique is developed to compute the approximate shortest path using a few beacon

nodes based on path deviation. Shortest path approximation between two randomly deployed beacon nodes is achieved by placing a normal node virtual hole between two beacon nodes. Further, how much path is diverted from direct path is computed. The performance of proposed algorithm is compared to another range free algorithm is different shaped region like C-shaped, E-shaped and S-shaped region The procedure achieves better accuracy of the location than other range-free algorithms.

S. Kumar et al. [90] proposed an advanced DV-Hop localization algorithm for WSNs. The first two steps are the similar to traditional DV-Hop. But, the third step of DV-Hop is modified for more accurate localization. A weighted least square algorithm is introduced to enhance the localization accuracy. The solution of the least square equation gives essential information through which the location estimation process can be refined. Further, a correction factor for improving localization error is also considered.

Y. Chen et al. [91] proposed an improved DV-Hop (iDV-Hop) localization algorithm for WSNs. The hop size of beacon nodes is refined with a minimum mean square error. In addition, an improvement variable is also implemented to improve the accuracy of the algorithm. The average hop-size between unknown nodes and beacon nodes is altered by the introduction of a dynamic weight coefficient. Now, the distance between unknown nodes and beacon nodes are computed by using a modified hop size. The locations of unknown nodes are identified using 2D hyperbolic localization algorithm. The nodes positions are further upgraded with solving system of equations. T. Li et al. [92] proposed a Novel DV-Hop (NDV-Hop) algorithm to enhance the localization accuracy for WSNs. Artificial Bee Colony optimization approach is introduced which works based on the Divide-and-Conquer scheme for precise localization. The proposed algorithm diminishes energy consumption as well as time duration which illustrate the significant improvement in the DV-Hop algorithm.

Y. Liu et al. [93] introduced an Improved DV-Hop localization algorithm based on Bat algorithm (IBDV-Hop) for reducing localization error in WSNs. IBDV-Hop algorithm includes optimization methods for improving average hop distance and fitness function to diminish localization error. A velocity correction nonlinear dynamic inertial weight

strategy is used to enhance the accuracy of local and global search scope for better optimization solution. The IBDV-Hop algorithm provides good stability, search capability, and convergence. As the number of iterations and bat groups increases, the localization accuracy of the proposed algorithm increases but the algorithm is weakly affected by density of beacon nodes and communication range. Also, the algorithm requires extra energy and time complexity as compared to other algorithms.

X. Wu. et al. [94] introduced Error Correction and Multi-Hop localization (EM-Hop) to reduce the localization error of DV-Hop. The hop size of each bacon nodes is refined using actual and estimated coordinates of beacon nodes. The transmission is limited to few hops, hence unknown nodes achieved location information from limited beacon nodes. The locations of each unknown nodes are discovered by using the ratio of the square of the distance. M. Peyvandi et al. [95] introduced the localization algorithm using corrected hop-size. At the first step, the difference between the actual and estimated distance between reference nodes is calculated across the network. After that hop size is modified by adding correction value and correction of one-hop distance is achieved using a Received Signal Strength Indicator (RSSI). At last, the positions of unknown nodes are optimized using Marquardt algorithm.

A. Kaur et al. [96] developed a hybrid localization algorithm using range-free localization to avoid high power consumption for WSNs. DV-Hop and centroid algorithm combined with low cost and no additional hardware. The transmission of location information of beacon nodes is limited to t hops instead of across the network. A weight factor is also introduced with the help of hop count, average hop size and communication radius. The algorithm gives superior results when the packets are limited to two hops.

G. Sharma et al. [97] introduced an Improved DV-Hop (IDV-Hop) algorithm using Teaching Learning Based Optimization (TLBO) for WSNs. The hop size of each beacon nodes is refined by adding a correction factor. In localization, the localization error occurs due to collinearity of beacon nodes. To reduce these errors, the concept of collinearity is introduced. For an accurate localization, the beacon nodes with collinearity are not selected to perform trilateration. Further, the localized unknown

nodes which are localized in the first step become assistant beacon nodes. Now, the assistant nodes provide support to unknown nodes for discovering their locations. Finally, the position of unknown nodes is optimized using TLBO.

W. Kun et al. [98] proposed an improved DV-hop with multihop localization for WSNs. The broadcasting of the location information is of linear growth which diminishes the consumption of energy. Further, the pseudo beacon nodes are extended for creating multihop neighbor nodes set for accurate localization. The location information can be easily collected between multihop nodes and the unknown node itself. Finally, the algorithm calculates the unlocalized node coordinated with the help of maximum likelihood estimation.

G. Li et al. [99] proposed a modified DV-hop localization algorithm by reducing mean square error in WSNs. Due to the non-uniform allocation of beacon nodes, the precision of the localization is influenced. The beacon nodes in the local region for the localization method are recognized to increase accuracy. To modify the hop count among sensor nodes, a dynamic weight is added. P. Wang et al. [100] proposed an advanced DV-Hop algorithm to mitigate the localization problem based on Non-dominated Sorting Genetic Algorithm (NSGA)-II. In this approach, a multi-objective model is constructed for beacon nodes to improve the accuracy of estimation in WSNs. Enhanced Weighted Centroid Localization algorithm (EWCL) is shown by G. A. L. Zodi et al. [101] to improve the localization accuracy and energy efficiency. S. Liu et al. [102] proposed a hybrid APIT and DV-Hop based localization for WSNs. Firstly, by using triangle region, all the unknown nodes are divided in two sections. The unknown nodes which rely on a triangle adopt the APIT approach for localization and the locations of rest ones unknown nodes are discovered using the DV-Hop algorithm. In DV-Hop, the weights of hops are included for localization.

D. Zhang et al. [103] introduced an improved APIT algorithm Homothetic Triangle Cyclic Refinement Location (HTCRL) in WSNs. The target area is narrow down using the perpendicular median surface to diminish the localization error. The probability of miscalculation by adding the conditions of judgment is reduced. With an additional condition evaluation, the proposed algorithm limits the probability of misjudgement.

Different parameters like uniform distributed network, randomly distributed network, node density, beacon nodes density and transmission range are considered for localization of the nodes. The proposed algorithm provides high accuracy compared with traditional APIT without introducing additional communication overhead and hardware.

D. Qiao et al. [104] proposed the Gradient descent algorithm to improve the localization accuracy for WSNs. W. Zhang et al. [105] developed a new distributed angle estimation technique under multipath propagation atmosphere for WSNs. Beacon with two antennas is deployed that can produce two linear chirp waves at the same time. The Angle of Departure (AOD) of the emitted wave by the antenna is computed at receiving node. The Received Signal Strength Indication (RSSI) is used to estimate the angle of wave. Multiple arrays of antennas are introduced which provide space diversity in improved estimation techniques. The proposed method is based on radio transceivers and frequency synchronization or precise time synchronization between the transceivers is not required.

S. Tomic et al. [106] introduced a novel local-estimator Distributed RSS-AoA for WSNs. Every node in the networks has its own computation on the basis of least square criterion. Further, second-order cone method is introduced to resolve the problem due to its non-convex nature. The maximum likelihood estimation of power is achieved using measured locations of nodes. G. Sharma et al. [107] developed an Improved Distance vector Hop (IDV-Hop) for WSNs using Teaching Learning Based Optimization (TLBO). The hop-size is modified by using the correction factor for precise localization. Further, the non-collinearity of the beacon nodes are also validated using the concept of collinearity. Additional localization errors are accumulated if the locations of unknown nodes are computed with three collinear beacon nodes. Therefore, before performing trilateration non-collinearity of beacon nodes are ensured in this algorithm. In the first phase of the localization, the unknown nodes become assistant nodes and these nodes assist remaining unknown nodes to get their places. Further, the locations of unknown nodes are optimized using TLBO optimization at

the last step. F. Shahzad et al. [108] introduced DV-Max Hop to improve localization accuracy without considering the energy cost and algorithm convergence time for WSNs. The broadcasting of location information packets is limited to max hops. Once the unknown nodes acquire the information from beacon nodes, the hop count is verified by each unknown nodes and the information is flouted if the hop count is greater than Max Hop. The threshold value of Max Hop is designated on the basis of various factors such as beacon nodes ratio, network density, network shape and expected the degree of irregularity. Multi-objective optimization can be employed to accomplish the optimal value of Max Hop. The proposed algorithm provides accurate localization in anisotropic and isotropic environments with much faster convergence, low energy and communication overheads.

S. Zhang et al. [109] presented Least Square method for DV-Hop (LSDV-Hop) for effective localization in WSNs. Firstly, the least square vector is extracted between actual and estimated location information of randomly chosen beacon nodes. All the beacon nodes are separated into two categories for better localization. Both categories are served to basic DV-Hop where one group of nodes act as a beacon node and remaining one act as unknown nodes. Further, the estimated locations of some beacon nodes are discovered with the localization process. Now, actual as well as estimated locations of beacon nodes are achieved and least square vector is derived with the available information. Consequently, the data of estimated positions information of unknown node is revised by the least squares transformation vector which helps to lower localization error of traditional DV-Hop algorithm .

L. Changyun et al. [110] presented Error Correction and Multi-Hop (EM-Hop) algorithm to reduce localization error for WSNs. The hop-size of each beacon nodes are computed using actual and estimated coordinates. The packets of location information are broadcasted to the limited number of unknown nodes. For different circumstances, the hop size of beacon nodes is computed using approximate distance and hop count. Finally, the locations of unknown nodes are computed using the ratio of square of distances. The proposed algorithm gives better node localization accuracy and reduces the localizing error as compared to the existing algorithm. S. Dong

and Y. Qi [111] introduced an improved DV-Hop localization algorithm to improve the localization accuracy of the WSNs. First two steps of the proposed algorithm are the same as basic DV-Hop algorithm. Firstly, the beacon nodes broadcast its location information to all unknown nodes within its neighborhood. In the third step, the locations of unknown nodes are computed using the Bat optimization algorithm. The optimal locations of unknown nodes can be accomplished using an optimization algorithm. Multi-Probability DV-Hop algorithm increases the accuracy of the node localization and reduces positioning error in WSNs.

J. Mass-Sanchez et al. [112] introduced a weighted hyperbolic DV-Hop to the localization accuracy for WSNs. The algorithm is the combination of WDV-Hop and weighted hyperbolic localization. In this, the correlation matrix is introduced using the estimated distance of unknown nodes and beacon nodes to achieve accurate localization.

G. Sharma et al. [113] developed a distributed DV-Hop localization algorithm for 3D WSNs to improve the localization accuracy. The DV-Hop algorithm is optimized using Genetic algorithm in this work. The hop size is modified using a correction factor. More localization error is accumulated due to co-planarity of beacon nodes. To mitigate this problem, the concept of co-planarity is introduced for beacon nodes. The three beacon nodes with co-planarity cannot take part in trilateration. Further, the unknown nodes which are localized in the first step of localization become assistant nodes. Now, the assistant nodes will help to remain unknown nodes for getting their locations. Finally, the genetic algorithm is applied for optimization purpose.

S. Phoemphon et al. [114] proposed a Fuzzy based weighted centroid localization algorithm with virtual node approximation for WSNs. The number of virtual nodes is determined with their locations using beacon-nodes triangles. The locations of unknown nodes are computed by using virtual nodes as well as beacon nodes. In this way, the accurate location of unknown nodes can be accomplished. Further, a fuzzy-based centroid algorithm is developed by allocating different weights factors. F. Darakeh et al. [115] presented Distributed cooperative Range-free Localization (DCRL) algorithm for WSNs. A bell-shaped bounded region is identified for inaccurate locations of each unknown node in DCRL-WSN. The extended bounds region of each unknown

nodes contracted iteratively causes accurate localization. Further, the bounded region is estimated for each unknown nodes through resolving two constrained convex optimization. L. Cui et al. [116] introduced an ameliorated DV-hop localization algorithm with differential evolution for WSNs. The discrete value of hop count between sensor nodes is improved by continuous one-hop nodes between adjacent nodes. Moreover, the process of location estimation is optimized on the basis of the weighted square of error of measured error. For achieving a global solution of localization problem, the differential evolution optimization algorithm is adopted in this work. The hybrid algorithm of DV-Hop and differential evolution is called DECHDV-Hop. Comparison of these different localization algorithms is shown in Table 3.1.

TABLE 3.1: *Literature-based on range-free localization.*

Author(s)	**Algorithm**	**Remarks**
H. Yu et al. (2013) [84]	Improved DV-Hop	M threshold value is used for distance estimation which rises the computation time, cost. Also, the deployment of sensor nodes is static in nature.
S. Kumar et al. (2014) [85]	PERLA algorithm	More localization error accumulated because Hop size is calculated by unknown nodes instead of anchor nodes.
Ma. Di et al. (2012) [86]	Localization based on hop count quantization	Distance between unknown nodes and beacon nodes are computed by using hop count and neighbor partition. The distribution of nodes is considered uniform.
S. Tomic et al. (2015) [87]	Improvement of DV-Hop localization	Three different algorithms are developed to reduced localization error. Different topologies are considered in static node deployment but have high complexity.
X. Chen et al. (2012) [88]	Improved DV-Hop algorithm	Some of the beacon nodes are deployed at the border to accomplish accurate localization. Also, the position of unknown nodes is optimized using PSO, but have more computational cost.

S. Lee et al. (2014) [89]	Multihop range free algorithm	The shortest path from beacon to the unknown node is calculated with the help of path deviation by using expected hop count but require high computational power
S. Kumar et al. (2013) [90]	Advanced DV-Hop localization	Hop size will change in the mobile environment and the communication between unknown nodes and anchor increase causes resource exhaustion
Y. Chen et al. (2018) [91]	Improved DV-Hop	The distances among sensor nodes are computed using modified hop size and the position of unknown nodes is computed using 2D hyperbolic localization. But validation for dynamic networks is required.
Y. Liu et al. (2017) [93]	IBDV-Hop localization	A weight factor is introduced for reducing localization error and Bat algorithm optimization is used for optimization. But it is suitable for static networks
Y. Xiuwu et al. (2016) [94]	EM-Hop localization algorithm	The localization error is reduced by using error correction and multi-hop, but it performs well only in static network scenarios
M. Peyvandi et al. (2015) [95]	Hybrid DV-Hop and RSSI algorithm	One-hop distance is validated through Received Signal Strength Indication (RSSI) which makes the algorithm complex and costly. Fault tolerance corporation is required.
A.Kaur et al. (2019) [96]	Enhanced Weighted centroid DV-hop algorithm	The broadcasting of anchor nodes information is limited to threshold hop count rather than across the network to reduce energy consumption. But it affects localization accuracy and more anchors nodes are required for localization.

G. Sharma et al. (2018) [97]	Modified energy-efficient algorithm	With the help of correction factor the second step of DV-hop is modified and after that optimal anchor node are selected for optimization process but the system is more complex
W. Kun, et al. (2016) [98]	Improved DV-hop with multi-hop localization	The locations of unknown nodes are evaluated using maximum likelihood estimation. But it performs well in static network scenarios.
G. Li et al.(2019) [99]	Advanced DV-Hop	The precise positions of sensor nodes are obtained by identifying beacon nodes in the local region.
P. Wang et al. (2019) [100]	DV-Hop based on Non-dominated Sorting Genetic Algorithm	A multi-objective model is constructed for beacon nodes to improve the accuracy of estimation but valid for static nodes.
G-A. Zodi et al. (2015) [101]	Enhanced Weighted Centroid algorithm (EWCL)	The position of each beacon nodes is weighted using linear weighting centroid. But, it performs well in static networks scenarios.
S. Liu et al. (2017) [102]	Hybrid APIT and DV-Hop	The locations of unknown nodes are identified with the help of DV-Hop and APIT. But, more errors are accumulated if the unknown node lies at the border of the area.
D. Zhang et al. (2017) [103]	Improved APIT algorithm using HTCRL	The target area is narrow down using the perpendicular median to reduce localization error. But, fault tolerance and mobility are required.

D. Qiao et al. (2011) [104]	Gradient descent algorithm	The locations of unknown nodes are computed with knowledge of inter-sensor distance measurement. The algorithm performs well in static network scenarios.
W. Zhang et al. (2013) [105]	Distributed angle estimation approach	Beacon nodes are deployed with two antennas and RSSI is used for signal measurement. All beacon nodes are required for localization which reduces the network lifetime.
S. Tomic et al. (2016) [106]	Distributed RSS-AoA	Sensor nodes update its computation using least square criterion, but applicable only for static networks.
G. Sharma et al. (2018) [107]	Modified DV-hop algorithm	Hop size is improved using correction factor and DCL Degree of Collinearity (DCL) ensure that collinear anchor node does not take part in localization but system complexity is more and need more energy.
F. Shahzad et al. (2016) [108]	DV-maxHop algorithm	By introducing control parameter maxHop propagation of information beyond maxHop value is eliminated. But, mobility is not considered and more complex in nature.
S. Zhang et al. (2016) [109]	LSDV-Hop algorithm	Hop size is modified by introducing correction factor and accurate localization is achieved by extracting a least-squares transformation vector between the true and estimated location data of anchor nodes, but fault tolerance is required.
C. Li. et al. (2014) [110]	EM-Hop algorithm	The error of hop size is reduced by using error correction and multi-hop, but the deployment of nodes is static and required fault tolerance.

S. Dong and Y. Qi (2015) [111]	MP (Multi-Probability)DV-Hop Localization algorithm	Hop size is further improved by taking the average of hop size and optimization is achieved using bat algorithm, but the complexity of the algorithm is high.
J. Mass-Sanchez et al. (2017) [112]	Weighted hyperbolic DV-Hop	The accuracy is improved by using a combination of WDV-Hop and weighted hyperbolic localization algorithm which include the estimated distances matrix between the node and the reference nodes. Mobility of nodes is required.
G. Sharma et al. (2018) [113]	Distributed DV-Hop	The hop-size of the beacon nodes is refined including the correction factor. Collinear beacon nodes incorporate more error in localization which is reduced by DCL. But the computational complexity of the algorithm is high.
S. Phoemphon et al. (2018) [114]	Fuzzy based weighted centroid algorithm	The locations of unknown nodes are computed using virtual nodes. But, the algorithm performs well for static network scenarios.
S. Kumar et al. (2016) [92]	Novel DV-hop localization	Hop size is calculated by unknown nodes instead of anchor nodes for reducing energy consumption and constrained optimization is used but complexity is high
F. Darakeh et al. (2018) [115]	Distributed cooperative Range-free Localization	Unknown nodes compute their locations using two constrained convex optimization. But, the computational complexity of the algorithm is high and required mobility.

Cui, L. et al. (2018) [116]	Ameliorated DV-hop with Differential Evolution	The discrete value of hop-count is converted into continuous to accomplish accurate localization. The concepts of mobility and fault tolerance are required.

Y. Sun et al. [117] proposed Krill Swarm optimization for computing the position of unknown nodes in WSNs. First, by using DV-Hop algorithm, distances are found between unknown nodes and beacon nodes. In addition, the locations of unknown nodes with Krill swarm are optimized. S.K. Gharghan et al. [118] introduced the Log-Normal Shadowing Model (LNSM) with hybrid Particle Swarm Optimization-Artificial Neural Network (PSO-ANN) to improve the localization performance. Firstly, the unknown nodes and beacon nodes distances are measured by using LNSM and PSO-ANN. The distance between the mobile node and coach is computed using a feed-forward neural network with Levenberg-Marquardt training algorithm. The RSSI measurement is achieved for both indoor and outdoor environments. C. Tao et al. [119] introduced an improved genetic algorithm for node localization with a low computational cost for WSNs. The research work can effectively improve the local search ability with a short time. Generally, the optimization algorithm converges at near-optimal and cannot reach global optimal. S. Ziwen et al. [120] presented a novel localization algorithm based on Multi-Objective Particle Swarm Optimization for WSNs. In this work, a multi-objective model is constructed based on space constraint and geometric constraint to mitigate localization problems. Accurate localization can be achieved with geometric topology constraint. To maintain the size of the archive, a dynamic method is introduced.

R. Rajakumar et al. [121] presented a novel Golf wolf Optimization for Localization node Problem (GWO-LP) in WSNs. The main motive of this work is to discover the positions of unknown nodes with the help of beacon nodes. GWO is introduced in localization to refine the position of unknown nodes. In this work, GWO works on the basis of principle, leadership hierarchy, and behavior of grey wolves. Z. Cui et al. [122] introduced a novel DV-Hop algorithm based on Orient Cuckoo Search (OCS)

for WSNs. Two diverse random distributions are adopted to achieve optimum global search proficiency. For more investigation, ten diverse distributions are introduced and compared with CEC2013 test. It is perceived from results that Levy distribution and Cauchy distribution performs well out of all ten distributions. M. Mehrabi et al. [123] introduced an improved DV-Hop algorithm for WSNs using evolutionary algorithms to achieve more accurate localization. Firstly, the beacon information is broadcasted across the network using the DV-Hop first phase. Secondly, the hop-size is evaluated and the distance between unknown nodes and beacon nodes are estimated. Further, the hop size is optimized using Shuffled-Frog Leaping Algorithm (SFLA). Moreover, the locations of unknown nodes are computed by applying hybrid GA-PSO optimization at last step of DV-Hop.

Genetic Algorithm (GA) based improved localization algorithm is presented for WSNs by B. Peng and L. Li [124]. The minimum hop-count and hop-size are computed for each beacon nodes. Further, the average hop size is calculated to overcome the localization error. The possible area of each unknown nodes is defined and create an initial population in the possible area. For each individual the fitness function is computed. This work performs well and gives more accurate localization for WSNs. C. Vimalarani et al. [125] presented an Enhanced PSO-based Clustering Energy Optimization (EPSO-CEO) to diminish the energy consumption for WSNs. The cluster head in this work is selected with the help of PSO. X. Luo et al. [126] investigated a Taylor based algorithm using the Extreme Learning Machine (ELM) for WSNs. For an accurate localization, Single-hidden Layer Feed-forward Network (SLFN) is introduced. The measurement error of Time Difference of Arrival (TDoA) is minimized by incorporating SFLN. Further, the errors are optimized by using ELM. The simulated results of SFLM are optimized by using Taylor series expansion algorithm. The measurement error of mobile station is also minimized by Taylor series. The ELM algorithm gains attention in this work due to its fast convergence capability. The effect of Non-Line-of Sight(NLOS) is reduced by ELM with Taylor series expansion.

P. Songyut et al. [127] introduced a hybrid localization algorithm using Fuzzy logic and Extreme Learning Machine (ELM) using Vector Particle Swarm Optimization

(VPSO) for WSNs. The localization approach is improved by incorporating a fuzzy logic in centroid and utilized an ELM. Firstly, the short coverage of nodes and low density of sensor nodes are appropriately utilized with fuzzy logic. Further, the robust localization process is achieved by using the ELM algorithm. Moreover, the accuracy of localization is improved with VPSO in heterogeneous networks. J. Zheng et al. [128] introduced a Neural Network Ensembles based Localization (LNNE) algorithm for WSNs. In this work, the location of unknown nodes is computed by using LNNE on the basis of connectivity information. With the help of diversity of NN, the localization errors are diminished. X. Yang et al. [129] introduced an efficient RSSI with DV-Hop localization based on Extreme Learning Machine and Regularized Correntropy Criterion (RHOP-ELM-RCC) for WSNs. In this work, the RSSI and DV-Hop localization algorithm are integrated for the better localization process. The location of the unknown nodes is discovered by implementing ELM and SFLN. To diminish the localization error, half-quadratic optimization technique is utilized instead of Least Square Estimation (LSE).

S. Sivakumar and V. Venkatesan [130] proposed an error minimization localization approach by introducing Fish Swarm Optimization (FSO) for WSNs. The locations of sensor nodes are discovered by utilizing Mobile Anchor Positioning - Mobile Anchor & Neighbor (MAP-M&N) localization approach. The beacon nodes are embedded with GPS and forward its location information to unknown nodes across the network. The unknown nodes can identify their locations once suitable information is gathered about beacon nodes. MAP-M&N with FSO is incorporated for discovering the location of nodes. Root Mean Square Error is computed as a recital factor to analyze the simulated results. V. Gupta and B. Singh [131] introduced a centroid based range-free algorithm with Particle Swarm Optimization (PSO) for WSNs. In this work, the localization process is achieved with the centroid algorithm under log-normal shadowing networks. Further, the position of unknown nodes is optimized using PSO. L. Jian Yin and M. Elhoseny [132] proposed a new DV-Hop based localization algorithm on the basis of Half-Measure Weighted Centroid for WSNs. All the sensor nodes are deployed in two-dimensional distributions with a short range of transmission. Then,

the distance between beacon nodes and unknown nodes are identified so that shortest route can be optimized. S. Amri et al. [133] introduced a new fuzzy logic localization algorithm mechanism for WSNs. The location estimation process is achieved by using centroid localization mechanism. The position of unknown nodes is computed using fuzzy logic approach. The distance between sensor nodes is figured using flow measurement through a wireless channel by fuzzy logic. Once the position of unknown nodes is discovered, the Cluster Head (CH) are elected which minimizes the energy consumption to prolong the network lifetime.

H. M. Kanoosh et al. [134] developed a Salp Swarm Localization Algorithm (SSLA) for location estimation process in WSNs. The beacon nodes discover their location through GPS and forwards that information to neighbored unknown nodes. Firstly, unknown nodes discover their Localized Unit (LU) in which at least three beacon nodes must be present. The unknown nodes act as a reference node whose locations are identified in the first iteration of localization process. G. Kumar et al. [135] proposed an improved localization algorithm by using vector-based swarm optimization. In this work, the load balancing problem is addressed in the localization process. Firstly, a CDS is constructed which consist of beacon nodes for the localization process. The beacon nodes are selected based on the degree of connectivity of nodes for CDS. Further, the load balancing among beacon nodes is obtained using vector-based Swarm optimization. Comparison of these different optimization algorithms is shown in Table 3.2.

TABLE 3.2: *Literature-based on optimization techniques.*

Author(s)	**Algorithm**	**Remarks**
Y. Sun, et al. (2016) [117]	Krill swarm DV-Hop	New DV-Hop is proposed to enhance location precision and each sensor node changes their location frequently using Krill optimization algorithm to get optimal value and increase the global convergence rate. But, the complexity of the algorithm is high.

S.K. Gharghan et al. (2016) [118]	Hybrid PSO-ANN	To improve localization accuracy efficiently, but the integration of PSO-ANN makes it is very costly and also not applicable for mobile networks.
C. Tao et al. (2015) [119]	Improved Genetic algorithm	Improved Genetic algorithm effectively improves the local searchability and the search accuracy by taking a short time. But, optimization algorithm converges at near-optimal and cannot reach global optimal.
S. Ziwen et al. (2015) [120]	Multi-objective swarm optimization	For the appropriate solution the multi-objective swarm optimization method is implemented which restrict the sample volume. To maintain the size of archive, dynamic method is introduced which increases the computational cost. Also, the proposed approach is not suitable for dynamic network scenarios.
R. Rajakumar et al. (2017) [121]	GWO-LP localization	The proposed algorithm follows the social behavior of the grey wolves and their attacking techniques and leadership hierarchy and it improves the localization accuracy, improves the success rate and estimates correct position of unknown nodes. But, optimization algorithm converges at near-optimal and cannot reach global optimal.
Z. Cui et al. (2016) [122]	Orient cuckoo search algorithm	Evolutionary oriented cuckoo search algorithm (OSO) is proposed for better localization accuracy and precision estimation and global search capability is dominated by using two different random distributions. Two random distribution algorithms increase computational cost and complexity.

M. Mehrabi et al. (2016) [123]	Evolutionary algorithm based DV-Hop	To improve the localization accuracy and minimize error, the second step of the DV-hop is modified by using Shuffled Frog Leaping and Third step is done by using a hybrid genetic-PSO algorithm. But, the computational cost is high due to various optimization algorithms.
B. Peng and L. Li. (2015) [124]	Genetic algorithm-based DV-hop	The position calculation of unknown nodes is optimizing using optimal solution owing to high searchability. But, the main drawback of this scheme is that it cannot be emphasized for mobile networks.
C. Vimalarani et al. (2016) [125]	Enhanced PSO based optimization	In this algorithm, the selection of cluster head is done through PSO and it improves network lifetime and minimized energy consumption. This approach can be considered for localization in WSNs.
X. Luo et al. (2014) [126]	Taylor localization algorithm using ELM	Time difference of arrival measurement error is reduced by SLFN and then optimization is achieved by Extreme learning machine and reduced NLOS effect. But, incorporation of neural network influences the computational cost, complexity, and proneness to overfit.
S. Phoemphon et al. (2018) [127]	ELM using Vector PSO	A fuzzy logic approach is incorporated with centroid localization algorithm. But, the centroid localization algorithm is not able to improve localization accuracy in mobile networks. It happens due to that centroid always change in dynamic scenarios. Also, ELM increases the computational cost of the algorithm.

J. Zheng et al. (2012) [128]	Range free localization based on Neural network	The locations of the nodes is computed by LNNE based on the WSNs connectivity information. But, the computational cost of the algorithm is high due to the neural network which increases the complexity. Also, it is not suitable for dynamic network scenarios.
X. Yang et al. (2017) [129]	RHOP-ELM-RCC algorithm	Distance between nodes is calculated by using DV-Hop and RSSI to improve the localization accuracy. RSSI belongs to range-based approaches which are included in the proposed algorithm. Range-based approaches are costly and need special hardware for operation.
S. Sivakumar and V. Venkatesan (2017) [130]	MAP-M&N algorithm using FSO	Unknown nodes are able to calculate their location using FSO optimization algorithm and it gives better localization accuracy. Only beacon nodes are considered as mobile and unknown nodes are static in nature. Both nodes can be considered mobile in nature.
V. Gupta and B. Singh (2018) [131]	Range-free algorithm based on PSO	The localization of unknown nodes is achieved by PSO optimization algorithm. But, the main drawback of the proposed scheme is that the algorithm converges at near-optimal and cannot reach global optimal.
L. Jian Yin and M. Elhoseny (2019) [132]	DV-Hop based on Half-Measure Weighted Centroid	Both the theoretical and experimental simulation is examined to analyze the performance of the algorithm. But, it cannot be applied in the mobile network because of center of the nodes changes in dynamic scenarios which affect the localization accuracy.

S. Amri, et al. (2019) [133]	Fuzzy logic based algorithm	The proposed algorithm cannot applicable to mobile networks. The disadvantage of the algorithm is that the results can be lead to the wrong conclusions based on logic and at some point, you will overanalyze things. Also, the residual energy is not considered during cluster head selection which makes the network partial failure.
H. M. Kanoosh et al. (2019) [134]	Salp Swarm Localization Algorithm (SSLA)	A localized unit of three beacon nodes is identified for estimating the locations of the unknown nodes. But more error will be accumulated if three beacon nodes are collinear in nature. Also, the network is considered static in nature, cannot be applied for mobile network scenario.
G. Kumar et al. (2019) [135]	Vector-based swarm optimized Connected Dominating Set	The CDS of beacon nodes is constructed for proper utilization of constraint resources. But, the beacon nodes for CDS construction are selected on the basis of the degree of connectivity. The network becomes partial available if the beacon with high degree of connectivity and low residual energy is selected for CDS.

3.2.2 Literature-based on construction of Connected Dominating Set

A. Najla et al. [136] presents two Connected Dominating Set (CDS) algorithms for WSNs. The main motive of both algorithms is to minimize the size of CDS. Various CDS algorithms are depicted in Figure 3.2. Both the approaches used Unit Disk Graph (UDG) for CDS construction. Firstly, an independent set S1 is identified for CDS construction. Secondly, a small set of nodes S2 are identified which dominates

various sensor nodes. Further, the nodes present in S2 are attached with the nodes in the S1 set, which makes a final CDS after adding more connecting nodes in the networks. S. Tuo et al. [137] introduced an adaptive algorithm to discover CDS for WSNs. In this, new methods of CDS construction are adopted using Energy Harvest called CDSEH. One method works in a centralized manner and the other one is distributed in nature. A limited number of energy harvesting sensor nodes are included during the process. Also, multiple CDS are constructed to save energy for WSNs.

P. Tayler et al. [138] investigated dominating set for WSN survivability. The energy conservation issue of sensor nodes with fluctuating initial energy is mitigated with this work. Three search algorithms are developed to prolong the network lifetime for sensor nodes. Local search is achieved using the initial feasible solution of multiple disjoint domination sets.

C. Chou et al. [139] introduced strongly CDS algorithm for heterogeneous WSNs. Efficient routing can evade excessive packet transmission which helps to save more energy of sensor nodes in WSNs. CDS in networking works as a virtual backbone and provide efficient routing. The construction of CDS suffers from a lot of problems in undirected unit disk graph. In this work, the construction of CDS is achieved with the directed graph called a Strongly CDS (SCDS) as a backbone of the network. M. P. Jasaswi et al. [140] represented the construction of Minimum Connected Dominating Set (MCDS) with pseudo domination set for WSNs. The research work diminishes the size of the CDS as possible. CDS has constructed initially and further the size of CDS is reduced by adopting an intelligent method. Some of the nodes are eliminated from CDS without affecting the connectivity. In CDS, sensor nodes face the problem of early exhaustion and make network partially operated. Therefore, to mitigate this problem CDS must be rotated periodically. L. Chuanwen et al. [141] proposed a novel distributed CDS and two factors such as link and degree of the connecting tree are considered to achieve Minimum Connected Dominating Set (MCDS). Initially, the dominating set is constructed based on the above two factors. Secondly, the connector nodes for DS are identified based on the connecting tree. W. Yiwei et al.

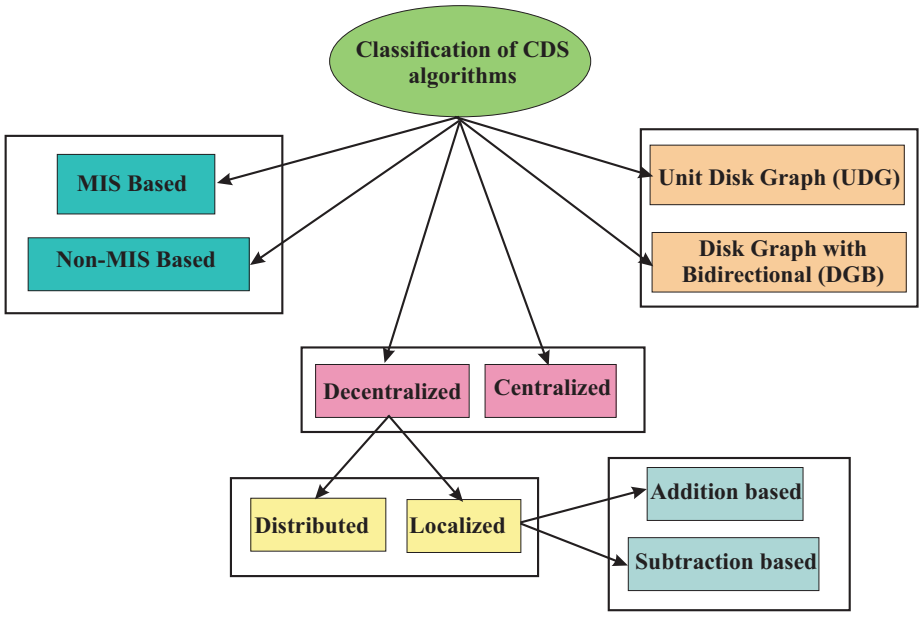

FIGURE 3.2: *Classification of algorithms for CDS creation.*

[142] introduced a k connected and m dominating set (kmCDS) for better routing and fault tolerance in WSNs. In this work, m dominating sets are discovered using centralize algorithms. Further, the k connectivity of the dominating set is identified using a distributed algorithm. All sensor nodes are stored in decreasing order with their degree of connectivity, energy and serial number. For DS construction, the higher preference is given to degree of connectivity. Because the size of the DS will be small if the nodes are elected on the basis of degree of connectivity. Also, energy is considered as a second factor for DS construction. The sensor nodes with more energy are highly preferred for dominating set The process of CDS construction is shown in Figure 3.3. F. Hamza et al. [143] proposed a CDS Algorithm on the basis of Optimized Region Efficient Data (AORED) routing protocols for WSNs. AORED routing is employed for constructing a dominating set The process of construction is divided into two phases: (1) set up phase (2) steady phase. The sensing field is separated into two groups of homogeneous sensor nodes. Each group has a different number of sensor nodes in the network and BS is deployed in the center of the field. The sensor nodes with a higher degree of connectivity are elected Dominator nodes. A. N. Najla et al. [144] present three algorithms for CDS construction for WSNs. Firstly; an independent set S1 is constructed in which the sensor nodes with three

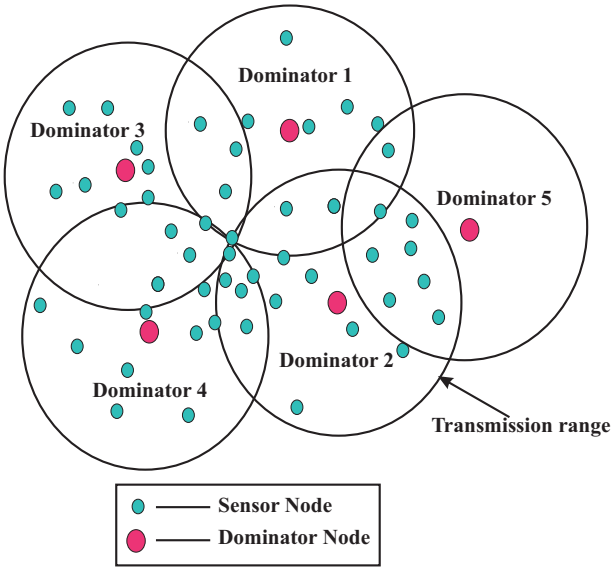

FIGURE 3.3: *CDS construction process.*

hops are included. Secondly, a set S2 of dominator nodes are selected from S1 using geometrical properties. Finally, the connector nodes are elected which connects the final CDS.

M. Rai et al. [145] introduced an energy-efficient Minimum Connected Dominating Set (MCDS) with the help of dominating set for WSNs. The research work is carried out in three steps: (1) discover dominating set (2) recognize connectors and, (3) pruning of dominating set In the first phase of algorithm, the dominating set is identified in which sensor nodes are elected based on the degree of connectivity of neighbor nodes. After constructing the dominating set, the connector for the dominator nodes is discovered. Finally, pruning is applied to achieve the MCDS which prolongs the network lifetime significantly. Comparison of these different backbone creation algorithms is tabulated in Table 3.3.

TABLE 3.3: *Literature-based on CDS construction.*

Author(s)	**Algorithm**	**Remarks**
N. Al-Nabhan et al. (2012) [136]	Two Connected Dominating Set	The proposed schemes consume low power, but the number of no upper and lower limit is given about sensor nodes in CDS.

S. Tuo et al. (2016) [137]	CDSEH	Two methods are adopted for backbone creation and one method work in a centralized manner and another one works in distributive. The network became partial if the single node fails at the central level.
T. Pino et al. (2018) [138]	Three dominating set methods	This approach is applicable only for static networks and validation of the same is required in dynamic network scenarios.
C. W. Chou et al. (2013) [139]	Strongly CDS	The deployment of sensor nodes with mobility requires to be examined. Mobility can degrade the performance of the algorithm.
J. P. Mohanty et al. (2016) [140]	MCDS with pseudo dominating set	Sensor nodes are eliminated from CDS to achieve MCDS. Elimination of random nodes makes the network partial available.
C. Luo et al. (2018) [141]	Distributed algorithm for MCDS	The algorithm is well suitable for static networks and needs attention for the mobile network.
Y. Wu et al. (2007) [142]	kmCDS	The algorithm consumes low power, but the upper and lower limit of the number of dominators is not defined.
H. Faheem et al. (2016) [143]	Optimized Region Efficient Data based algorithm	The algorithm is appropriate only for homogeneous WSN and validation in heterogeneous environments are requisite.
N. Al-Nabhan et al. (2016) [144]	Three algorithms for CDS construction	Validations in mobile networks are required.

M. Rai et al. (2009) [145]	Energy-efficient MCDS	The dominator sensor nodes are constructed elected on the basis of the degree of connectivity which affects the network lifetime.

3.2.3 Literature based on Energy-Efficient techniques

Sensors nodes have energy resources and energy is the most challenging issue of WSNs. It requires energy minimization techniques and mechanism reduces energy consumption and prolongs the lifetime of the network because it is difficult to renew sensors energy source or battery.

L. Cheklat et al. [146] developed an energy-efficient model for Peer to Peer (P2P) WSNs to prolong the network lifetime. The length of path is optimized using chord assets which minimize the hop count between sensor nodes. The cluster head is selected dynamically over time for energy efficiency. The highest energy nodes are selected as a cluster head which minimizes the chord topology. A. Ali et al. [147] proposed an energy consumption model for WSNs. The parameters of both layer physical and MAC are considered for model construction. The consumption of energy for both above-mentioned layers is analyzed in the real environment and NS-2 also. The transmitted power of the model is optimized which reduces energy consumption. P. Nayak and B. Vathasavai [148] introduced a clustering Type-2 Fuzzy Logic (T2FL) algorithm to prolong the network lifetime for multi-hop WSNs. All sensor nodes are divided into different level based on distance from BS. The cluster head is nominated at each level using Fuzzy Logic schemes. Higher energy sensor nodes are most preferred as a stand by cluster head close to BS for handling any cluster head failure suddenly.

M. Abo-Zahhad et al. [149] presented an energy-efficient model for WSNs. This work computes the energy consumption per payload bit transferred at MAC and physical layer without error. For Additive White Gaussian Noise (AWGN) the power for transmission is selected in such a way that it consumes minimum power. D. Apiletti et al. [150] introduced SElecting REpresentatives in sensor NEetworks (SERENE)

to reduce energy consumption in WSNs. SERENE generates a model with the help of correlation analysis and selection of sensor representatives. The temporal correlation is identified among sensor nodes using correlation analysis in terms of time and strength of the correlation. Further, the spatial correlation is identified among sensor nodes and faraway. Representative-Sensors (R-Sensors) are selected out of all sensor nodes in the network. Different parameters such as distance among nodes and cost of transmission are considered for representative sensor selection process.

Z. Zhu et al. [151] developed the energy-aware workflow model for WSNs to prolong the network lifetime. In this work, a mathematical model is provided which evaluates the energy consumption of sensor nodes. Most of the energy is consumed at an active period of sensor nodes and idle time consumes low power as much as possible. D. Antonio et al. [152] developed an energy-efficient consumption model for WSNs. A set of Colored Petri Nets (CPN) is utilized to evaluate energy consumption in this research work. The energy consumption for all sensor nodes is computed by CPN automatically. A cooperative MAC protocol is introduced by H. W. Kim et al. [153] for underwater WSNs. The proposed scheme is completed in two phases named channel reservation and data transfer. In the first phase, the channel is reserved by source sensor nodes by identifying cooperators nodes in the control packets. In the second phase, the source node broadcast the data to destination node through suitable cooperative nodes. H. R. Shamna and L. Jacob [154] introduced a distributed cooperative MAC protocol for wireless networks. The prime motive of cooperative protocols is to improve throughput, reliability, delay, network coverage and prolong the network lifetime. The research work is introduced for single-hop as well as multi-hop networks. The energy consumption is reduced by forwarding packets using cooperative communication at the MAC layer. Further, energy efficiency and network lifetime are improved by using distributed cross-layer cooperative MAC protocols. Y. I. Joo and K. Hur [155] proposed a Distributed Cross-layer cooperative MAC (DCMAC) protocols for WPAN. In multi-hop communication, a slow single-hop communication between BS and sender nodes is replaced by multi-hop communication using cooperative communication. The appropriate cooperative nodes are selected based on residual energy,

queue size, and data rate. Cooperative communication at MAC layer improves the network lifetime significantly.

S. Hangguan et al. [156] proposed a Distributed Cooperative MAC (DCMAC) protocols for wireless networks. In multi-hop communication, a slow single-hop communication between BS and sender nodes is replaced by multi-hop communication using cooperative communication. The appropriate cooperative nodes are selected based on residual energy, queue size, and data rate. Cooperative communication at MAC layer improves the network lifetime significantly. K. Liu et al. [157] developed a power-optimized cooperative MAC protocol for WSNs to prolong the network lifetime. For energy-efficient communication, one or more cooperative sensor nodes are selected for cooperation. The transmission power of cooperative nodes is optimized by minimizing the residual energy during data transmission. Further, the cooperative nodes are nominated on the basis of residual energy and sufficient channel gain. Data packets are broadcasted with the help of cooperative only if the cooperative nodes are able to diminish energy consumption. Cooperative MAC transmission is shown by J. Lin and M. A. Weitnauer [158] for WSN to extend the lifetime. The energy hole problem is addressed by developing On-demand Scheduling Cooperative MAC (OSC-MAC) for multi-hop WSNs. The Spatio-temporal challenges during cooperative communication are handled by OSC-MAC. The traffic contention during transmission is diminished by using orthogonal and pipelined duty cycle scheduling.

M. Sami et al. [159] presented an Energy-Aware Cross-layer Cooperative MAC (EACC-MAC) protocol for Ad Hoc wireless networks. Cooperative communication has recently gained attention as an efficient technique which improves channel impairment, network lifetime and radio spectrum constraints. The optimal communication mode is selected between direct communication and cooperative communication based on source-destination link quality and destination queue. Further, the cooperative node is selected by considering location information and residual energy of nodes which prolongs the network lifetime significantly. X. Wang and J. Li [160] proposed an improved Cooperative MAC protocol for Mobile Ad-hoc NETworks (MANET) to prolong the network lifetime. A novel cross-layer Distributed Energy-adaptive

Location-based CMAC protocol called as DEL-CMAC is utilized for energy efficiency. The best cooperative node is selected based on location information and residual energy of nodes for cooperative communication. The energy consumption on transceiver circuitry and transmit amplifier are also included for the model. Comparison of these different energy models is shown in Table 3.4.

TABLE 3.4: *Literature-based on Energy-Efficient techniques.*

Author(s)	**Algorithm**	**Remarks**
C. Lamia et al. (2017) [146]	Limited energy model for P2P	To prolong network lifetime proposed algorithm uses chord assets that optimize the length of the path by using shortest hop. But, the energy factor is only used for the cluster head selection process, a number of sensor nodes present on that cluster are not considered causes more cluster heads in the networks.
P. Nayak and B. Vathasavai (2017) [148]	Energy-efficient algorithm based on T2FL	Cluster heads are elected based on T2FL. But it is not suitable for heterogeneous networks. Also, the mobility of nodes required to be considered.
A. Ali et al. (2016) [147]	Energy consumption model for WSNs	Energy consumption at the physical layer and MAC layer are considered for modeling. The received power can be optimized.
M. Abo-Zahhad et al. (2015) [149]	Minimum energy consumption model	To reduce energy consumption, energy consumed at MAC and the physical layer is derived using the proposed model in the real environment. But, suitable only for homogeneous networks.

D. Apiletti et al. (2011) [150]	SERENE model	The optimal representative sensors can be selected by considering the energy parameter.
Z. Zhu et al. (2012) [151]	Energy awareness workflow	The lifetime of the nodes can be enhanced by designing sensor nodes with low power consumption. The validation of the proposed schemes required in mobile network scenarios.
D. Antonio et al. (2017) [152]	CPN model for evaluating Energy consumption	The proposed algorithm used a set of CPN (Colored Petri Nets) models to evaluate the energy consumption of nesC operator.
Kim, H. W. et al. (2018) [153]	Cooperative MAC protocol	The proposed research work is suitable for static networks. Also, the parameter of energy can be considered for cooperative nodes selection.
H. R. Shamna and J. Lillykutty (2017) [154]	Distributed cooperative MAC	The proposed scheme is suitable for single-hop and multi-hop. But, cannot perform well in dynamic networks.
Y. I. Joo and K. Hur (2013) [155]	Distributed Cross-layer cooperative MAC (DC-MAC)	The cooperative nodes are selected bases on residual energy and data queue to perform the task. The distance between the cooperative node and destination node also affects the performance of the scheme.

H. Shan et al. (2009) [156]	Distributed Cooperative MAC	The proposed scheme is applicable only for static networks.
K. Liu et al. (2016) [157]	Power optimized cooperative MAC	The cooperative nodes are nominated on the basis of residual energy and sufficient channel gain, but sometimes nodes with higher residual energy reside far from the destination.
J. Lin and M. A. Weitnauer (2018) [158]	On-demand Scheduling Cooperative MAC	This scheme is appropriate for homogeneous and static networks scenarios.
M. Sami, et al. (2015) [159]	Energy-Aware Cross-layer Cooperative MAC	The protocol prove its effectiveness but does not support the mobility of nodes.
X. Wang and J. Li (2015) [160]	Improved Cooperative MAC protocol	The cooperative node is nominated on the basis of residual energy and sufficient channel gain, but the distance between the destination and cooperative nodes must be included for better performance.

3.2.4 Literature on Secure localization

Localization of sensor nodes is very essential because various network operations depend upon the location of nodes and the detected event also bounded with the location of nodes. When sensor nodes are deployed in the remote area or hostile area, the adversary may steal the location or they may attack the localization process to make estimated location wrong. By using jamming, tampering, exhaustion, Denial of Service (DOS) attack and interference they may incorrect the estimated location of

the nodes [77]. WSNs are mostly installed in hazardous, infrastructure-less and lack of physical security environments and different types of attacks on various layers are shown in Figure 3.4. G. Han et al. [161] developed a collaborative secure localization

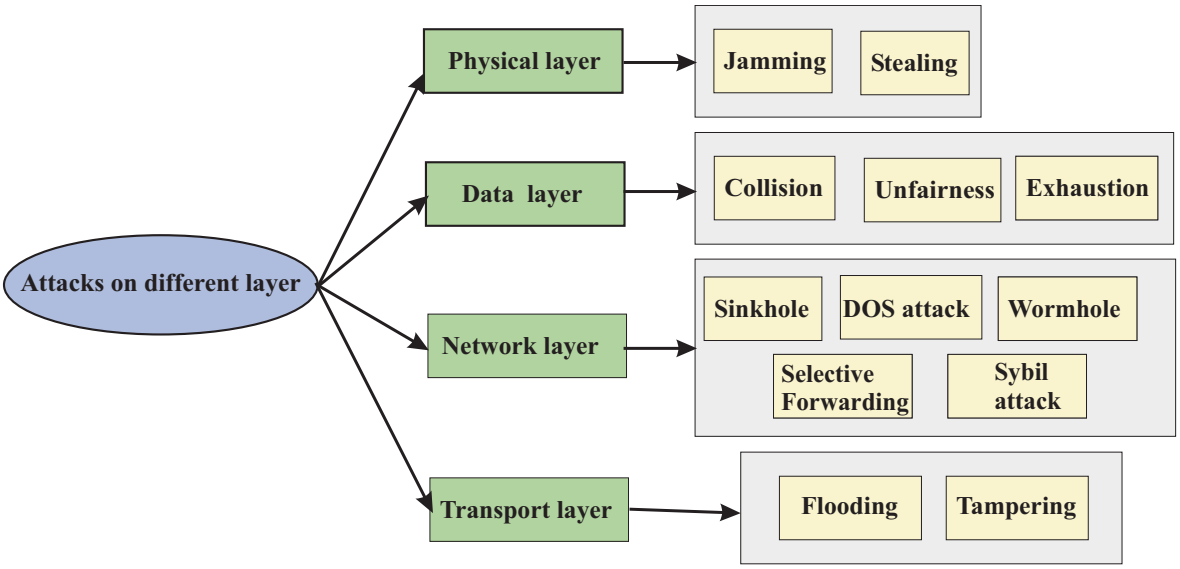

FIGURE 3.4: *Different types of attacks at each layer on localization in WSNs.*

algorithm for underwater WSNs. The process of secure localization is achieved into five phases: trust evaluation of beacon nodes, location estimation of unknown nodes, trust evaluation of reference node, reference node selection and again location estimation of unknown nodes. Firstly, the trust value of each beacon nodes is evaluated directly and indirectly. The location of unknown nodes is discovered by highly trusty nodes. Once the unknown nodes find its location act as reference nodes and compute its trust. Further, the reference nodes help to remaining unknown nodes for discovering their location. R. Garg et al. [162] introduced an efficient gradient descent scheme for secure localization in WSNs. Most of the localization approach depends on beacon nodes information for location estimation process. Any malicious nodes can tamper the information of beacon nodes and wrong location information is broadcasted by beacon nodes which affect the localization accuracy of the algorithm. This research work is achieved in two phases. In the first phase, the location information of beacon nodes is stored and the cost function is involved for that information. Secondly, the inconsistent information measurement is done by selective pruning which mitigates the effect of malicious nodes. The gradient descent approach performs well for in the

presence of non-coordinated attacks.

N. Yu et al. [163] proposed a BRS-based robust algorithm for secure Localization (BRSL) for WSNs. The proposed scheme is introduced to overcome the impact of malicious nodes on localization. The scheme is established into two phases. In the first phase, the trust values are evaluated based on beta distribution. Secondly, a weighted Tayloe-series least square method is utilized for computing the location of unknown nodes. The distance between beacon nodes and unknown nodes are identified on the basis of range-based approaches. T. Bao et al. [164] presented a game-based algorithm for secure localization for dynamic WSNs. The accurate localization in dynamic networks is more challenging than is static networks. Initially, sensor nodes adopt the grade of behavior based on time and space information in multiple hop communication. Further, the multi-risk level strategy is generated based on grade behavior and updated from time to time. Finally, sensor nodes select behavior grade with the highest value for getting the optimal solution. The proposed work enhances the cooperation capability among sensor nodes in the networks.

G. Kumar et al. [165] introduced a mutual authentication and insider node validation based secure localization for WSNs. All the sensor nodes are deployed with random mobility. The distribution of certificate to beacon nodes and unknown nodes is achieved by BS. BS is considered trusty in nature and provides the public key to all sensor nodes. After key distribution, the information of unknown nodes within the one-hop neighborhood is collected by beacon nodes. Further, the collected information is broadcasted to BS for localization process. The process of localization is performed by BS instead of beacon nodes. R. Garg et al. [166] introduced an iterative gradient descent based secure localization for mobile WSNs. In static network scenarios, the localization process is performed at the time of deployment of sensor nodes. But, it is necessary to keep track of the location of the node from time to time in mobile networks. Firstly, the cost function is evaluated based on the location information of bacon nodes. Further, the inconsistent measurements of nodes are obtained using selective pruning for accurate localization. T. Zhang et al. [167] proposed a Signcryption-based Secure Localization Scheme (SSLS) to ensure the integrity and

confidentiality in WSNs. The localization algorithm should be able to provide legal location information to neighbor nodes. The above problem is mitigated by using SSLS algorithm. Firstly, the beacon nodes signcrypts its location information and forward the information to neighbor unknown nodes. Each node verifies the beacon information using designcryption and received the information. Successful acceptance of information means the unknown nodes received the information correctly; otherwise, the location information is discarded. Further, the unknown nodes compute their location by using received location information.

H. Chen et al. [168] developed a DV-Hop based secure localization approach against wormhole attack in WSNs. In this work, a label-based scheme is used which discovers the forbidden link among sensor nodes. Firstly, all the beacon nodes are separated and labeled based on their geographical relationships under a wormhole attack. Further, all the beacon nodes are distinguished based on labeling results of obtained from neighbor beacon nodes. The abnormal link is eliminated among the labeled beacon nodes. X. Liu et al. [169] introduced an efficient DV-Hop secure localization for WSNs. In the first phase, the beacon nodes broadcast location information with authentication across the network. To mitigate the effects of capture attack, the weight of beacon nodes are introduced for the detection of attacks. S. Mukherjee et al. [170] introduced a novel ordinal Multi-Dimensional Scaling (MDS) using Round Trip Time (RTT) to prevent wormhole attack in WSNs. The ordinal MDS is used to discover the relationship between the observed distance and Euclidean distance between nodes. Firstly, the scaling of nodes is done based on the rank order of the disparity. The distance among nodes is computed using RTT based approach. Further, the malicious nodes are identified by applying filtering process and a list of suspected nodes is generated. Finally, the wormhole nodes are filtered from the normal nodes.

C. Chang et al. [171] presented a dynamic user authentication and key agreement scheme for secure localization in WSNs. The smart card is utilized for secure localization. The secure algorithm is completed in five phases: initialization, registration, login, authentication and key agreement and changing passwords. Four types of participants take part in the process such as sensor node, users, cluster head and BS.

Initially, BS generates its secret key and shared with cluster heads using a secured channel. Further, all data from sensor nodes are collected by cluster heads. If a user wants the information about the network, the registration process is necessary for BS to getting its identity or smart card. The smart card is used for the login process. This scheme is more suitable for application-oriented WSNs. T. Shu et al. [172] proposed a protected multi-lateral localization for pervasive. A malicious node can utilize the location information to attack the localization infrastructure and offer inaccurate localization. In this scheme, the positions of unknown nodes are computed without beacon nodes and the information id limited up to unknown node itself. It provides security to node exact location as well as the side information which is required for localization in WSNs. A secured Least-Squared Error (LSE) estimation is expressed for the determined linear system. Three privacy-preserving solutions are also introduced by incorporating leveraging with information-hiding and homomorphic encryption.
Y. Wei and Y. Guan [173] introduced a lightweight location verification secure localization algorithm for WSNs. Sensor nodes are deployed in hostile environments and localization schemes are mostly affected by various malicious activities. Therefore, the location of sensor nodes needs location verification in such types of networks. In this scheme, on-spot and in-region locations verification is introduced. In on-spot verification, it is verified whether the position of nodes are far from a specified distance or not. The abnormal locations of nodes are detected by using both algorithms. P. Bao and M. Liang [174] introduced a Threshold and Vote Security Localization for WSNs to resolve localization problems. The security of nodes locations is improved by using threshold and voting concepts. Threshold value improves the robustness of the location estimation process and ensures the safety of nodes against malicious activities. Y. Choi [175] introduced a temporal credential-based mutual authentication based secure algorithm with multiple password scheme in WSNs. Three-factor based security is achieved by using multiple passwords and a session key between user and sensor nodes are generated. The authentication process is achieved into five phases such as registration phase, login phase, authentication and key exchange phase, update the password phase and dynamic-node addition phase.

D. He et al. [176] proposed the new temporal-credential-based Mutual Authentication And Key Agreement (MAAKA) secure algorithm for WSNs security. The secure approach is accomplished into three phases i.e. registration phase, login phase and authentication with key agreement phase. This scheme provides security against off-line password guessing, user and sensor impersonation attack, modification attack, and user anonymity problem. O. AlFarraj et al. [177] presented an Activation Function-based Trusted Neighbor Selection (AF-TNS) for WSNs. AF-TNS approach works in two phases: trust evaluation and additive metric-based node evaluation. The trusted and un-trusted sensor nodes are identified by using random transigmoid function and trustworthiness of nodes are computed. The additive metric is evaluated using two parameters such as residual energy and trust. D. Chen et al. [178] introduced an attack-resistant RSS-based algorithm for secure localization based on L1 regularization in WSNs. Attack model is constructed by introducing unknown perturbations into a path loss model. The sparsity of malicious attacks on nodes by formulating secure localization as a nonlinearly constrained optimization problem. This problem is solved by introducing a projected gradient with Backtracking-Armijo algorithm. Comparison of these secure localization algorithms is shown in Table 3.5.

TABLE 3.5: *Literature-based on secure localization.*

Author(s)	**Secure Technique**	**Remarks**
G. Han et al. (2016) [161]	The collaborative secure algorithm	Only trusted beacon nodes are performed trilateration in localization. But, the algorithm cannot perform consistently when sensor nodes are mobile.
R. Garg, et al. (2012) [162]	Gradient Descent Approach	Improve localization accuracy with secure localization in the presence of an uncoordinated attack. The error-prone distance can affect the performance of the pruning stage.

N. Yu. et al. (2013) [163]	Beta-based Robust Secure Localization (BRSL)	The locations of unknown nodes are estimated using trustworthy beacon nodes. But, usage of range-based approaches makes it is costly and complex.
T. Bao et al. (2015) [164]	Game theory-based secure algorithm	The strategy level is generated based on the grade behavior of a node in mobile networks. The algorithm can be applied to other applications.
G. Kumar et al. (2017) [165]	Mutual authentication based secure localization	The proposed algorithm is suitable for mobile network scenarios. But, the external attacks are not emphasized.
G. Ravi et al. (2012) [166]	Efficient Gradient-based secure localization	The proposed algorithm is suitable for mobile network scenarios. External attacks can be considered.
T. Zhang et al. (2012) [167]	Signcryption-based secure localization	The location information is broadcasted using a signcryption scheme to ensure integrity. But, the algorithm cannot perform consistently when sensor nodes are mobile.
H. Chen et al. (2015) [168]	Secure DV-hop algorithm	The labeling of beacon nodes mitigates the impact of the wormhole. External attacks can be emphasized for the algorithm. Also applicable for packet loss-free transmission.
X. Liu et al. (2015) [169]	Efficient secure DV-hop localization	The proposed algorithm is suitable only for the static network. Mobility of networks can be incorporated.

S. Mukherjee et al. (2016) [170]	Wormhole attack detection algorithm	The wormhole nodes are identified by using ordinal MDS with RTT. But, the range-based approach makes the algorithm costly and complex. Also, internal attacks can be emphasized in the algorithm.
C. Chang, et al. (2016) [171]	Dynamic User Authentication and Key Agreement Scheme	The proposed algorithm ensured privacy using a smart card. The BS provides a secret to each cluster head. The trustworthiness of BS is required. Only suitable for static networks.
T. Shu et al. (2015) [172]	Multi-lateral privacy-preserving schemes ,	To improve localization efficiency with combinations of information hiding and homomorphic encryption. But, usage of range-based approaches makes it is costly and complex.
Y. Wei and Y. Guan (2013) [173]	Lightweight location verification algorithm	The location of nodes is verified by using on-spot and in-region algorithms. The proposed work can be emphasized for external attacks.
B. Peng and L. Ma (2011) [174]	Threshold and Vote Security Localization (TVSL)	The proposed algorithm ensures the security of node location using threshold and vote concept. But, this scheme can be affected by different malicious activities in the network.
Y. Choi (2017) [175]	Mutual Authentication with Multiple-Password Scheme	Communication and computational cost of the proposed scheme is high. Also, susceptible to off-line password attack.

D. He et al. (2015) [176]	Temporal Credential-Based mutual authentication scheme	Provide security against a different type of attacks i.e. user impersonation attack, the sensor node impersonation, and modification attack. Mobility of nodes can be considered.
O. Al-Farraj et al. (2018) [177]	An Activation Function-based algorithm	The trustworthiness of the nodes is computed based on trust and residual energy. But the proposed scheme can be extended for external attacks.
D. Chen et al. (2018) [178]	Attack resistant RSS-based algorithm	The proposed approach is constructed using RSSI approach. Therefore, the computational cost of the algorithm is high and complex in nature.

3.2.5 Literature-based on Blockchain

The localization process is more exposable to various attacks in WSNs due to the hostile environment in which it is operating with random deployment and dynamicity. These types of networks are also vulnerable to different kind of malicious activities which affects the operation of sensor nodes. Localization plays a crucial role to support various applications in WSNs, with non-trusted environment; it is difficult to discover precise locations of nodes in the presence of malicious nodes. Under these circumstances, blockchain technology in location estimation is introduced and is discussed below:

Z. Lu et al. [179] introduced a privacy-preserving trust model for secure Vehicular Ad hoc NETworks (VANETs) with blockchain technology. A Blockchain-based Anonymous Reputation System (BARS) is developed to establish a trust model for better privacy. The process of certificate distribution and revocation is accomplished by introducing the concept of proofs of presence and absence in the blockchain. The public

key of vehicles is used as pseudonyms during communication process without revealing actual identity of the users to maintain anonymity. The reputation of the vehicles is evaluated based on direct historical and indirect opinions to avoid distribution of the forged messages.

Z. Yang et al. [180] developed a decentralized trust management system using blockchain for VANETs. The proposed scheme evaluates the credibilities of broadcasted message in non-trusted environments. The vehicle validate the messages received from neighboring vehicles using Bayesian Inference Model and generates a rating for each vehicle which broadcast the message. Therefore, Road Side Units (RSUs) collects the rating forwarded by vehicles and compute the offsets trust values of each vehicle involved in communication. Further, each RSU add the trust values of the vehicles into block and generates a blockchain of trust offsets. A joint Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanism are utilized for mining process.

S. Kushch and F. Prietocastrillo [181] proposed a rolling blockchain technology for dynamic WSNs smart city. Rolling blockchain enables each smart card to participate in the network as a node. In this work, the blockchain consists of different parts with a limited number of blocks into in. the number of blocks in the chain depends on the parameters and capabilities of the devices. Once the memory of nodes is cleared, only last block of the chain is preserved which act as a genesis for new chain. R. J. ul Hussen Khan et al. [182] introduced a blockchain-based process for node recovery in WSNs. In this approach, the failure nodes are identified based on the node degree. Firstly, the cluster heads identified all the failure nodes based on their state. Secondly, the recovery process is performed for inactive nodes. Node recovery of nodes is achieved using a smart contract written in blockchain technology. S. Ali et al. [183] proposed an incentive-based blockchain model for secure data storage in WSNs. The approach provides an efficient and distributed storage mechanism by encrypting the data for privacy purposes. The private secure keys are exchanged using the elliptic curve Diffie-Hellman among the network nodes. T. H. Kim et al. [184] introduced a novel trust-based secure localization algorithm using the concept of blockchain technology. In this approach, the trust values of beacon nodes are evaluated using the

behavioral and data-based trust of nodes. Further, the composite trust values of nodes are computed and broadcasted towards BS. Finally, the blockchain of trust values is generated which ensures the reliability and security in localization.

T. M. Fernndez-Carams and P. Fraga-Lama [185] provided a survey of blockchain technology for Internet of Things (IoT). The paradigm of IoT gains much attention in the world due to advancement in technologies and smartness. These technologies require authentication, privacy, robustness against malicious activities, security and self-maintenance. These features can be provided by blockchain technology with cryptocurrency. The main contribution of this work is to emphasize the impact of blockchain on different application of IoT. Various challenges which affect the deployment of blockchain are also discussed.

E. F. Jesus et al. [186] presented a survey for secure IoT and stalker attack using blockchain technology. The main motive of this work is to offer the structure and operations of blockchain which provides the security and privacy to IoT. Also, IoT enables to deal with stalker attack using blockchain technology. Y. P. Lin et al. [187] introduced the application of blockchain technology for Information and Communications Technology-agriculture (ICT-agriculture). Blockchain technology can provide emerging and immutable data integrity to record management and environmental data for those who contribute to data management. A model based on blockchain is developed for ICT-agriculture which is used at the local and regional scale.

S. Goka and H. Shigeno [188] introduced a Distributed Management Trust model and Reward (DMTR) system for secure Mobile Ad-hoc NETworks (MANET). Due to the dynamic nature of MANETs, the management system should be highly secured to manage trust and reward. The proposed work can detect malicious nodes which drops the packets illegally effectively using blockchain. Blockchain technology manages the virtual credits in P2P networks. Mining nodes are arranged by DMTR that perform the managing task and cooperative mining is performed by nodes to speed up the process. A. Reyna et al. [189] presented various challenges and opportunities of blockchain integration with IoT. Blockchain is an emerging technology that transforms the way of sharing information. To secure the distributed systems without

any central authorities is an advancement that can change various industries. In this work, all the possible challenges of blockchain integration with IoT have discussed in order to potentially improve the IoT.

A. Lei et al. [190] introduced a blockchain-based certificate revocation scheme for VANet Security and privacy in vehicular communication is an important concern nowadays. The communication systems can be prevented from attacks and threats using the concept of certificate revocation. The structure of the network and distributed maintenance is efficiently achieved using blockchain for Certificate Revocation List (CRL) which diminishes the communication overheads and computational cost.

A. Dorri et al. [191] introduced a Memory-Optimized and Flexible BlockChain (MOF-BC) which ensures resilience against malicious activities and modification of the information in IoT. MOF-BC enables the user to add, remove or summarize their information and old data. Multiple keys are utilized to maintain the security of the information on different transactions. Generator Verifier (GV) is introduced by MOF-BC which is a signed hash for security. A simple transaction fee model and reward incentives mechanism is proposed for the users which encourage the user to optimize the memory consumption. Comparison of implementation of blockchain in different fields is shown in Table 3.6.

TABLE 3.6: *Literature-based on Blockchain technology.*

Author(s)	**Technique**	**Remarks**
Z. Lu et al. (2018) [179]	Blockchain-based Anonymous Reputation System	A blockchain-based privacy-preserving trust model is developed for VANETs.
Z. Yang et al. (2018) [180]	Trust management based on Blockchain	The trust offsets of each vehicle maintained in blockchain to form a decentralized consensus. Compromised RSU can generate a false rating about vehicles to affect the performance.

S. Kushch and F. Prietocastrillo (2018) [181]	Rolling based blockchain	The size of the blocks is kept limited and memory of nodes is cleared after a time interval.
R. J. ul Hussen Khan et al. (2020)[182]	Blockchain-based node recovery in WSNs	The recovery of failure nodes in the network is performed using blockchain technology.
S. Ali et al. (2020) [183]	An incentive-based data storage using blockchain technology In WSNs	The data storage mechanism is performed by using blockchain for more privacy and security in WSNs.
T.H. Kim et al. (2010) [184]	A novel trust-based secure localization using blockchain in WSNs	The trust values of beacon nodes are stored as a consensus using blockchain technology.
T. M. Fernandez-Carames and P. Fraga-Lama, (2018) [185]	Blockchain technology for IoT	The applications of blockchain technology in various domain of IoT are discussed.
E. F. Jesus et al. (2018) [186]	Survey of blockchain in IoT and stalker attack	This work contributes to the description of the structure of the block and operations of blockchain in IoT.

Y.-P. Lin et al. (2017) [187]	Blockchain model for ICT-agriculture	Blockchain technology is adopted for record data management and environmental data management.
S. Goka and H. Shigeno, (2018) [188]	DMTR scheme	The mining process is performed in a cooperative manner by nodes.
A. Reyna et al. (2018) [189]	Challenges of blockchain in IoTs	Different challenges of blockchain integration with IoTs have discussed to improve the applications of IoT.
A. Lei et al. (2018) [190]	Blockchain-based Certificate Revocation technique	The revocations of unsuitable certificates are achieved using blockchain technology for vehicular communication.
A. Dorri et al. (2019) [191]	Memory-Optimized and Flexible BlockChain	The memory consumption of user transactions is optimized by using blockchain technology.

CHAPTER 4

An Energy-Efficient localization for Mobile WSNs

4.1 Introduction

WSNs have been traced by services industry and academia since the 1990s. According to ONWORLD [192], the WSN Systems and Services industry is projected to develop in the order of roughly 46 billion US dollars, an increase about 500 million US dollars higher than the current stage of the industry. Numerous sensor devices are implemented in the specified region of interest formed a network called WSNs. These sensor nodes are capable of sensing any physical activities i.e. temperature, light, velocity, pressure, motion, and sound, etc. After observing the event, collected information is broadcasted to the Base Station (BS) either directly or intermediate nodes for further processing on data. The sensor nodes are self-configured and communicate with each other through a wireless medium. Due to resource constraint, each sensor node has limited resources in terms of limited power, memory and computational capability [80]. Therefore, sensor nodes have various restrictions and require optimum

design. Moreover, sensor nodes should be of low-cost, compact with long-life, robust, self-organizing and operable in harsh and remote environments [193].

Apart from that, the location of sensor nodes is very important in WSNs. There are number of applications that require precise locations of nodes to make sensed informative (e.g., fire detection, target tracking, and rescue operations, etc.) otherwise, the collected data will be worthless [29][36][50]. Hence, the process of estimating the locations of sensor nodes is called localization which plays a vital role in WSNs. Two types of sensor nodes such as beacon nodes and unknown nodes are deployed for sensing purpose in localization. The position of beacon nodes are prior known through GPS and the positions of unknown nodes are to be estimated using information from beacon nodes information. The process of localization is classified as direct and indirect localization. Direct approaches further divided into two categories: GPS based and manual configuration. In GPS-based localization, all the sensor nodes are equipped with GPS receivers for locating the sensor nodes [194]. The deployment and replacement of sensor nodes are done manually which is impractical or even impossible for remote and large areas in manual approach [195].

Indirect approaches are divided into two categories: range-based and range-free approaches. The former approach utilized point to point information for locating the sensor nodes and provides better accuracy of estimation. Angle of Arrival (AoA) [58], Time of Arrival (ToA) [73], Time Difference of Arrival (TDoA) [196], and Received Signal Strength Indication (RSSI) are the example of range-based approach [70]. The major researches done in range-free localization are summarized in Table 4.1 with their benefits and limitations.

TABLE 4.1: *Various improved DV-Hop algorithms with their benefits and limitations.*

Author(Year)	**Proposed algorithm**	**Benefits**	**Limitation**
D. Niculescu et al. (2003) [76]	Basic DV-hop	It is easy to implement and cost-effective	Gives poor localization accuracy

H. Chen et al. (2008) [197]	DV-hop with improvement	Improve localization accuracy and simple in implementation	Homogenous network scenario is considered
D. Liu et al. (2014) [198]	Weight-based DV-Hop	Reduce localization error by introducing weight factor	Mobility of network is not considered
G. Kumar et al. (2018) [52]	Improved DV-hop with MCDS	Both beacons as well unknown nodes are mobile in nature	CDS is only created using the degree of connectivity of beacon nodes
C. L. Tseng et al. (2017) [199]	Boundary Improved DV-Hop	Hop count is calculated on the basis of degree of irregularity	Mobility of network is not considered
L. Gui et al. (2015) [200]	Novel DV-hop	The locations of unknown nodes are estimated by selecting three appropriate beacon nodes	It has more computational cost and complexity
W. Z. Ping and C. Xuan (2015) [201]	DV-Hop and Steffensen method	Steffensen method is used to reduce localization error	The algorithm is highly complex and is only useful for a homogeneous network.
S. Dong et al. (2015) [111]	Multi-Probability DV-hop algorithm	Beacon nodes based on probability are recognized for localization and Bat algorithm is used to optimize localization results.	High computational cost and complexity. Also, mobility is not considered

J. Yu et al. (2012) [202]	Improved DV-hop algorithm	With the help of correction factor, the accuracy of estimation is improved.	Mobility of nodes is not considered
S. Kumar et al. (2014) [203]	Power-efficient range -free algorithm	Reduce energy consumption by eliminating one-way communication	High computational cost and complexity. Also, mobility is not considered
S. Kumar et al. (2013) [90]	Advanced DV-hop	For improving accuracy, the weight matrix is introduced	Mobility is not considered
Y. Hu and X. Li (2013) [204]	An improvement of DV-Hop	Location is estimated within threshold M hops	The algorithm is highly complex and is only useful for a homogeneous network.
C. Yu et al. (2016) [205]	Error correction and multi-hop algorithm	Localization errors are reduced by adding a correction factor	The algorithm is highly complex and is only useful for a homogeneous network.
G. Sharma et al. (2018) [113]	Improved DV-hop using TLBO	Localization accuracy is improved by introducing Teacher learning-based optimization	The algorithm is highly complex and is only useful for a homogeneous network.
G. Sharma et al. (2018) [97]	Modified energy-efficient	Improve the scalability and accuracy of the algorithm	High computational cost and complexity. Also, mobility is not considered

M. Mehrabi et al. (2017) [206]	Improved DV-hop based on evolutionary algorithms	Hop-size of the algorithm is modified using the Bat algorithm	The algorithm is highly complex and is only useful for a homogeneous network.
S. Kumar et al. (2017) [92]	Novel DV-hop algorithm	One way communication is eliminated to reduce energy consumption	The system has more complexity.
P. Singh et al. (2018) [207]	Localization based on PSO and HPSO	Single moving beacon nodes is utilized for location estimation with PSO and Hybrid PSO optimization	Only a single moving beacon node is considered
L. Cui et al. (2018) [208]	DV-Hop localization based on Differential Evolution	The localization process is achieved by applying Differential Evolution with hop count refinement	Mobility of network is not considered
F. Darakeh et al. (2018) [115]	Distributed cooperative-based range-free localization	Location of nodes is estimated by bounding box condition	The complexity of the algorithm is high
O. Cheikhrouhou et al. (2018) [209]	Hybrid DV-Hop localization with RSSI	All located node nodes operate as beacon nodes for the other nodes.	The computational cost of the algorithm is high due to introducing a range-based algorithm

R.R. Priyadarshini et al. (2018) [210]	Adelson-Velskii and Landis tree rotation clustering	The cluster head is elected based on MCDS	High computational cost and complexity

The computational cost of range-based approach is very high because special hardware is required for the location estimation process. On the other hand, range-free approaches estimate the positions of sensor nodes on the basis of connectivity and hop information among sensor nodes and Distance Vector-Hop (DV-hop), centroid method, Multi-Dimensional Scaling-MAP (MDS-MAP) and amorphous method are coming under the range-free algorithms [211]. These approaches are very popular due to its simplicity and low-cost devices but provide less accuracy of estimation in localization. However, range-free approaches are mostly known among researchers. One of the most widely available techniques is the DV-Hop algorithm and it was proposed by D. Niculescu [76].

In this algorithm, a multiplied hop-distance with hop-counts defines the range between unknown and beacon nodes. Finally, unknown node locations are estimated using the trilateration technique [212]. We have improved the DV-hop algorithm in this chapter in order to improve accuracy and decrease beacon nodes power usage. Several range-free location technologies have been used over the last two decades, but owing to its ease, costs and stabilization, DV-hop received more exposure. The DV-Hop algorithm can estimate the position of unknown nodes with the help of a few beacon nodes with compromised localization accuracy. In this chapter, the problems in existing localization algorithms are addressed by the proposed algorithm and tabulated in Table 4.2. The remaining parts of this chapter are organized as follows; proposed algorithm and the network model are given in section 4.2 and 4.3, respectively. Performance metrics and simulation results are discussed in section 4.4 and the conclusion of the chapter is given in section 4.5.

TABLE 4.2: *Addressing existing problem with proposed algorithm*

Existing Algorithm	**Existing Problems**	**Solution in proposed algorithm**
Basic DV-hop [76]	Gives least accuracy of the location and is only appropriate for uniform network	By improving the hop-size and mobility all sensor nodes are also considered to improve the precise location of the proposed algorithm .
A weighted DV-Hop [198]	All beacon nodes are necessary for localization process and only compatible with the stationary network for localization.	By constructing EECDS, the number of beacon nodes needed for localization is decreased.
DV-Hop with Steffensen iterative method [201]	Overall validation for mobile system is not taken into account.	All sensor devices (beacon nodes as well as unknown nodes) in the proposed system have a mobile aspect and the proposed algorithm encourages complete network mobility.
Modified energy efficient with TLBO [97]	As target nodes are act as a beacon nodes after localization, therefore consumes more energy for localization	As EECDS is maintained by beacon nodes so that remaining beacon nodes can be at rest and can be utilized later
Improved DV-hop with MCDS [52]	As beacon nodes are selected on the basis of maximum degree of connectivity, partial exhaustion of network exists	Beacon nodes for dominating set are elected by considering residual energy and maximum degree of connectivity

4.2 Proposed Algorithm

In WSNs, all the sensor nodes are having limited resources in terms of energy, communication, memory, and computation. Sensor nodes are operated by batteries which have limited energy for operation. The sensor nodes are deployed in aggressive environments where human intervention is almost impossible so that replacement or recharging of these batteries is even not possible. In the proposed algorithm, beacon nodes are more privileged in terms of resources as compared to unknown nodes. These resources of beacon nodes must be utilized efficiently and optimally to prolong the network lifetime. Therefore, only one-hop neighbor unknown nodes of beacon nodes are considered in the proposed algorithm. For energy efficiency, some of the beacon nodes are selected based on their residual energy and degree of connectivity with one-hop neighbor unknown nodes to construct a Dominating Set (DS) called Energy-Efficient Connected Dominating Set (EECDS). The process

of EECDS construction is distributed in the manner as explained in subsection 4.2.2 and it repeats itself periodically due to dynamic network scenario. The size of EECDS affects the performance in terms of energy and it happens because more beacon nodes in EECDS consume more energy. Therefore, to minimize the size of EECDS, the process of pruning is applied on EECDS and Minimum EECDS (MEECDS) is achieved as a backbone of the network. The beacon nodes which are not included in MEECDS will be utilized for localization in a later stage. The location of unknown nodes is estimated by a group of beacon nodes called localizing unit and at least three beacon nodes are required in backbone/MEECDS to perform trilateration for estimating the coordinates of unknown nodes. Moreover, the localization error is also affected when three beacon nodes in the localizing unit are collinear that means they may not have an area of intersection. In such a situation, localization may not be possible. To solve this problem, the Degree of Collinearity (DCL) is introduced in the proposed algorithm. Only those beacon nodes will participate in the localization process which is not collinear. After collinearity check, the locations of unknown nodes are estimated using MEECDS beacon nodes. In the proposed algorithm, the beacon nodes and unknown nodes are deployed in a random scenario and represented with black and grey color respectively as shown in Figure 4.1. The proposed algorithm is completed in 5 steps and is described in the following subsections:

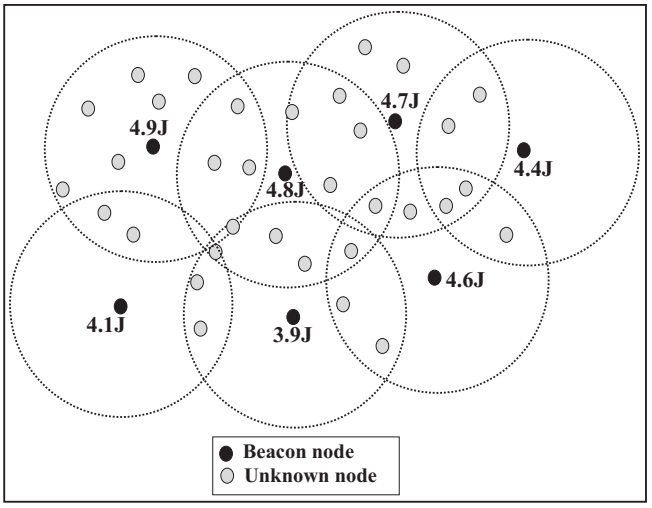

FIGURE 4.1: *Random deployment of unknown nodes and beacon nodes.*

4.2.1 Selection Parameter for EECDS

The residual energy and maximum degree of connectivity are calculated for each beacon node for constructing EECDS and selection parameter is a factor which makes a decision for dominating set All the possible state for selection parameter are shown in Table 4.3. Selection parameter is computed on the basis of residual energy and

TABLE 4.3: *Different possible state for selection parameter*

Cases	E_r**(Residual Energy of Nodes)**	D^{conn} **(Degree of connectivity)**	P**(Selection Parameter)**
1.	$If E_j^r = 0$	$\forall D_j^{conn}$	$P_j = 0$
2.	$\forall E_j^r$	If $D_j^{conn} = 1$	*Pj=0*
3.	If $E_j^r = E_i^r$	and $D_j^{conn} = D_i^{conn}$	$P_j = P_i$
4.	If $E_j^r > E_i^r$	and $D_j^{conn} \geq D_i^{conn}$	$P_j > P_i$
5.	If $E_j^r \geq E_i^r$	and$D_j^{conn} > D_i^{conn}$	$P_j > P_i$
6.	If $E_j^r \neq E_i^r$	and $D_j^{conn} \neq D_i^{conn}$	$P_j \neq P_i$

connectivity of beacon nodes. Connectivity of beacon nodes is nothing but the total number of unknown nodes within the one-hop neighborhood. Selection parameter is computed using Equation 4.1:

$$P_j(T) = E_j^r(T) \times log(D_j^{conn}(T)) \tag{4.1}$$

where $P_j(T)$ represents selection parameter of node j at time T, $E_j^r(T))$ is the residual energy of node j at time T and $D_j^{conn}(T)$ represents the degree of connectivity of node j at time T with the unknown nodes. Each beacon node computes its node degree for EECDS construction according to algorithm 1. The degree of connectivity for each beacon node is calculated using the following Equation 4.2:

$$D_j^{conn}(b) = \sum_{b \in N, b \neq u} (hop_{b,u} = 1) \tag{4.2}$$

$$E_j^{CT}(k, D_{(b,u)}^{est}) = (E_j^{tx}(k, (D_{(b,u)}^{est})^2) + E_j^{adct} + E_j^{os} + E_j^{rx}(k) + E_j^{adcr} + E_j^{idle} + E_j^{sleep}) \tag{4.3}$$

$$h_j^t = \sum_{i \neq j} h_{ij}^t \tag{4.4}$$

$$E_j^T = E_j^{CT} \times h_j^t \tag{4.5}$$

where $E_j^{CT}(k, D_{(b,u)}^{est})$ = total energy consumption of j^{th} beacon node during k bit packets for one-hop; E_j^{tx}= energy consumption for transmission; E_j^{os}= consumption of energy for on/off state; E_j^{adct}= energy consumption for analog and digital circuitry of the transmitter; E_j^{rx} = energy consumption for the receiver; E_j^{adcr}=energy consumption of analog and digital circuitry of the receiver; E_j^{idle}= consumption of energy during the idle state; E_j^{sleep}= consumption of energy during the sleep state. h_{ij}^t= number of hop-count between node i and j at any instant; h_j^t= total number of hop-count between j^{th} beacon nodes to all nodes; E_j^T= total energy consumption of j^{th} beacon nodes after information transmission to whole network. Consider $E_j^{initial}$ is the initial energy of each beacon node, therefore we can compute the residual energy denoted by E_j^r using the following Equation 4.6:

$$E_j^r = E_j^{initial} - E_j^T \tag{4.6}$$

It can be seen from Equation 4.3 that the energy consumption of beacon nodes depends on the distance between beacon node b and unknown node u, more the distance more the energy consumption. In the proposed algorithm, a total of six possible cases of selection parameter are considered on the basis of beacon residual energy and degree of connectivity. In the first case, the residual energy of the beacon node is considered zero that means the same node cannot be considered in the construction process of EECDS. The beacon nodes are assumed to be located at the border of sensing field in case 2 and again the node cannot be considered as a member of EECDS. The beacon nodes with the least connectivity value 1 are most likely located at the border of network. The degree of connectivity of beacon nodes helps to elect the most appropriate unknown node. Both the parameters such as residual energy and degree

of connectivity of beacon node i and j are considered equivalent, for that situation both nodes can become a member of EECDS. Cases 4 and 5 explained in Table 4.4 with the help of example depicted in Figure 4.2. It is observed that node 2 is more superior to node 1 because $E_2^r > E_1^r$ for the same connectivity $D_2^{conn} = D_1^{conn}$. Case 6 represents $E_j^r > E_i^r$ and $D_j^{conn} < D_i^{conn}$.

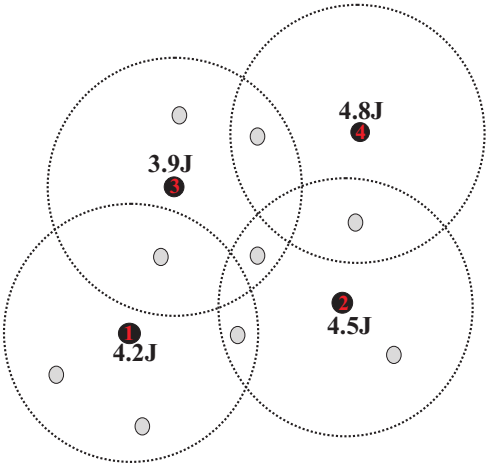

FIGURE 4.2: *Example of selection parameter with 4 nodes.*

TABLE 4.4: *Values of selection parameter for different beacon nodes*

Node No.	**Residual Energy** E^r	**Degree of node** (D^{conn})	**Selection parameter (P)**
1	4.2 J	4	2.52
2	4.5 J	4	2.7092
3	3.9 J	4	2.348
4	4.8 J	2	1.44

4.2.2 EECDS construction

Total N sensor nodes are randomly deployed with random mobility with a set of M beacon nodes and n unknown nodes that are represented by $(b_1, b_2, b_3, ..., b_M)$ and $(u_1, u_2, u_3, ..., u_n)$ respectively.

$$N = M + n$$

For constructing the EECDS, firstly the beacon nodes are prioritized based on their residual energy and degree of connectivity. The beacon node with the highest value of selection parameter is selected as a member of EECDS. The process of EECDS construction is repeated until either all the beacon nodes become the member of EECDS or all the one-hop neighbor of each beacon nodes are covered by a member of EECDS. From Figure 4.2, it is perceived that beacon node $1, 2, 3$ have the same degree of connectivity but their residual energy is different. Therefore, beacon node 2 is elected as a member of EECDS in the first iteration due to its highest value of selection parameter. Beacon node $1, 3$ and 4 may become the members of dominating set if it attains a favorable selection parameter. The procedure of EECDS construction is explained in algorithm 1.

Algorithm 1 EECDS construction

1: Deployment of M beacon nodes $(b_1, b_2, b_3, ..., b_M)$
2: Deployment of n unknown nodes $(u_1, u_2, u_3, ..., u_n)$
3: Beacon nodes broadcast information like (id_i, h_i, x_i, y_i) to unknown nodes
4: Unknown nodes maintain a about beacon nodes information
5: Create an empty dominating set (EECDS)
6: Compute residual energy E^r for each beacon node (b_i)
7: Calculate the maximum degree of nodes (D^{conn}) within one-hop neighboured unknown nodes for each beacon nodes b_i
8: Compute $P(b_i)$ that is selection parameter for EECDS
9: Compute Maximum $P(b_i)$ and returns the beacon nodes (b_p) whose parameter value is maximum
10: Store b_p in EECDS
11: Repeat the process until all beacon nodes become a member of EECDS or all unknown nodes $(u_1, u_2, u_3, ..., u_n)$ are covered by any beacon node
12: $EECDS(b_i \geq 3)$

4.2.3 Pruning of EECDS

The pruning method is initiated after the construction of EECDS to minimize the size of EECDS affecting the efficiency of localization algorithms. The size of EECDS must be small for the efficiency of virtual backbone of network. The pruning procedure will minimize the number of beacon nodes and allow unknown nodes more

connective. Trilateration method started after pruning and at least three beacon nodes are required to perform localization. All pruning steps are shown in algorithm 2. All unknown nodes are covered by EECDS beacon nodes $1, 2, 3$ and beacon node 4 is eliminated from EECDS as shown in Figure 4.2. This dominating set is called Minimum Energy Efficient Connected Dominating Set (MEECDS).

Algorithm 2 Pruning of EECDS

1: Apply EECDS as an input
2: If $EECDS(b_i \geq 3)$ //then consider minimum degree beacon nodes M[min]
3: If $M[min] \subset M[b_1] \cup M[b_2] \cup ....M[b_n]$, //check that all nodes of M[min] is covered by remaining beacon nodes
4: EECDS= EECDS-M[min], //If M[min] nodes are covered by remaining nodes then eliminate that node from EECDS.
5: Iteratively prune after eliminating min from EECDS
6: Returns MEECDS

4.2.4 Selection of Beacon nodes on the basis of collinearity

Further, after getting MEECDS, one significant parameter of collinearity among beacon nodes is introduced to improve the performance of algorithm. After pruning process, unknown nodes get localized with the help of three or more than three beacon nodes. Generally, more beacon nodes give precise locations of unknown nodes and more accuracy of estimation. However, due to the random and dynamic topology relationship between beacon nodes and unknown nodes, affects the performance of localization. When three beacon nodes lie on a straight line that means the location estimation process is achieved with more error because the intersection point between nodes could be far from the actual location of nodes. The concept of collinearity is explained where three beacon nodes almost lie on a straight line as shown in Figure 4.3. The location of unknown node U cannot be estimated precisely because two intersection points are given by three beacon nodes and two locations of unknown node U may be computed as U or U^*. A flowchart for the proposed algorithm is shown in Figure 4.4.

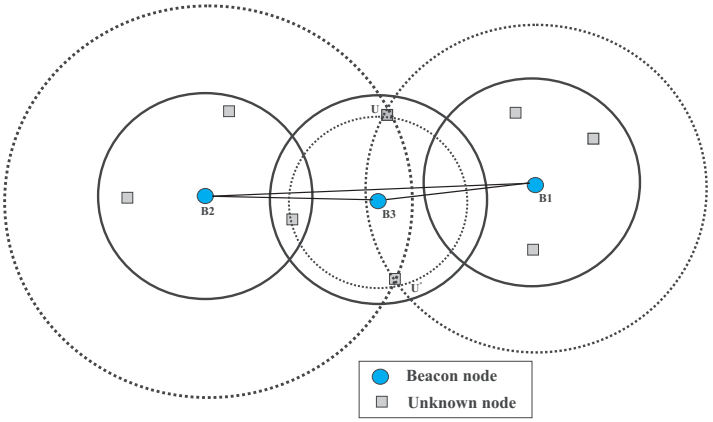

FIGURE 4.3: *Concept of collinearity among beacon nodes.*

4.2.4.1 Condition of collinearity

The area formed by three beacon nodes is zero when these nodes lie on a straight line or are collinear. Therefore, for precise location estimation, three non-collinear beacon nodes are highly desirable. The area for these points can be calculated by Equation 4.7:

$$\Delta = 1/2 \begin{bmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{bmatrix} \tag{4.7}$$

where Δ represents the area formed by three beacon nodes and (x_1, y_1), (x_2, y_2) and (x_3, y_3) represent to the coordinates of beacon nodes. Degree of Collinearity (DCL)is represented by Equation 4.8:

$$\zeta = \begin{cases} 0 & collinear \\ \Delta & else \end{cases} \tag{4.8}$$

In the aforementioned equation, ζ is the value of DCL and the value of area is computed using Equation 4.7. The condition of DCL does not allow to collinear beacon nodes to take part in localization. All the steps for DCL are shown in algorithm 3.

Algorithm 3 Collinearity check for MEECDS

1: Apply MEECDS as an input
2: Initially $\Delta_i = 0$, //(Area of intersection between three nodes)
3: Initialize $DCL = 0$, //(Empty set of Degree of collinearity)
4: $\Delta_i = [(b_{i-2} - b_{i-1)} + (b_{i-1} - b_i)]$, //(Calculate area of intersection between MEECDS beacon nodes)
5: $DCL = \Delta_i$
6: If Δ_i is zero for any three beacon nodes then again construct MEECDS using algorithm 2, otherwise
7: Perform trilateration for estimating the location of unknown nodes

4.2.5 Refinement of Average Hop Distance

As we know, more localization errors are accumulated in the DV-Hop localization algorithm due to poor distance estimation. The process of distance estimation mostly depends on the hop-size distance of beacon nodes and number of hop-count among sensor nodes. Therefore, to minimize the localization error, a correction factor is introduced in the proposed algorithm for modifying the hop-size distance of beacon nodes.

4.2.5.1 Calculation of Correction factor

In the first step of the DV-Hop algorithm, each sensor node accumulates minimum hop-count information between itself and other sensor nodes. The actual distance between beacon nodes can be computed using Equation 4.9:

$$D_{ij}^{act} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \quad where\, i \neq j \tag{4.9}$$

(x_i, y_i) and (x_j, y_j) represent the coordinates of beacon nodes i and j respectively and (D_{ij}^{act}) is the actual distance between beacon node i and j. The estimated distance among beacon nodes is computed by multiplying the average hop distance and hop-count between them. Consider D_{ij}^{est} is the estimated distance among beacon nodes i

and j, and it is determined by Equation 4.10.

$$D_{ij}^{est} = AverageHopDistance_i \times h_{ij}, \quad where\, i \neq j \tag{4.10}$$

The difference between D_{ij}^{est} and D_{ij}^{act} is called distance error denoted by D_{ij}^{e} and calculated by using Equation 4.11, where h_{ij} represents the number of hop-count between nodes. The difference between D_{ij}^{est} and D_{ij}^{act} is called distance error denoted by D_{ij}^{e} and calculated as:

$$D_{ij}^{e} = (D_{ij}^{est} - D_{ij}^{act}) \tag{4.11}$$

The D_{ij}^{e} of beacon node i can be used to calculate the correction factor of beacon node i and denoted by φ_i. The correction factor is calculated by Equation 4.12:

$$\varphi_i = \frac{\sum_{i \neq j} D_{ij}^{e}}{\sum_{i \neq j} h_{ij}} \tag{4.12}$$

The correction factor is added to the average hop distance for improving localization accuracy. The distance between beacon nodes and unknown nodes is calculated using by Equation 4.13:

$$D_{ui} = (AverageHopDistance_i + \varphi_i) \times h_{ui} \tag{4.13}$$

where h_{ui} is the hop count between unknown node u and beacon node i. After calculating the distance, the position of unknown nodes is calculated by using the trilateration method. Let the coordinates of beacon node i and unknown node u is (x_i, y_i) and (x_u, y_u), respectively. After calculating the distance, the position of unknown nodes

is calculated by using the trilateration method as following:

$$\begin{cases} (x_u - x_1)^2 + (y_u - y_1)^2 = d_{u1}^2 \\ (x_u - x_2)^2 + (y_u - y_2)^2 = d_{u2}^2 \\ . \\ . \\ (x_u - x_k)^2 + (y_u - y_k)^2 = d_{uk}^2 \end{cases} \tag{4.14}$$

Equation 4.14 can be represented in matrix form $AP_u = B$ as follows:

$$A = -2 \times \begin{pmatrix} x_1 - x_k & y_1 - y_k \\ x_2 - x_k & y_2 - y_k \\ . & \\ . & \\ x_{k-1} - x_k & y_{k-1} - y_k \end{pmatrix} \tag{4.15}$$

$$B = \begin{pmatrix} d_{u1}^2 - d_{uk}^2 + x_1^2 + x_k^2 - y_1^2 + y_k^2 \\ d_{u2}^2 - d_{uk}^2 + x_2^2 + x_k^2 - y_2^2 + y_k^2 \\ . \\ . \\ . \\ d_{u(k-1)}^2 - d_{uk}^2 + x_{(k-1)}^2 + x_k^2 - y_{(k-1)}^2 + y_k^2 \end{pmatrix} \tag{4.16}$$

$$P_u = \begin{pmatrix} x_u \\ y_u \end{pmatrix} \tag{4.17}$$

At last, the position of the unknown nodes is obtained by applying the least square method shown in Equation 4.18.

$$P_u = (A^T A)^{-1} A^T B \tag{4.18}$$

4.3 Network Model

All the simulations of proposed algorithm are performed using Matrix laboratory (Matlab) 2017. For the simulations, deployments of beacon nodes and unknown nodes are considered mobile in nature with varying transmission range. The network scenario is modeled as an undirected graph. The network is assumed dynamic where all nodes including beacon nodes and unknown nodes are mobile in nature with different transmission range. WSNs are modeled as undirected graph $G(N; E)$, where N denotes the total sensor nodes (both beacon nodes and unknown nodes) and E denotes the link set.

Definition 1*: A DS for a graph $G(N, E)$ is defined as a subset of N in such a way that all unknown nodes in N are one-hop neighbor of at least one beacon node in DS . The beacon nodes in DS are called dominators.*

Definition 2*: An EECDS of G is a dominating set which induces a connected subgraph of G. In graph G, The non-EECDS unknown nodes within one-hop neighbor are called dominates.* Considering b as beacon nodes and u as unknown nodes $((b, u) \in N)$ and $((b, u) \in E)$ only if b and u are lies within one hop neighboured transmission range. The dominating set of the graph G is $EECDS \subseteq N$ in such that EECDS consists of only beacon nodes and its one-hop neighbor unknown nodes covered by at least one member of EECDS. The MEECDS for graph G can be defined as a $MEECDS \subseteq N$ in such a way that MEECDS only have a minimum number of beacon nodes and all unknown are covered by any member of EECDS.

4.3.1 Design parameter

In the proposed algorithm, various design parameters are considered in terms of transmission range, residual energy, and mobility of nodes. These parameters are explained as follows:

1. Transmission Range:

Variable range of transmission is considered in the different application scenario. The

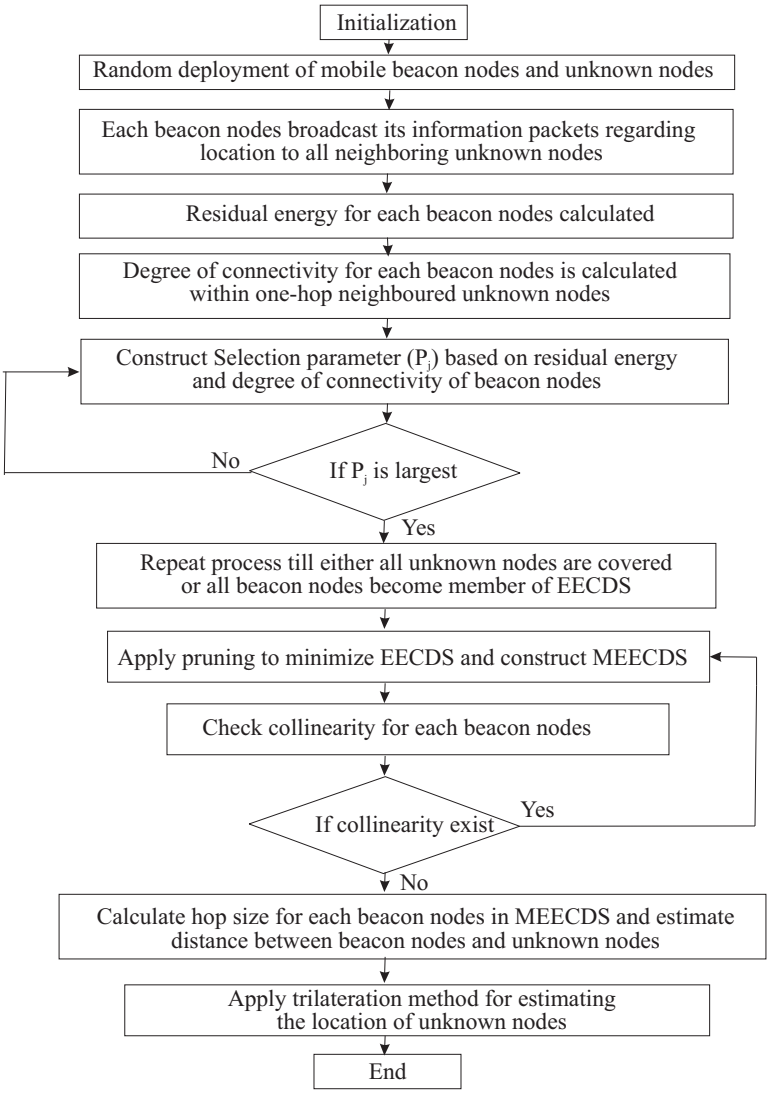

FIGURE 4.4: *Flowchart for the proposed algorithm.*

transmission range varies from maximum to minimum range as network scenario is dynamic in nature. The transmission range (T_R) is computed by Equation 4.19.

$$T_R = (T_{max} - 1) + Random(0, 1) \times [(T_{min} - 1) - (T_{max} - 1)] + 1 \tag{4.19}$$

where T_{min} $(15m)$ and T_{max} $(60m)$ are the minimum and maximum range of transmission respectively.$Random(0, 1)$ is a random function having value in between the range of 0 to 1.

2. Mobility of nodes:

Beacon nodes and unknown nodes are deployed with random mobility. For computing the direction of movements, relative mobility of nodes is computed. It states that whether any sensor nodes are coming closer or going far away from the particular sensor nodes in network. The relative mobility ($RM_{i,j}$) between sensor node i and j are computed at any time t by the following Equation 4.20:

$$RM_{ij} = d_{ij}^{t} - d_{ij}^{(t-1)} \tag{4.20}$$

where d_{ij}^{t} and $d_{ij}^{(t-1)}$ represent the distance between node i and node j at time t and $(t-1)$ respectively and are computed as follows:

$$d_{ij}^{t} = \sqrt{(x_i^t - x_j^t)^2 + (y_i^t - y_j^t)^2} \tag{4.21}$$

$$d_{ij}^{t-1} = \sqrt{(x_i^{t-1} - x_j^{t-1})^2 + (y_i^{t-1} - y_j^{t-1})^2} \tag{4.22}$$

where (x_i^t, y_i^t) and (x_i^{t-1}, y_i^{t-1}) are the coordinates of node i at time t and $(t-1)$ respectively, and (x_j^t, y_j^t) and (x_j^{t-1}, y_j^{t-1}) are the coordinates of node j at time t and $(t-1)$ respectively.

4.3.2 Performance Evaluation

All the sensor nodes are deployed in the two-dimensional area of $100 \times 100m^2$ with dynamic network scenario. Red star nodes represent the beacon nodes and black dots are unknown nodes in Figure 4.5. The simulated results of proposed algorithm are evaluated in terms of localization error with respect to various performance metrics such as beacon node ratio, nodes density, communication range, and sensing field. The simulation parameters are shown in Table 4.5.

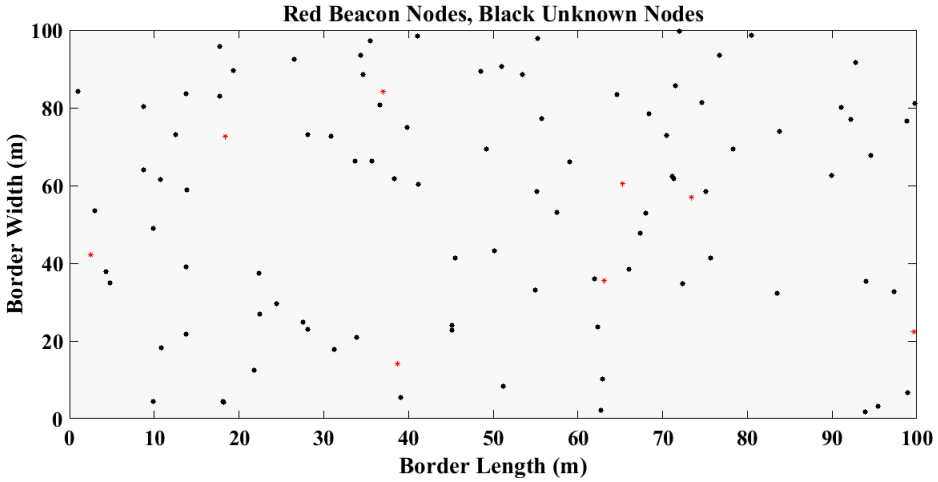

FIGURE 4.5: *Deployment of sensor nodes.*

TABLE 4.5: *Simulation parameters*

Parameters	**Value of parameters**
Sensing area	100*100 m^2
Transmission range	15-60 m
Network topology	Random way point mobility
Speed	0-20 m/s
Maximum iteration	500
Initial energy ($E_{initial}$)	5 J
Node density	100
Beacon node ratio	5-25%

4.3.3 Simulation performance metrics

For performance evaluation, the comparison of simulated results is prepared with other existing algorithms by considering similar network scenario on the basis of different performance parameters. The parameters considered for the results as follows: *1. Localization Error (LE):*

$LE(m)$ of the algorithm is defined as difference between actual coordinates and estimated coordinates of the nodes and it is computed using the following equation:

$$\xi = \sqrt{(x_i^e - x_i^a)^2 + (y_i^e - y_i^a)^2} \tag{4.23}$$

where (x_i^e, y_i^e) and (x_i^a, y_i^a) are the estimated coordinates and true coordinates of sensor nodes respectively.

2. Average Localization Error (ALE):

ALE ALE (m) represents the ratio of localization error to the total number of sensor node. *ALE* can be expressed as:

$$\phi = \frac{\sum_{i=M+1}^{N} \sqrt{(x_i^e - x_i^a)^2 + (y_i^e - y_i^a)^2}}{(N-M)} \tag{4.24}$$

3. Root Mean Square Error (RMSE):

RMSE defined as the mean square root of squared difference of estimated coordinates and true coordinates of the sensor nodes and computed as follows:

$$RMSE = \sqrt{\frac{\sum_{i=M+1}^{N} (x_i^e - x_i^a)^2 + (y_i^e - y_i^a)^2}{(N-M)}} \tag{4.25}$$

4.4 Simulation Results

In the proposed algorithm, the performance of work is compared with Basic DV-hop [76],Weighted DV-Hop [198],Steffensen based DV-Hop [201] and Modified DV-Hop [97]under similar network scenario. The performance is evaluated by varying various parameters such as beacon nodes ratio, sensing field, node density, and communication range.

4.4.1 Localization Error of unknown nodes

The simulated results of the proposed work are tabulated in Table 4.6 in terms of maximum, minimum and average localization errors. For the simulation, 100 sensor nodes are randomly deployed in the sensing field of $100 \times 100m^2$ with 5 to 20 % beacon nodes. It is observed from Table 4.6 that the proposed algorithm outperforms in terms of localization accuracy as compared to existing ones. As expected, localization error decreases with an increasing number of beacon nodes.

TABLE 4.6: *Localization error comparison with different number of beacon nodes*

Localization Algorithm	**No. of Beacon nodes**	**Max. localization error (meter(m))**	**Min. localization error (meter(m))**	**ALE (meter(m))**
Basic DV-hop [76]	5	32.213	2.154	26.643
	10	31.105	2.004	25.166
	15	29.246	1.987	23.489
	20	28.015	1.235	21.450
Weighted DV-Hop [198]	5	29.520	1.117	23.653
	10	28.403	1.761	21.314
	15	26.233	1.245	21.104
	20	25.058	1.145	20.423
Steffensen based DV-Hop [201]	5	26.156	0.419	20.986
	10	26.203	1.019	19.164
	15	24.563	1.024	18.164
	20	24.103	0.986	17.080
Modified DV-Hop [97]	5	22.146	0.480	14.116
	10	21.018	0.532	13.145
	15	20.078	0.356	12.225
	20	20.136	0.312	11.153
Proposed Algorithm	5	20.148	0.119	10.034
	10	19.456	0.246	9.897
	15	19.246	0.173	9.047
	20	19.563	0.101	7.567

4.4.2 Effect of Transmission range on MEECDS size

The impact of transmission range on size of MEECDS is demonstrated in Figure 4.6 by varying number of unknown nodes. From the simulated results it is observed that as the transmission range of nodes increases, the size of MEECDS decreases efficiently. It happens due to the requirements of beacon nodes decrease for localization as the transmission range increases, but a minimum of three beacon nodes is required to perform localization. Total 20 to 100 unknown nodes are deployed in the sensing field for observing the effect of transmission range on MEECDS size.

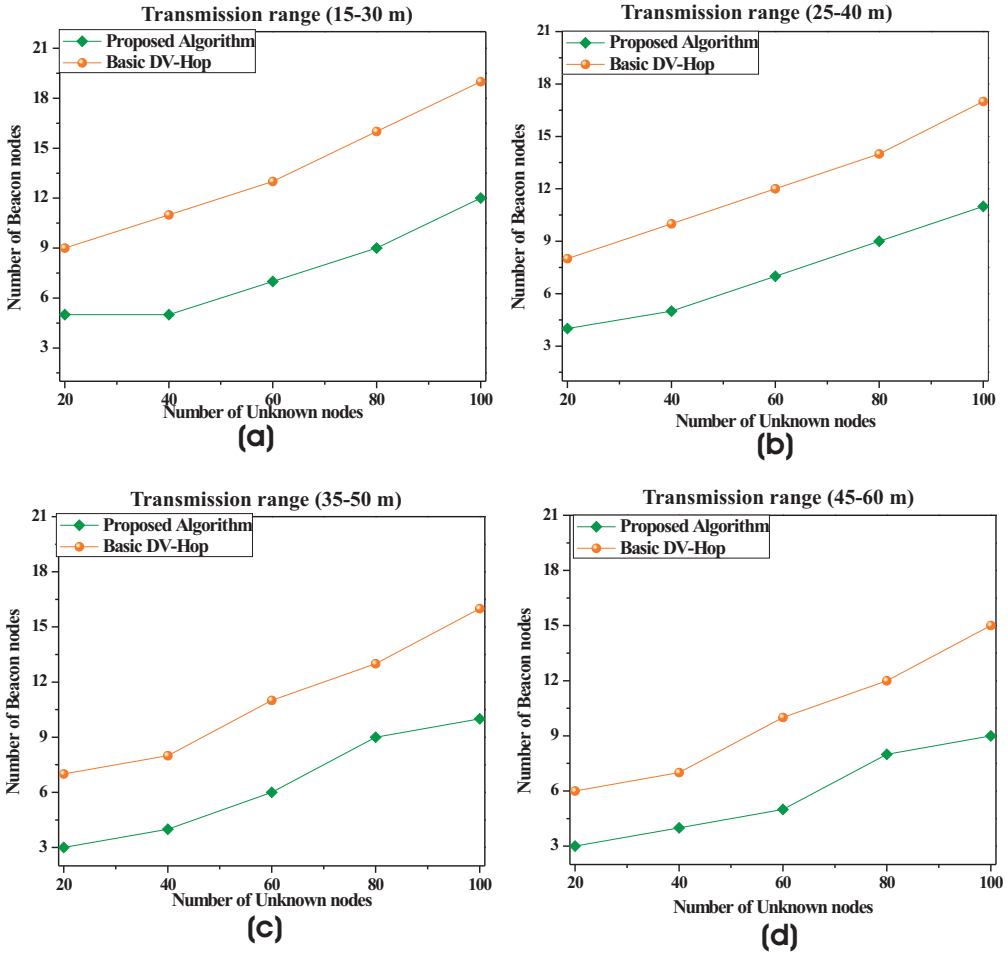

FIGURE 4.6: *Number of beacon nodes for localization with different Transmission range.*

4.4.3 Effect of Node Density on Localization error

To evaluate the impact of node density on ALE, the communication range and unknown nodes are varied from $15 - 60m$ and 20 to 100 respectively with 20% beacon nodes. The simulated results are demonstrated in Figure 4.7 and it is observed from the simulated results that average localization error decreases as the density of sensor nodes increases in network. We observed that the localization accuracy of all algorithms is affected significantly by varying nodes density. It happens due to the fact that, the network becomes more connected with more sensor nodes and unknown nodes gather more location information for estimating their locations. Also, hop-count between nodes decreases as the transmission range increases which gives

accurate hop-size distance. The proposed algorithm performs effectively as compared to other existing algorithms.

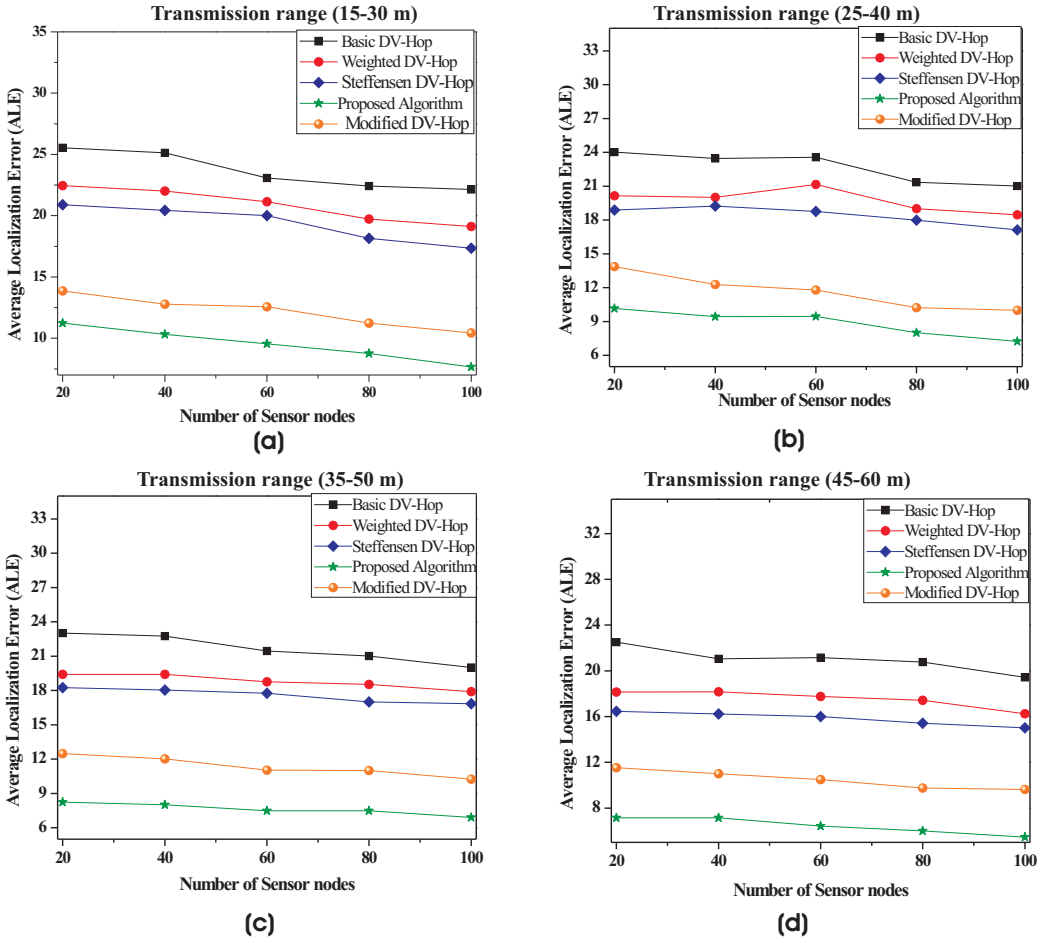

FIGURE 4.7: *Effect of node density and transmission range on ALE.*

4.4.4 Impact of the ratio of beacon nodes on localization error

To analyze the impact of the ratio of beacon nodes on ALE, the simulation is conducted with 100 sensor nodes having a variable transmission range $15 - 60m$ with varying beacon ratio from 5% to 25%. The simulated results are illustrated in Figure 4.8 and it is observed from the results that the ALE for all algorithms decreases as the number of beacon nodes increases in network. It happens because hop-count

between beacon nodes and unknown nodes decrease with the increasing total number of beacon nodes. A small hop-count gives more precise localization to unknown nodes. The proposed algorithm provides more accurate localization as compared to existing ones.

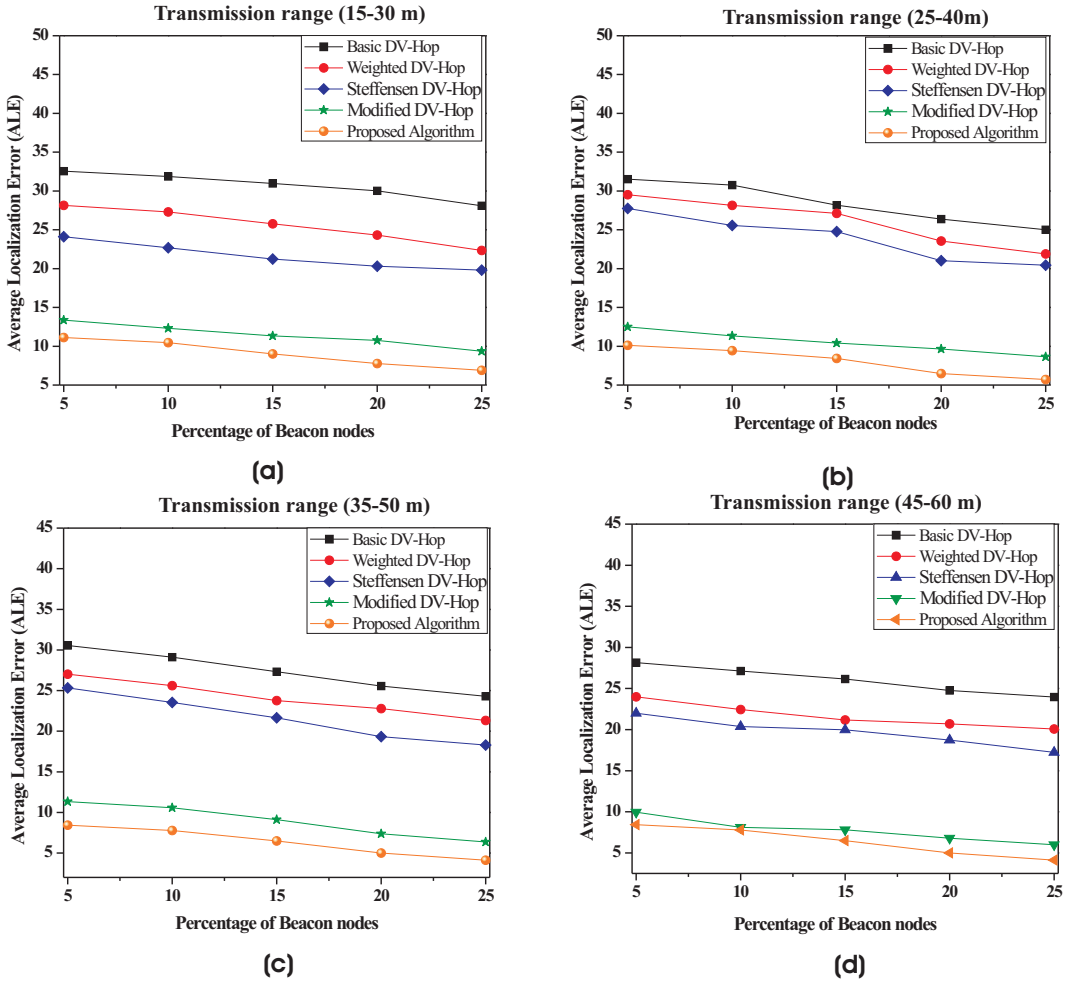

FIGURE 4.8: *Effect of ratio of beacon nodes on ALE.*

4.4.5 Effect of sensing area on Localization error

To evaluate the performance of algorithms, the sensor nodes are deployed in the variable sensing field from 100×100 to $400 \times 400m^2$. For the simulation, 100 sensor nodes are deployed with transmission range $30m$ and 20% beacon nodes. The simulated results are demonstrated in Figure 4.9 in which SF1 represents $100 \times 100m^2$,

SF2 represents $150 \times 150m^2$ and so on up to $400 \times 400m^2$ represented by SF7. It is determined from Figure 4.9 that increasing sensing field increases the ALE of all algorithms significantly. It happens due to network becomes less connective when the sensing field increases. The proposed algorithm gives more precise locations of unknown nodes as compared to other existing algorithms which prove the effectiveness of the proposed algorithm.

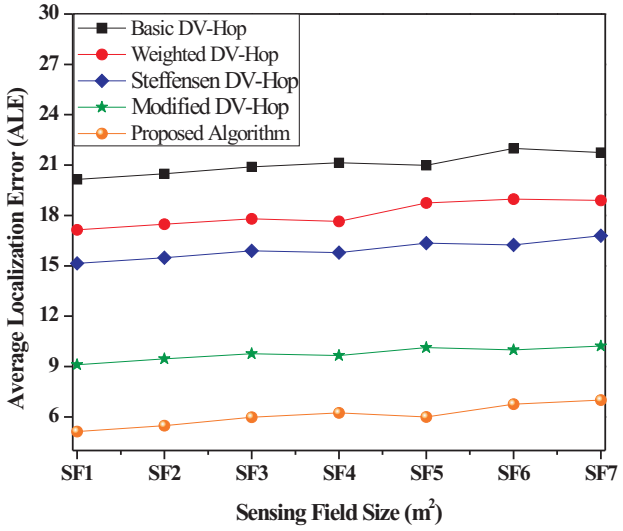

FIGURE 4.9: *Effect of different sensing field on ALE.*

4.4.6 Communication cost and computational efficiency

With the improvement in localization accuracy, cost-effectiveness is also an important aspect for any algorithms to be used in WSNs. The total number of transmitted and received packets for localizing unknown nodes describes the communication cost of the algorithm. All the algorithms {proposed algorithm, Basic DV-hop [76], Weighted DV-Hop [198], Steffensen based DV-Hop [201] and Modified DV-Hop [97]} are completed in three phases. Firstly, the location information of beacon nodes are broadcasted to the unknown nodes and all algorithms have the same communication cost at the first phase. In the second phase, the hop-size distance of each beacon node

is transmitted across network and received by all unknown nodes in network. But in the proposed algorithm, the same information is received by only one-hop neighbor unknown nodes of beacon nodes which reduce the energy consumption and communication cost of the algorithm. Therefore, in the second phase, all algorithms consume more power which increases the communication cost. Total communication cost of DV-Hop [76] is lower than all algorithms. The algorithm [97] have more computational cost because of hop-size modification, upgrading unknown nodes to the assistant beacon nodes and compute the location of nodes by using TLBO. Communication cost of the proposed algorithm is lower than [97].

Further, the complexity of the algorithms are evaluated in terms of computational cost and it is computed by considering the time taken by an algorithm to complete the specific task which is termed as localization time. The localization time for each algorithm is illustrated in Figure 4.10 by changing the density of unknown nodes. Localization time for the proposed algorithm is lower than [97], but a bit faster than [201]. In the proposed algorithm, construction of MEECDS, refinement of average hop-size and collinearity check for beacon nodes consume more time, but it gives more localization accuracy. Therefore, we need to balance the localization time and localization accuracy in practical scenarios.

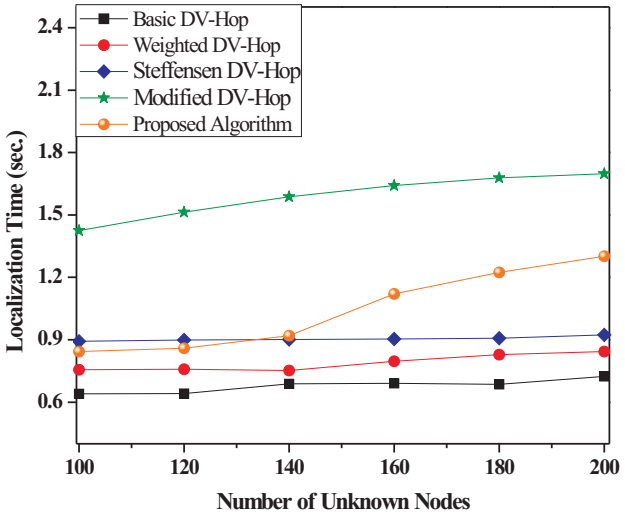

FIGURE 4.10: *Localization time with varying number of unknown nodes.*

4.5 Conclusion

In this chapter, an advanced DV-Hop algorithm is proposed to improve the performance of localization. In the proposed algorithm, all the sensor nodes including beacon nodes as well as unknown nodes are randomly deployed with random mobility. The beacon nodes are prioritized on the basis of their residual energy and degree of connectivity for constructing EECDS. Minimum EECDS is achieved by applying a pruning process on EECDS to reduce the size of EECDS. Further, the concept of DCL is introduced to mitigate the problem of collinearity for improving localization accuracy. The localization error is reduced by introducing a correction factor which modifies the hop-size distances of beacon nodes. To evaluate the performance of the proposed algorithm, various simulations are conducted. It is perceived from the simulated results that the proposed algorithm outperforms in terms of accuracy, energy efficiency and scalability as compared to existing algorithms. It is observed that the proposed algorithm provides 50%, 42%, 35%, and 22% more accurate results as compared to other widely used algorithms.

CHAPTER 5

Energy-efficient Cooperative communication at Media Access Control layer

5.1 Introduction

Location of each sensor node is important aspects in WSNs to make collected information useful. Various applications of sensor networks require precise location of nodes for informative processing of data. Sensor networks for high-risk environments, irrespective of the localization approaches, have limited resources in terms of power, size, memory, bandwidth, and cost of sensor nodes [213][25][214]. Therefore, improvement in the energy efficiency, accuracy and network lifetime of localization algorithm are the most challenging concerns for WSNs. Also, advancement in technology needs dynamic network as per the requirement in various applications to obtain the robust and precise output of the detected event. The energy efficiency and accuracy of

location estimation in such networks are more challenging. After exploring the literature works, it is observed that localization algorithms are lagging behind in terms of supporting mobility and network lifetime. Most of the energy of sensor nodes are consumed during transmission of data over the networks such as multiple data transmission to other nodes, usage of channel and packet transmission [215][216].

Hence, to design MAC protocols for energy-efficiency of WSNs is an issue of concern for the researchers. The concept of cooperative communication in localization can be included to prolong the network lifetime and energy efficiency of the localization algorithms. At present, MAC protocols provide the strongest impact for cooperative localization algorithm in WSNs. The overall performance of the network in terms of life can be significantly upgraded through proper utilization of energy by sending packets at the MAC layer with cooperative communications for localization. Initially, researches on cooperative communication concentrate on the physical layer to reduce energy consumption, Bit Error Rate (BER) and by transmitting data packets from source to final destination using cooperative or relay nodes. Now, recent advancements in cooperative communication focusing on a higher layer such as MAC layer [217][218][219] and network layer [220][221] for energy-efficient communication. The MAC layer comes just after physical layer and the protocols relevant to this can be implemented among sensor nodes for channel sharing, exchanging information and cooperative communication between sensor nodes using relay nodes which avoid collision during transmission [222]. To improve the localization accuracy, various localization algorithms have been developed so far, but the incorporation of MAC layer/comparative communication/ localization algorithm for conserving energy to prolong the network lifetime is less considered and is a gap of statement.

The remaining parts of this chapter are organized as follows; the proposed network model is described in section 5.2. Results and discussion of this chapter is discussed in section 5.3 and the conclusion of the chapter is given in section 5.4.

5.2 Network model

The sensor networks can be directed as an undirected graph $G(V, E)$, where V and E represent the set of sensor nodes and set of edges respectively. For the proposed algorithm, a set B having m beacon nodes ($M = i_1, i_2, i_3, ..., i_M$) and set U having total u unknown nodes ($u = j_1, j_2, j_3, .., j_u$) are randomly deployed with random waypoint mobility model. These sensor nodes are considered in 2-dimensional (2D) area S of dimension $L * L$ where L is the length of the side. The range of transmission of each sensor node is represented by a circle where the center of the circle signifies the corresponding node itself. Each sensor node has its unique MAC address and the wireless channel is shared among multiple sensor nodes. The concept of cooperative communication is introduced in the proposed algorithm in which one-hop communication between beacon nodes and Base-Station (BS) is replaced by two-hop communication for exchanging the information. Moreover, the following are the assumption stand throughout the chapter:

1. A static BS is deployed in the network that can control all the beacon nodes and unknown nodes. The BS is most privileged in terms of resources and computational cost. Hence, all the computing task of localization is performed by BS.

2. In the network, some special nodes are deployed whose locations (x_i, y_i) are prior known with the help of GPS termed as beacon nodes. All the beacon nodes are deployed with random mobility and these nodes are more privileged in terms of resources and communication than unknown nodes.

3. Some of the beacon nodes act as a helper node or cooperative node at any instant for broadcasting the information from one point to another point. Helper nodes just receive the information from source beacon nodes and forward that information to BS.

Definition 1: The sensing field $S(B_i, R_i)$ represents the coverage area covered by beacon nodes in the network, where $(i = 1, 2, 3, ..., M)$. The area of coverage of each

beacon node is computed by Equation 5.1 and every unknown node lie in that area is known as one-hop neighbors of the beacon node.

$$S(B_i, R_i) = \pi R^2 \tag{5.1}$$

Definition 2: Let ξ is the average number of sensor nodes lies in the transmission range of beacon node called average connectivity and ξ can be different at a different time interval and it is computed as follows:

$$\xi = \lambda \pi R^2 \tag{5.2}$$

$$\lambda = \frac{|U|}{M} \tag{5.3}$$

where $|U|$ represents the set of unknown nodes and M represents the total beacon nodes in the network. Due to the dynamic nature of nodes, relative mobility of nodes is an important parameter and it is computed with the help of distances between beacon nodes and unknown nodes. The estimated distances among sensor nodes are computed as the following:

$$P_r = P_t \times G_t \times G_r \times \frac{(Wavelength)^2}{(4 \times \pi \times Distance)^2} \tag{5.4}$$

where P_t represents the transmitted power, G_t and G_r is the gain of transmitting and receiving antenna.

$$wavelength = \frac{c}{f} \tag{5.5}$$

where c is the speed of light and f is the operating frequency of the signals. Estimated distances between beacon nodes and unknown nodes are computed as follows:

$$Distance^t_{(b,u)} = \frac{k}{\sqrt{P_r}} \tag{5.6}$$

In Equation 5.6, k represents the constant and $Distance^t_{(b,u)}$ shows the approximation of distances between nodes, but actual distances among nodes cannot be obtained with the help of the aforementioned equation.Further, the relative mobility ($M^t_{(b,u)}$)

among beacon node b and unknown node u is computed as follows:

$$M^{t}_{(b,u)} = Distance^{t}_{(b,u)} - Distance^{(t-1)}_{(b,u)} \tag{5.7}$$

$Distance^{t}_{(b,u)}$ and $Distance^{(t-1)}_{(b,u)}$ represent the distance between node b and u at any instant of time t and $(t-1)$ respectively. $M^{t}_{(b,u)}$ demonstrates the moving direction of sensor nodes and it defines whether the sensor nodes are moving closer or away from other sensor nodes in the network. All sensor nodes move in a direction with speed v and stay at each location for a pause time t_{pause}. Let d be the distance between two waypoints and average speed of nodes is computed as follows:

$$v_{avg} = \frac{v \times d}{d + (v \times t_{pause})} \tag{5.8}$$

In the proposed algorithm, the BS broadcasts its location to beacon nodes across the network. The distances among BS and beacon nodes are computed using coordinates information received by every beacon node. The format of broadcasted message by BS is as following:

$$\text{BS} \rightarrow \text{Beacon nodes: } \{BS\_address, (X, Y)\}$$

where (X, Y) represents the coordinates of BS. Now, each beacon node forwards Nearest Neighbor Request ($NNReq$) to one-hop neighbor unknown nodes by using the following packet format:

$$\text{NNReq: } \{Id_i, (x_i, y_i), Hop\_count = 0\}$$

where Id_i is the identification of the beacon node and (x_i, y_i) represents the coordinates of the beacon node and hop-count is set to zero initially. Sometime, it may happen that $NNReq$ packets are received by two-hop neighbor unknown nodes, in that cases the unknown nodes check the value of Hop_count. If the value of Hop_count is more than 1, the unknown nodes will simply discard the message and stop Hop_count counter. After receiving $NNReq$ from beacon node, the unknown nodes broadcast a reply with Nearest Neighbor Reply ($NNRep$) with its identification Id_u and Hop_count value incremented by 1. The format for $NNRep$ packets are as following:

$$\text{NNRep: } \{Id_i, (x_i, y_i), Hop\_count = 1, u\_Id\}$$

u_Id is the address of the unknown node. In random network scenario, generally the same message is received within two hops nodes, in such cases after verifying the Hop_count value the message is discarded by the nodes.

Once the beacon nodes receive the $NNRep$ from unknown nodes, each beacon node enlists its one-hop neighbor unknown nodes in a Neighbor Node list (NNL) for the localization process. Further, the NNL list is forwarded to BS either directly or with two-hop communication using the following packet:

$$\text{Beacon Node} \rightarrow \text{BS: NNL} = \{Id_i, (x_i, y_i) | u\_1, u\_2, ...\}$$

The entire sensor nodes are deployed with random mobility which causes the beacon nodes may be located at a far place from the position of BS. In this situation, direct communication between beacon nodes and BS consumes energy for transmission of packets. Therefore, cooperative communication in localization can provide development in the performance of the algorithm by introducing a new paradigm beyond the traditional point to point and point to multi-point communication models. The process of cooperative communication is demonstrated with the help of Figure 5.1. In this figure beacon node S1 is located two-hop away from BS and data packets transmission would consume more energy for direct communication between S1 and BS. On the other hand, the energy consumption can be reduced if the information is forwarded with the help of S6 and S2 to BS called cooperative communication and S6 or S2 act as helper node.

5.2.1 Co-operative communication at the MAC layer

Beacon nodes forward the list of NNL to BS either directly or using cooperative communication. In the case of direct communication, sender-beacon nodes ($Sender_{BN}$) broadcasts the information directly to BS, but the data packets are broadcasted with the help of helper node ($Cooperative_{BN}$) in cooperative communication. Each beacon node computes weight metric on the basis of residual energy and distance between BS and itself, and prioritizes based on weight metric for cooperative

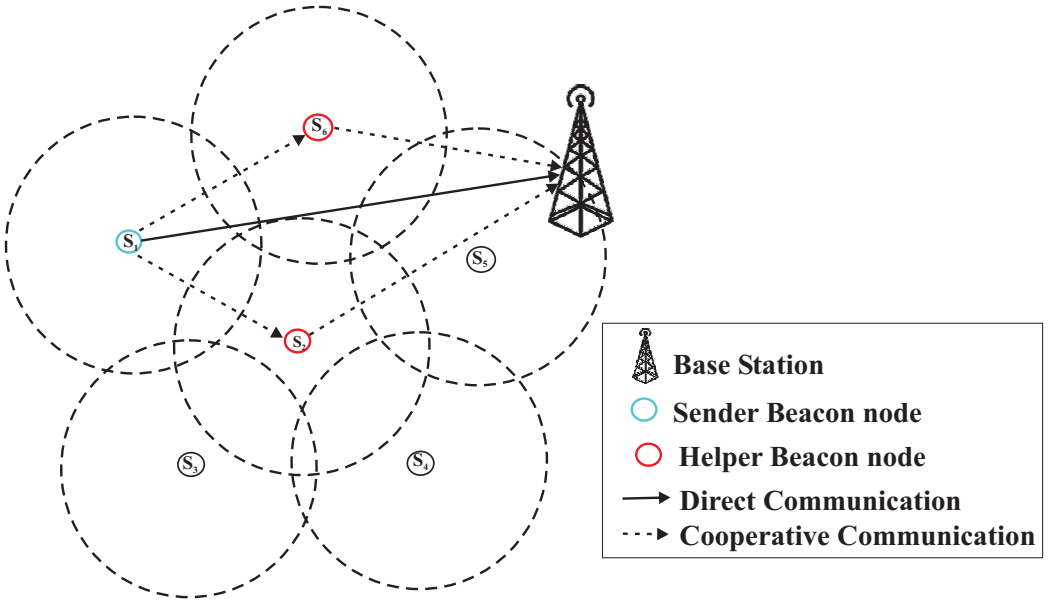

FIGURE 5.1: *Network Example with Direct and cooperative communication.*

communication. The weight metric is computed as follows:

$$\begin{cases} W_i = w_1 \times E_r^b + w_2 \times [log(\frac{1}{Distance_{BS}^b})] \\ w_1 + w_2 = 1,\ 0 < w_1 \ and \ w_2 < 1 \end{cases} \tag{5.9}$$

where E_r^b is the residual energy of the beacon node, the distance between BS and beacon node is denoted by $Distance_{BS}^b$ and $(w_1 + w_2)$ is considered as a random factor for biasing. A beacon node with highest weight metric is elected as a $Cooperative_{BN}$ by nearest beacon nodes. A cooperative table is maintained by each beacon node that has the information about helper nodes, as tabulated in Table 5.1. The table is updated periodically to store recent information. The procedure of frame exchange

TABLE 5.1: *Cooperative table format*

Helper node	**Weight metric**	**Distance from source node to helper**	**Distance from helper to BS**	**Residual Energy**
h_1	W_1	$Distance_{SN}^{h1}$	$Distance_{BS}^{h1}$	E_r^1
h_2	W_2	$Distance_{SN}^{h2}$	$Distance_{BS}^{h2}$	E_r^2
...	...	...	...	...
h_i	W_i	$Distance_{SN}^{hi}$	$Distance_{BS}^{hi}$	E_r^i

for data transmission on the MAC layer and algorithm for cooperative nodes selection is described below:

5.2.1.1 Handshaking procedure of proposed Algorithm:

In traditional IEEE 802.11 MAC standard, three control packets/frames such as Request-to-Send (RTS), Clear-to-Send (CTS) and Acknowledgment (ACK) are utilized for data broadcasting. But, in the proposed algorithm two additional frames denoted as Helper-to-Send (HTS) and Cooperative-CTS (CCTS) are considered for cooperative communication.

1. Firstly, $Sender_{BN}$ sense the channel to check the status idle or busy before broadcasting the packets to Destination BS ($Destination_{BS}$). If $Sender_{BN}$ found the idle status of the channel for duration Distributed Interframe Space (DIFS), it reserves the channel by forwarding the RTS frame for a required duration of time. A timer Network Allocation Vector (NAV) is assigned during which the channel would be busy and NAV(RTS) is computed by Equation 5.10.

$$NAV(RTS) = 5 \times SIFS + T_{HTS} + T_{CCTS} + T_{ACK} + \zeta \tag{5.10}$$

$$\zeta = \frac{Length}{Datarate} \tag{5.11}$$

   SIFS represents the Short Interframe Space, T_{HTS}, T_{CCTS} and T_{ACK} are the time durations of HTS, CCTS and ACK frames respectively and the ratio of the length of the packet to the data rate of transmission is represented by ζ in Equation 5.11.

2. When RTS frame is received by the neighboring node of $Sender_{BN}$, $Cooperative_{BN}$ is selected on the basis of weight metric and it reserves the channel for duration NAV(HTS) that is computed as follows:

$$NAV(HTS) = 4 \times SIFS + T_{CCTS} + T_{ACK} + \zeta \tag{5.12}$$

3. Once the RTS and HTS frames are received by $Destination_{BS}$, it forwards a CCTS frame which represents that the cooperative node is ready for transmission and reserves the channel for a duration NAV(CCTS) computed by Equation 5.14. If the $Destination_{BS}$ receives the RTS frame, did not receive HTS frame within a particular duration HTS_time_{out}, it broadcasts CTS frame to SenderBN that means the DestinationBS is ready for direct communication. The HTS_time_{out} duration is computed as follows:

$$HTS\_time_{out} = (SIFS + T_{HTS}) \tag{5.13}$$

$$NAV(CCTS) = 3 \times SIFS + T_{ACK} + \zeta \tag{5.14}$$

Low power signals are carried by both CCTS and CTS frames during transmission from $Sender_{BN}$ to $Destination_{BS}$. After receiving the CCTS frame, the helper nodes compute its minimum power to transmit information to the $Destination_{BS}$.

4. If the $Sender_{BN}$ receives the HTS and CCTS frame within a time duration $CCTS\_time_{out}$, it broadcasts the information to DestinationBS with the help of, $Cooperative_{BN}$ otherwise, the broadcast the information packets directly. The time duration for $CCTS\_time_{out}$, and NAV(CTS) is computed as follows:

$$CCTS\_time_{out} = (2 \times SIFS + T_{maxBackoff} + T_{HTS} + T_{CCTS}) \tag{5.15}$$

$$NAV(CTS) = 2 \times SIFS + T_{ACK} + \zeta \tag{5.16}$$

5. Once the information is received successfully by $Destination_{BS}$, it forwards an ACK frame directly to $Sender_{BN}$. The $Sender_{BN}$ goes in the idle state till next communication once the ACK frame is successfully collected by itself. But, it reserves the channel again if the ACK packet is not received within ACK_time_{out} which shows that the transmission is failed due to some reasons. ACK_time_{out}

computed by Equation 5.17:

$$\begin{cases} ACK\_time_{out} = (2 \times SIFS + \zeta + T_{ACK}) \ \ i.e.\ ACK\ in\ Cooperative\ transmission \\ ACK\_time_{out} = (SIFS + \zeta + T_{ACK}) \ \ i.e.\ ACK\ in\ Direct\ transmission) \end{cases} \tag{5.17}$$

The working principle of direct communication and cooperative communication between $Sender_{BN}$ and $Destination_{BS}$ is illustrated in Figure 5.2. In Figure 5.3, the flowcharts of frame exchanges at $Sender_{BN}, Cooperative_{BN}$ and $Destination_{BS}$ are demonstrated respectively.

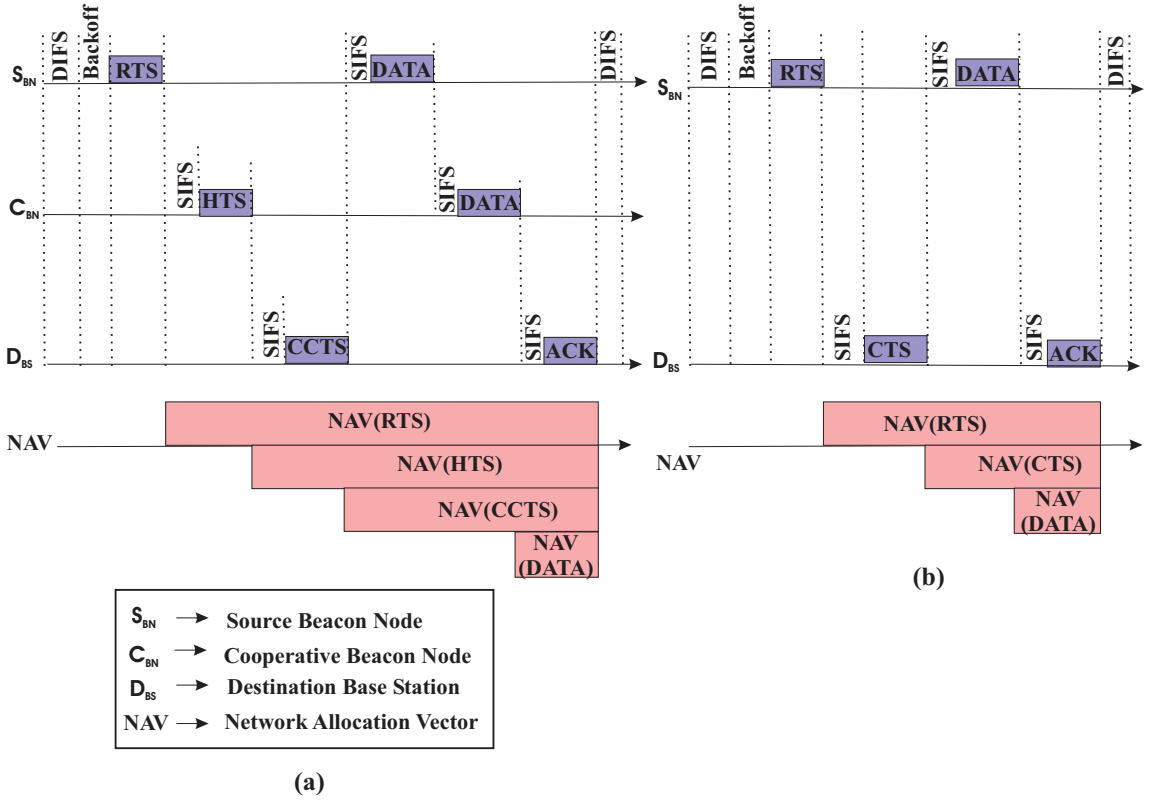

FIGURE 5.2: *(a) Procedure for Cooperative Communication and (b) procedure for direct communication.*

5.2.1.2 Optimal Cooperative node selection procedure

Before broadcasting the NNL to $Destination_{BS}$, $Sender_{BN}$ ensures the availability of neighbor helper nodes that are ready for cooperative communication. Once

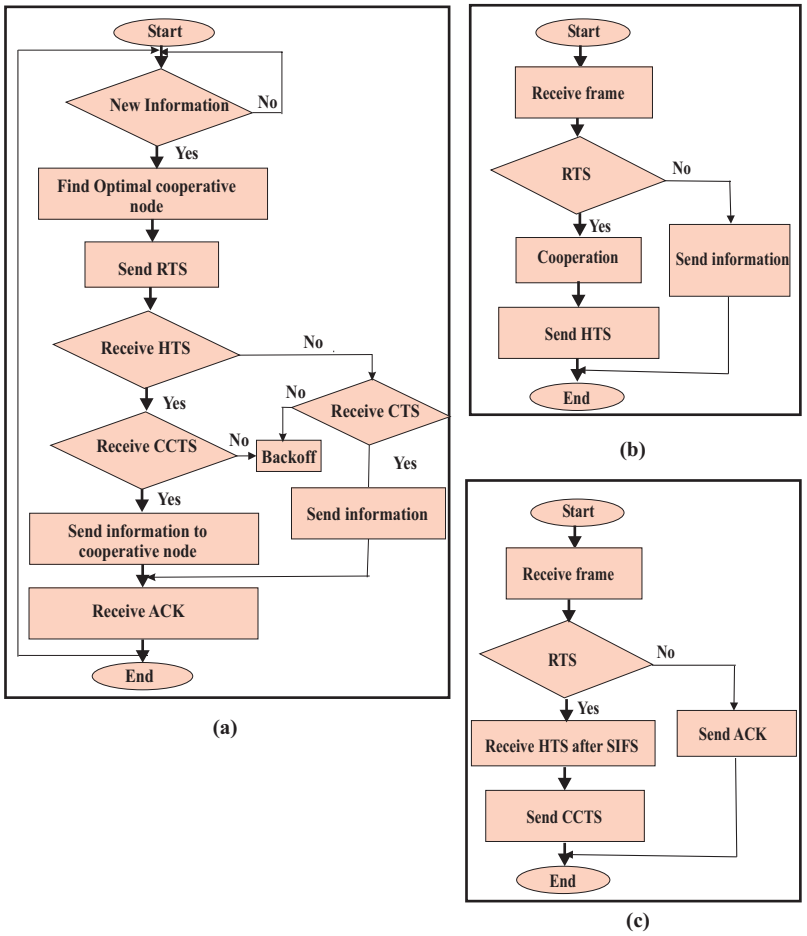

FIGURE 5.3: *Flowcharts for (a) Frame exchanges at $Sender_{BN}$ (b) Frame exchanges at $Cooperative_{BN}$ and (c) Frame exchanges at $Destination_{BS}$.*

RTS and CCTS frames are received by $Sender_{BN}$, it selects $Cooperative_{BN}$ on the basis of higher weight metric and ensures that the selected $Cooperative_{BN}$ is able to diminish overall energy consumption or not through cooperative communication. The consumption of energy during direct and indirect communication is computed by using Equation 5.18 and 5.20 respectively.

$$E_{direct} = (P_t + P_r) \times \varphi + (P_t^{Sender_{BN}} + P_r) \times \zeta \tag{5.18}$$

$$\varphi = T_{RTS} + T_{CTS} + T_{ACK} \tag{5.19}$$

where E_{direct} represents the energy consumption during direct communication, P_t is the required power for transmission of RTS, CTS and ACK frames, φ is the total time duration for transmission of RTS, CTS and ACK frames, $P_t^{Sender_{BN}}$ represents the

transmission power for data packet transmission from $Sender_{BN}$ to $Destination_{BS}$ in case of direct transmission and P_r is the power for the reception that can be calculated using the free-space propagation model [223].

$$E_{Cooperative} = (P_t + P_r) \times \alpha + (P_t^{Sender'_{BN}} + P_t^{Cooperative_{BN}} + 2P_r) \times \zeta \tag{5.20}$$

$$\alpha = (T_{RTS} + T_{CTS} + T_{HTS} + T_{ACK}) \tag{5.21}$$

where $E_{Cooperative}$ represents the energy consumption during cooperative communication and α is the total time duration of RTS, CTS, HTS and ACK frames. The information is forwarded to $Destination_{BS}$ using cooperative transmission if the $Cooperative_{BN}$ reduces overall energy consumption significantly otherwise direct transmission would be preferred.

$$\Delta_E = E_{direct} - E_{Cooperative} \tag{5.22}$$

$$\Delta_E = ((P_t + P_r) \times T_{HTS}) + (P_t^{Sender_{BN}} - P_t^{Sender'_{BN}} - P_t^{Cooperative_{BN}} - P_r) \times \zeta \tag{5.23}$$

For cooperative transmission, $Cooperative_{BN}$ satisfied the following condition:

$$\Delta_E > 0 \tag{5.24}$$

In Equation 5.22, the zero value of Δ_E represents that any of transmission can be utilized in such situation. Further, an energy factor ξ is considered in the proposed algorithm for selecting optimal $Cooperative_{BN}$ among all helper nodes and it is computed as follows:

$$\xi = \frac{E_c^b}{E_r^b} \tag{5.25}$$

where E_c^b and E_r^b are the consumed energy and residual energy of $Cooperative_{BN}$ respectively. For the simplicity, energy consumption during data transmission is considered and energy consumption during sensing and data processing are simply ignored. $Cooperative_{BN}$ with the smallest ξ is selected for cooperative communication and with the help of energy factor, the proposed algorithm can simply avoid the situation

where random beacon nodes are selected for cooperation which degrades the lifetime of the network.

5.2.1.3 Condition for Transmission power:

To improve the performance in terms of energy of the proposed algorithm, the transmission power $P_t^{Sender_{BN}}$ and $P_t^{Cooperative_{BN}}$ should satisfy two conditions for data transmission. The transmission power of $Sender_{BN}$ should satisfy the Shannon theorem shown in Equation 5.26.

$$B_u \leq \frac{1}{2} log_2[1 + (\frac{P_t^{Sender_{BN}}}{N_0})] \tag{5.26}$$

In the aforementioned equation, B_u is the bandwidth required for data transmission and white Gaussian noise power is represented by N_0. The information forwarded from $Sender_{BN}$ to $Destination_{BS}$ using two hops is as follows:

$$\begin{cases} Sender_{BN} \rightarrow Cooperative_{BN} \\ Cooperative_{BN} \rightarrow Destination_{BS} \end{cases}$$

Therefore, each one-hop transmission occupies half of the channel resources for data transmission and is represented by introducing 1/2 factor in Equation 5.26. The aforementioned equation can be deduced as follows:

$$(\frac{P_t^{Sender_{BN}}}{N_0}) \geq 2^{2R} - 1 \tag{5.27}$$

The condition shown in Equation 5.22 must be satisfied by $Cooperative_{BN}$ during data transmission. All beacon nodes across the network should adjust their transmission power as shown in Equation 5.28 and Equation 5.29.

$$0 < P_t^{Sender_{BN}} \leq P_{max.} \tag{5.28}$$

$$0 < P_t^{Cooperative_{BN}} \leq P_{max.} \tag{5.29}$$

$P_t^{Sender_{BN}}$ must be always positive because it is the essential power required to forward information to the destination. But, the $P_t^{Cooperative_{BN}}$ can be zero because in that case the information can be forwarded directly to the $Destination_{BS}$ without involving any cooperative node. Shannon theorem is utilized in the proposed algorithm to limits the transmission power within the range of maximum transmission power and it offers the boundary to the transmission power of the beacon nodes.

5.2.1.4 Condition for Residual energy and channel gain of cooperative nodes:

Further, to prolong the network lifetime, the residual energy among SenderBN and $Cooperative_{BN}$ should be maximized and expressed by Equation 5.30 and Equation 5.31 respectively.

$$E_r^{Sender_{BN}} = min\{E^{Sender_{BN}} - \vartheta\} \tag{5.30}$$

$$\vartheta = (P_t + P_r) \times \varphi \times T \tag{5.31}$$

$$E_r^{Cooperative_{BN}} = min\{E^{Cooperative_{BN}} - \chi\} \tag{5.32}$$

$$\chi = (P_t + P_r) \times \alpha \times T \tag{5.33}$$

In aforementioned equations, $E^{Sender_{BN}}$and $E_r^{Sender_{BN}}$ are the energy of $Sender_{BN}$ before and after current packet transmission respectively, T represents the duration of packet transmission and total energy consumption during data packet transmission. Similarly, $E^{Cooperative_{BN}}$ and $E_r^{Cooperative_{BN}}$ are the energy of χ $Cooperative_{BN}$ before and after packet transmission respectively and is the total energy consumed for data packet transmission at cooperative nodes. The factors ϑ and χ should be optimized in order to maximize the residual energy which prolongs the network lifetime shown as follows:

$$[max.\{E_r^{Sender_{BN}}, E_r^{Cooperative_{BN}}\}] \tag{5.34}$$

Further, the residual energy and channel gain between $Cooperative_{BN}$ $Sender_{BN}/Destination_{BS}$ must meet some certain conditions. The residual energy of $Cooperative_{BN}$ before communication must be larger than the residual energy of $Sender_{BN}$ after information directly to $Destination_{BS}$.

$$E^{Sender_{BN}} - P_D T < E^{Cooperative_{BN}} \tag{5.35}$$

where P_D is the required transmission power for direct transmission, T represents the duration of packet transmission and direct power from $Sender_{BN}$ to $Destination_{BS}$ can be calculated by Shannon theorem as follows:

$$B_u \leq log_2[1 + (\frac{P_D}{N_0})] \tag{5.36}$$

After rearranging equation 5.32

$$2^{B_u} - 1 \leq (\frac{P_D}{N_0}) \tag{5.37}$$

$$P_D \geq N_0(2^{B_u} - 1) \tag{5.38}$$

All beacon nodes broadcast NNL to BS through an optimal cooperative node or direct transmission.

5.2.2 Localization problem in WSNs

The whole process of localization is executed at BS after getting the NNL from each beacon node. Let us consider, total m beacon nodes and u unknown nodes are randomly deployed in the two-dimensional area with random waypoint mobility model. The coordinates of all sensor nodes are represented through a vector $= [v_1, v_2, v_3, ..., v_{(m+u)}]$ initially and $v_i = [x_i, y_i]^T$. The beacon nodes are already aware of their coordinates represented by $[(x_1, y_1), (x_2, y_2), ..., (x_m, y_m)]$. To compute the locations of unknown nodes $[(x_{(m+1)}, y_{(m+1)}), (x_{(m+2)}, y_{(m+2)}), ..., (x_{(m+n)}, y_{(m+n)})]$ by using location information of beacon nodes is the main motive of the localization

process and this process can be represented mathematically as follows:

$$(\hat{x}, \hat{y}) = F_{i=1,2,...m}(x_i, y_i, Distance_i) \tag{5.39}$$

where $(\hat{x}, \hat{y})$ are the estimated coordinates of unknown nodes, (x_i, y_i) represents the coordinates of i^{th} beacon nodes and $Distance_i$ is the estimated distance among nodes.

In the aforementioned equation, $(\hat{x}, \hat{y})$ and (x_i, y_i) are the coordinates of the unknown node and i^{th} beacon node respectively and the distance among unknown node and beacon node is denoted as $Distance_i$.

5.2.2.1 Localization of Unknown Nodes

The positions of unknown nodes are computed by applying a 2D hyperbolic method instead of trilateration or triangulation method at BS. The distance between beacon nodes and unknown nodes are calculated as follows:

$$Distance_i^{est} = \sqrt{(x_i - \hat{x})^2 - (y_i - \hat{y})^2} \tag{5.40}$$

By rearranging the aforementioned equation, we have the following expression

$$x_i^2 + y_i^2 - 2x_i\hat{x} - 2y_i\hat{y} + (\hat{x})^2 + (\hat{y})^2 = (Distance_i^{est})^2 \tag{5.41}$$

$$A_i = x_i^2 + y_i^2 \tag{5.42}$$

$$B = (\hat{x})^2 + (\hat{y})^2 \tag{5.43}$$

Equation 5.40 can be represented as:

$$(Distance_i^{est})^2 - A_i = -2x_i\hat{x} - 2y_i\hat{y} + B$$

$$P_c = [\hat{x}, \hat{y}, B]^T$$

$$K_c = \begin{pmatrix} -2x_1 & -2y_1 & 1 \\ -2x_2 & -2y_2 & 1 \\ . & . & . \\ . & . & . \\ -2x_i & -2y_i & 1 \end{pmatrix}$$

$$H_c = \begin{pmatrix} (Distance_1^{est})^2 - A_1 \\ (Distance_2^{est})^2 - A_2 \\ . \\ . \\ (Distance_i^{est})^2 - A_i \end{pmatrix}$$

$$K_c P_c = H_c \tag{5.44}$$

The position of unknown nodes can be determined by the following Equation:

$$P_c = (K_c^T K_c)^{-1} K_c^T H_c \tag{5.45}$$

Now, the coordinates of the unknown nodes are given as:

$$\begin{cases} \hat{x} = P_c(1) \\ \hat{y} = P_c(2) \end{cases}$$

The difference between the actual and estimated $Distance_i^{est}$ distances must be minimized to get more accurate location of unknown nodes. In real network scenario, the estimated distances between nodes are mostly affected by Gaussian noise in WSNs. Therefore, to minimize the localization error, $Distance_i^{est}$ are adjusted as follows:

$$\widehat{D_i} = Distance_i + n_i \tag{5.46}$$

In the aforementioned equation n_i is the noise that affects the $Distance_i^{est}$ in the range of $(Distance_i \pm Distance_i(\frac{p_n}{100}))$, where P_n represents the percentage of noise.

5.3 Results and Discussion

The performance of the proposed algorithm is evaluated in MATLAB 2017 and different simulations are conducted for getting the simulated results. All the simulation parameters used during the simulations of the proposed algorithm are shown in Table 5.2.

TABLE 5.2: *Simulation parameters*

Parameters	**Value of parameters**	**Parameters**	**Value of parameters**
RTS	160bits	Population size	30
HTS	192bits	$k_{max.}$	30
CCTS	120bits	c_1, c_2	2.0
CTS	128bits	Sensor nodes	$100 - 400$
ACK	112bits	$\omega_{max.}$	0.9
SIFS	$10\mu s$	Beacon nodes	$10 - 40\%$
DIFS	$50\mu s$	Communication radius	$15 - 60m$
$P_{max.}$	$50mw$	Network topology	Random way point mobility
B_u	$10khz$	Maximum iteration	500

5.3.1 Simulation parameters and performance metric

The simulation results of the proposed algorithm are examined by using different performance metrics such as localization error, Average Localization Error (ALE), error variance and network lifetime. From Equation 5.47, it is observed that the total number of sensor nodes and beacon nodes affect the performance of localization algorithms significantly. Therefore, the impact of total sensor nodes, beacon nodes, communication radius, and sensing field are examined on accuracy of localization algorithms.

Localization error:

LE is defined as the difference between estimated location and actual location of

unknown node u and it is computed as follows:

$$Error_u = \sqrt{(x_u^{est} - x_u^{act})^2 + (y_u^{est} - y_u^{act})^2} \tag{5.47}$$

In the aforementioned equation, (x_u^{est}, y_u^{est}) and (x_u^{act}, y_u^{act}) represent the estimated and actual coordinates of unknown node u respectively. *Average localization error (ALE):* ALE is defined as the ratio of the sum of localization error of unknown nodes to the total number of unknown nodes in the network. It is computed as follows:

$$ALE = \frac{\sum_{u=m+1}^{N} \sqrt{(x_u^{est} - x_u^{act})^2 + (y_u^{est} - y_u^{act})^2}}{(N-m) \times R} \tag{5.48}$$

$$LEV = \sqrt{\frac{\sum_{u=m+1}^{N} (\sqrt{(x_u^{est} - x_u^{act})^2 + (y_u^{est} - y_u^{act})^2} - ALE \times R)^2}{(N-m) \times R^2}} \tag{5.49}$$

where LEV is the localization error variance and R represents the communication radius. Further, the accuracy of localization algorithms is computed as follows:

$$Accuracy = (1 - ALE) \times 100 \tag{5.50}$$

The Proportion of Localized Sensor Node (PLSN): PLSN is the ratio of total number of unknown nodes that are localized successfully to the total number of unknown nodes considered for the localization process. It gives the measurement of positioning coverage and computed as follows:

$$PLSN = \frac{S_{LN}}{(N-m)} \tag{5.51}$$

The Proportion of Unlocalized Sensor Node (PUSN): PUSN is defined as the ratio of number of unlocalized unknown nodes to the total number of unknown nodes considered for the localization process. The unlocalized nodes are those nodes which did not get their location after the localization process and PUSN is computed as follows:

$$PUSN = \frac{U_{LN}}{S_{LN}} \tag{5.52}$$

The unlocalized nodes are those nodes which have localization error more than $\frac{R}{2}$.

$$\begin{cases} E_{Tx}(k, Distance) = k \times E_{Elec} + k \times E_{FS} \times Distance^2 & Distance < d_0 \\ E_{Tx}(k, Distance) = k \times E_{Elec} + k \times E_{MP} \times Distance^4 & Distance \geq d_0 \\ d_0 = \sqrt{\frac{E_{FS}}{E_{MP}}} \end{cases}$$

$$E_{Rx}(k) = k \times E_{Elec} \tag{5.53}$$

In the aforementioned equation, $E_{Tx}(k, Distance)$ represents the energy required for transmission of k bits from one point to another point at a particular distance, $E_{Rx}(k)$ represents the required energy for the reception of k bits information, E_{Elec} is the energy consumed by electronic circuitry, E_{FS} is the energy required for free space model amplifier and E_{MP} is the required energy for multipath fading model amplifier. The average residual energy (E_r^{avg}) of beacon nodes is an important parameter to evaluate the performance of any algorithm.

$$E_r^{avg} = \frac{1}{N} \sum_{j=1}^{N} E_r^{b_j} \tag{5.54}$$

The variance of the residual energy of all nodes is computed as follows:

$$E_r^{Var} = \sqrt{\frac{1}{N} \sum_{j=1}^{N} (E_r^{b_j} - E_r^{avg})^2} \tag{5.55}$$

5.3.2 Simulation results

The simulated performance of the proposed algorithm is compared to existing algorithms such as IDV-HOP [204], NDV-Hop [92], Modified DV-Hop [107] and Improved DV-Hop [123]. The simulated results are evaluated by varying the different parameters such as beacon node ratio, sensor node density, transmission range, sensing field and residual energy and these parameters affects the performance of the localization algorithms effectively. Therefore, different simulations are conducted to analyze the performance of the algorithms.

- Experiment 1: Average Localization Error (ALE)
- Experiment 2: Effect of ratio of beacon nodes
- Experiment 3: Effect of the total number of sensor nodes
- Experiment 4: Effect of sensing field
- Experiment 5: Frequency of error occurrence
- Experiment 6: Residual energy
- Experiment 7: Localization time
- Experiment 8: Effect of Network Connectivity on localization
- Experiment 9: Effect of ratio of beacon nodes and total sensor nodes on LEV

5.3.2.1 Experiment 1: Average Localization Error (ALE)

For conducting experiment 1, 100 sensor nodes are randomly deployed with 25% beacon nodes in the sensing area of $100 \times 100m^2$ by considering $25 - 40m$ communication radius. Instantaneous localization error of each node is displayed in Figure 5.4 and it is observed from the simulated results that the proposed algorithm accomplishes better as compared to other algorithms. Maximum, minimum and average localization errors accomplished by all algorithms are tabulated in Table 5.3.

TABLE 5.3: *Minimum, maximum and average localization error comparison of algorithms*

Algorithm	**Minimum Localization Error**	**Maximum Localization Error**	**Average Localization Error**
IDV-HOP [204]	7.1274	31.099	20.226
NDV-Hop [92]	9.3037	27.7576	18.9072
Improved DV-Hop [123]	6.2963	22.9624	15.2289
Modified DV-Hop [107]	6.0042	20.2041	14.0147
Proposed Algorithm	0.1064	9.95611	5.3407

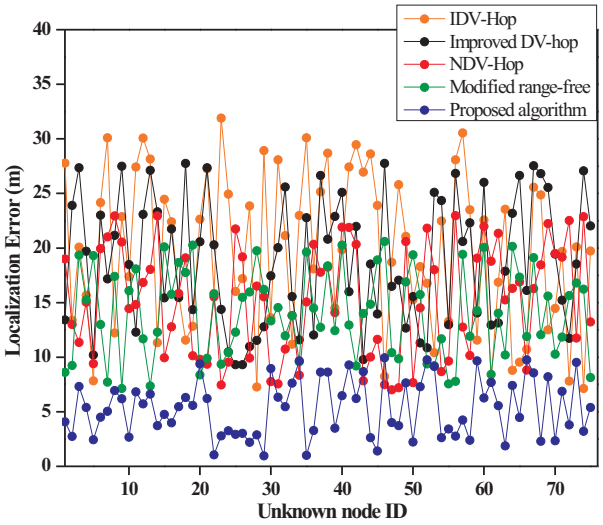

FIGURE 5.4: *Localization error of each unknown node for a single simulation at any instant.*

5.3.2.2 Experiment 2: Effect of ratio of beacon nodes

The density of beacon nodes affects the performance of localization algorithms significantly. For experiment 2, 100 sensor nodes are deployed in the sensing area of $100 \times 100m^2$ by considering communication radius $15 - 60m$. The simulated results of the algorithms by varying beacon node ratio are depicted in Figure 5.5. From the simulated results, it is observed that as the ratio of beacon nodes increases, the ALE for all algorithms decreases. It happens because additional location information about unknown nodes can be collected by more beacon nodes. It is observed from Figure 5.5 that the proposed algorithm accomplishes least localization error as compared to other existing algorithms. The performance of the all localization algorithm is affected by the communication radius of sensor nodes. From the simulated results it is observed that as the communication radius of sensor nodes increases ALE of each algorithm decreases. It is due to fact that the network becomes more connective when communication radius increases.

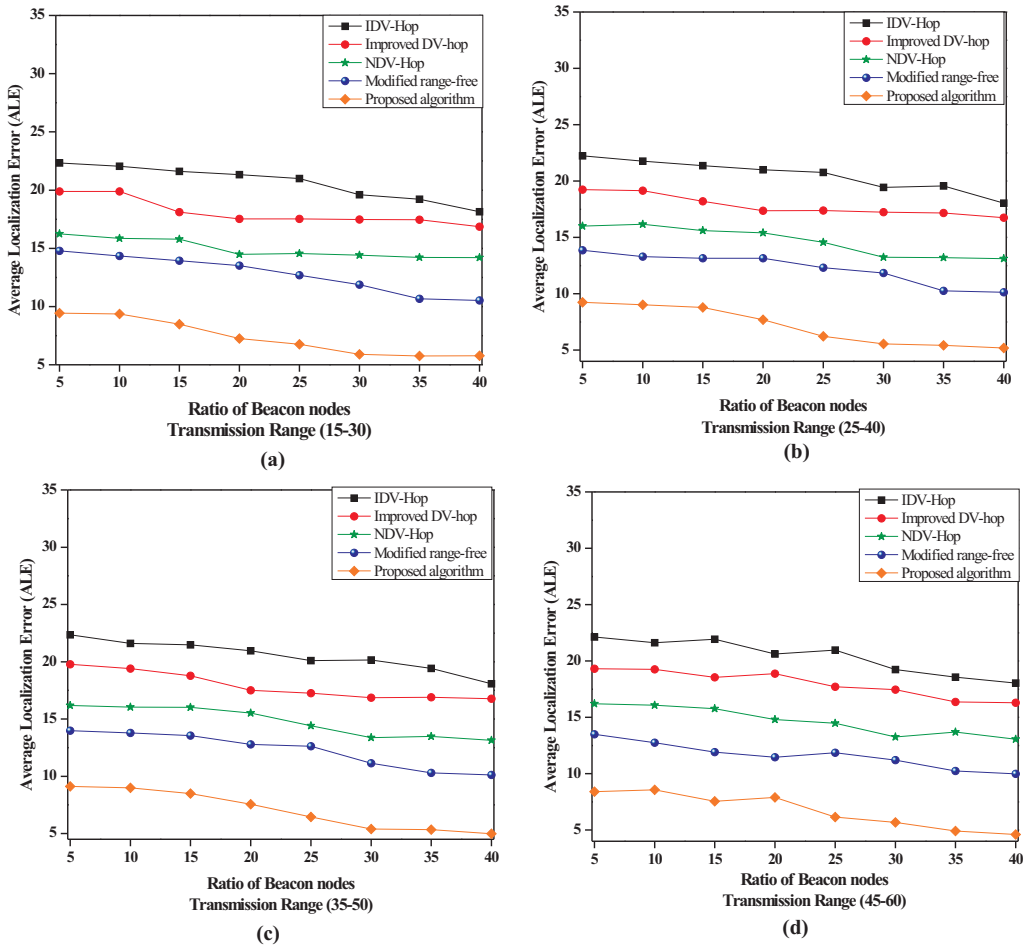

FIGURE 5.5: *Effect of ratio of beacon nodes and transmission range on ALE.*

5.3.2.3 Experiment 3: Effect of sensor node density

To examine the impact of sensor node density on ALE, experiment 3 is conducted. To analyze the performance, total 100 to 400 sensor nodes are randomly deployed in a sensing area 100×100 with 20% beacon nodes ratio and by varying communication radius from 15 to $60m$. The simulated results of all algorithms are demonstrated in Figure 5.6 and it can be observed from results that nodes density have a great impact on ALE. As the density of nodes increases, ALE for all algorithm decreases. It happens due to the fact that as number of nodes increases, network becomes more connective and large location information about beacon nodes can be

collected by unknown nodes. But, after reaching a certain limit of sensor nodes, network connectivity does not contribute more variation and also minor variation take place in ALE. From the simulated results depicted in Figure 5.6, it is perceived that the proposed algorithm outperforms as compared to existing ones.

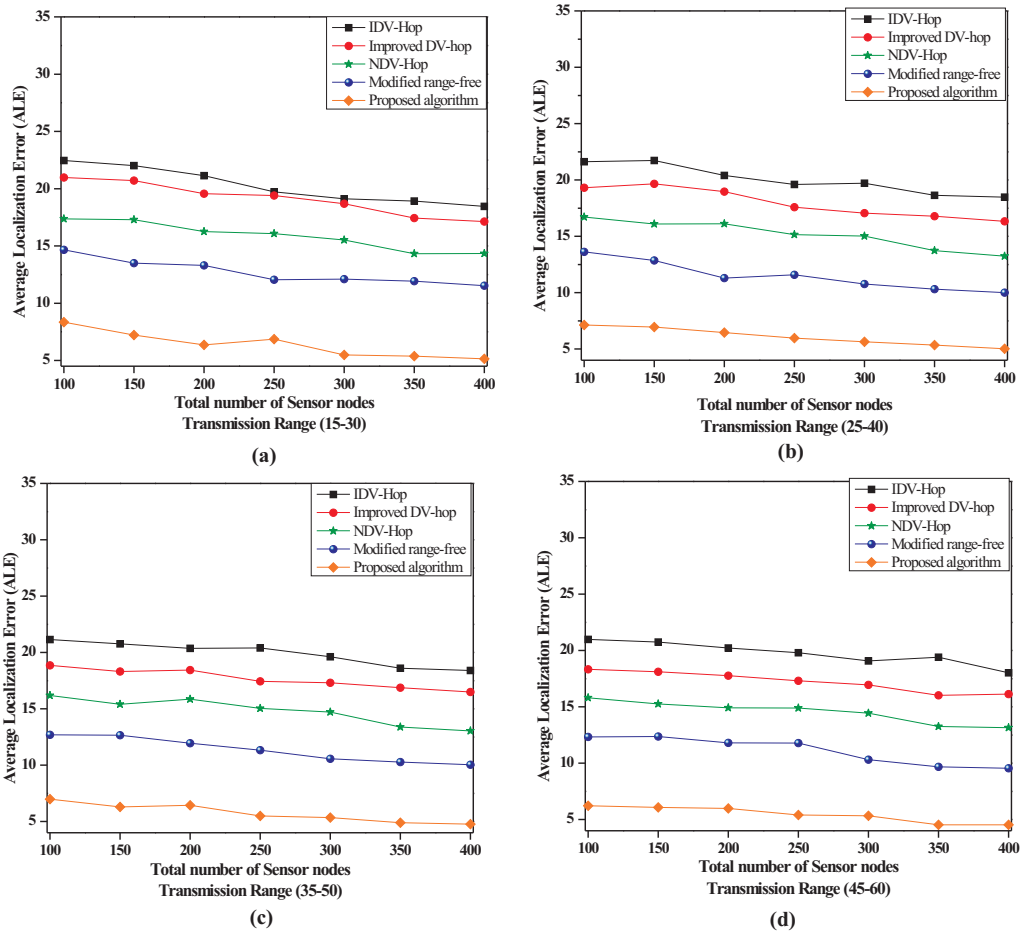

FIGURE 5.6: *Effect of the total number of sensor nodes and transmission range on ALE.*

5.3.2.4 Experiment 4: Effect of sensing field

To analyze the effect of sensing field on ALE, experiment 4 is conducted. For the simulation, 100 sensor nodes with 20% beacon nodes are randomly deployed in the sensing field $100 \times 100m^2$ to $400 \times 400m^2$ with considering communication radius form 25 to $40m$. From the simulated results, it is observed that as the sensing area increases

the ALE of each algorithm decreases significantly. It happens because the connectivity of network decreases as the sensing area increases which affects the performance of the algorithms effectively. The simulated results of all algorithms are demonstrated in Figure 5.7 and it can be seen that the proposed algorithm outperforms in terms of accuracy as compared to existing ones.

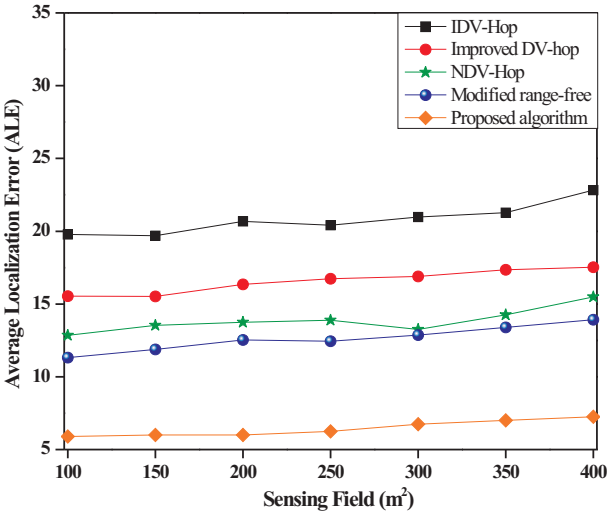

FIGURE 5.7: *Effect of variation in the sensing field on ALE.*

5.3.2.5 Experiment 5: Frequency of error occurrence

To analyze the frequency of error occurrence for different algorithms, experiment 5 is conducted. For the simulation, 100 sensor nodes are deployed with 20% beacon node ratio in sensing field of $100 \times 100m^2$. To analyze the performance of the algorithms, 100 numbers of simulations are conducted. The simulated results of all algorithms are demonstrated in Figure 5.8 and it is perceived from the results that that proposed algorithm performs better in terms of accuracy as compared to existing ones.

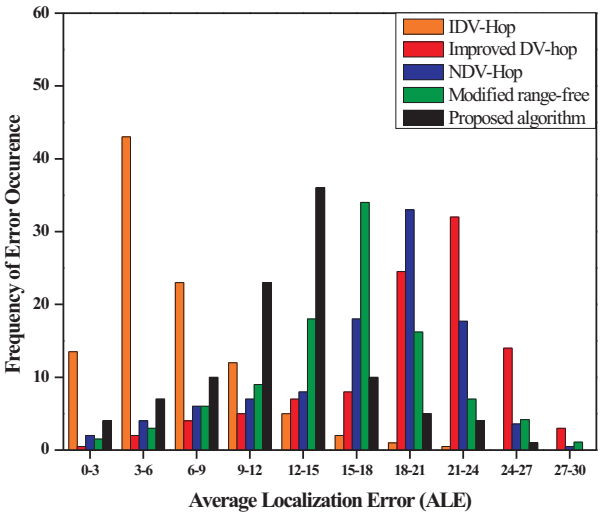

FIGURE 5.8: *Frequency of error occurrence for different algorithms.*

5.3.2.6 Experiment 6: Effect of ratio of beacon node and total sensor nodes on the percentage of Residual energy

To analyze the impact of the ratio of beacon nodes and node density on residual energy, experiment 6 is conducted. For the simulation, total 100 to 400 sensor nodes are deployed with 10 to 40% beacon nodes by considering communication radius 25 to $40m$. The information regarding unknown nodes collected by beacon nodes is broadcasted to BS for further processing by using cooperative communication. The whole process of localization and optimization are performed at BS which reduces the message exchanges between beacon nodes and unknown nodes. The simulated results of all algorithms are illustrated in Figure 5.9. It is observed from the simulated results that the percentage of residual energy of the proposed algorithm is higher than other algorithms and it shows an effective point of the proposed algorithm.

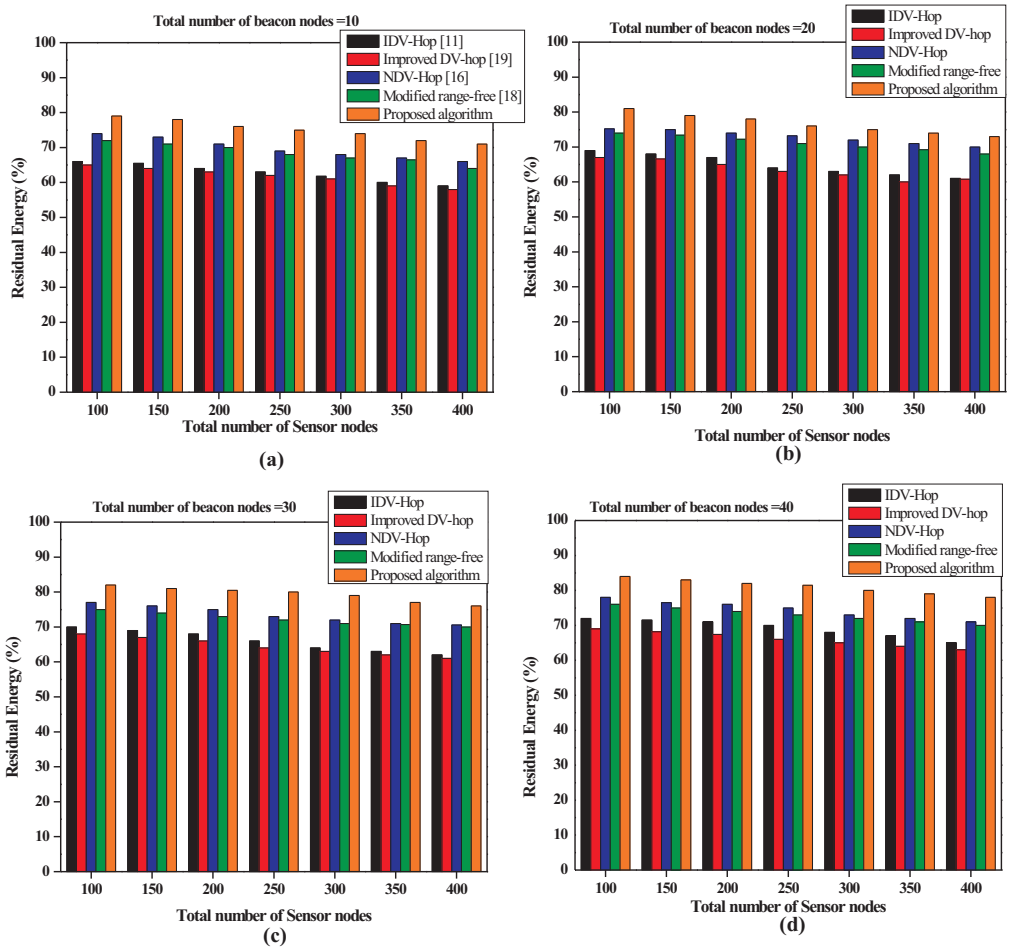

FIGURE 5.9: *Effect of ratio of beacon node and total sensor nodes on the percentage of Residual energy.*

5.3.2.7 Experiment 7: Effect of ratio of beacon nodes and total sensor nodes on LEV

To analyze the impact of the ratio of beacon nodes and node density on LEV, experiment 7 is conducted. For this experiment, a total of 100 to 400 sensor nodes are randomly deployed with 10 to 40% beacon nodes. The communication radius for sensor nodes is considered $25 - 40m$. The simulated results of all algorithms are depicted in Figure 5.11 and it is perceived from the results that both parameters affect the LEV significantly. It is interpreted from Figure 5.10 that as the ratio of beacon nodes and nodes density increases, the LEV decreased and the proposed algorithm outperforms in terms of localization accuracy as compared to existing ones.

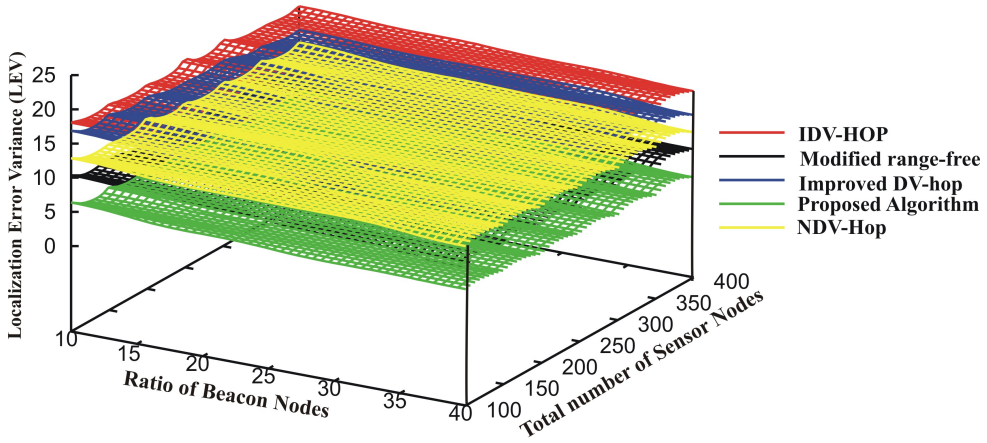

FIGURE 5.10: *Effect of variation in the ratio of beacon nodes and total sensor nodes on LEV.*

5.3.2.8 Experiment 8: Effect of Network Connectivity on localization

To measure the performance of the localization algorithm, proportion of localized nodes and unlocalized nodes are important metrics in WSNs. Also, the area of coverage in localization is the main parameter of concern. PLSN and PUSN are computed by varying the connectivity form 2 to 16 to evaluate the impact of network connectivity on coverage of the algorithms. The simulated results are demonstrated in Figure 5.11 and it can be observed from the figure that after approaching network connectivity 9, all the unknown nodes for the proposed algorithm are successfully localized. The simulated results reveal that the proposed algorithm has better coverage as compared to the existing algorithms.

5.3.2.9 Experiment 9: Computational Efficiency

The computational cost of an algorithm represents the measure of complexity and it is computed by estimating the time consumed to perform a specific task of an activity. Localization time is defined as the time required for computing the location of all unknown nodes. The simulated results of all algorithms are demonstrated in Figure 5.12. From the simulated results, it is perceived that the localization time of IDV-HOP [204] is lowest and Modified range-free [107] is faster as compared to all

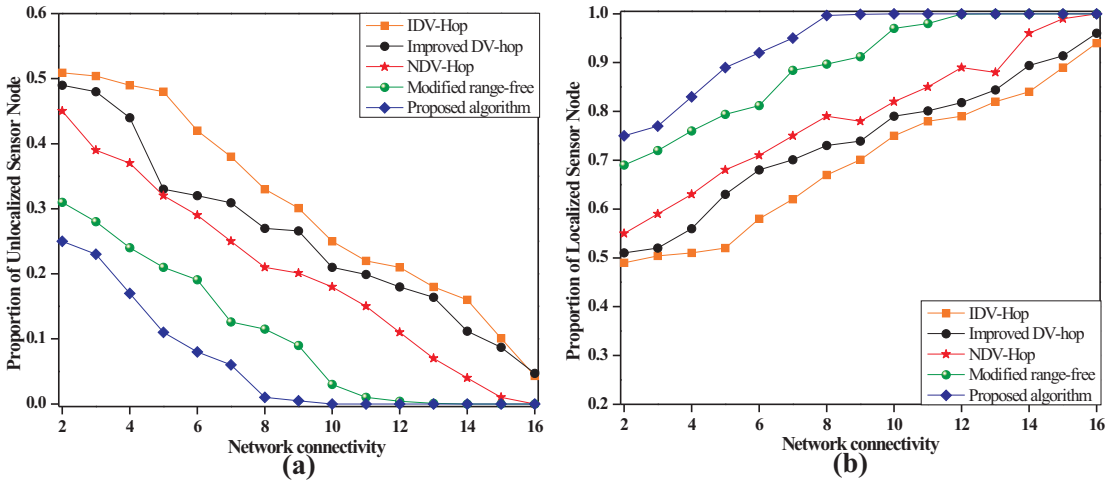

FIGURE 5.11: *Effect of network connectivity on (a)PUSN (b) PLSN.*

algorithm because of using TLBO for optimization. Localization time of the proposed algorithm is a bit faster than NDV-Hop [92].

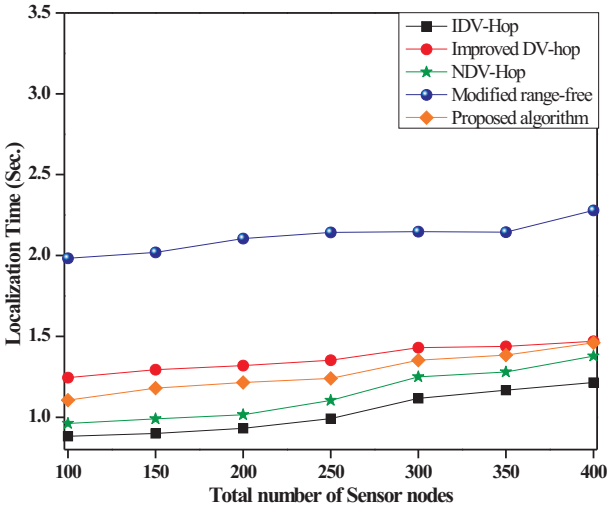

FIGURE 5.12: *Effect of variations in total sensor nodes on localization time.*

5.4 Conclusion

A range-free Power Efficient Cooperative-MAC (PECo-MAC) localization algorithm is proposed by using cooperative communication among sensor nodes in WSNs. in the proposed approach, a novel concept of cooperative transmission at MAC is considered instead of traditional direct transmission. To maximize the residual energy of sensor nodes, the location information from sensor nodes is communicated to BS by incorporating cooperative beacon nodes. The cooperative nodes are elected for cooperation on the basis of least energy consumption using an efficient and effective scheme. Total energy consumption of the network is significantly reduced by including this step which prolongs the network lifetime. Furthermore, the localization accuracy of the proposed algorithm is minimized by using correction factor for localization at BS. The localization at BS ensures the minimum messages exchange between sensor nodes as the location information is collected within one-hop neighbors. Moreover, the simulated results of the proposed approach are compared to the recent localization algorithms. It is observed from the simulated results that the proposed approach is more superior in terms of accuracy and energy efficiency. The proposed algorithm accomplishes about $65\%, 62\%, 51\%$ and 42% better accuracy as compared to IDV-HOP, NDV-Hop, Modified DV-Hop, and Improved DV-Hop respectively.

CHAPTER 6

Secure localization algorithm with Blockchain technology

6.1 Introduction

In Wireless Sensor Networks (WSNs), the tiny sensing devices are installed for observing the various physical activities [225] and these devices forwards the information to Base Station for further processing [226]. In some specific applications, to make information more authentic, location information of nodes play an important role in WSNs. The process of estimating the positions of sensor nodes is called localization [227]. In fact, the extension of WSNs from static to the dynamic environment was unavoidable due to the exponential growth of information technology that necessitated the monitoring and controlling of WSNs. In dynamic network scenarios, due to random deployment, hostile and remote areas of operation the process of localization are more exposable to various attacks. The malicious activities in the network affect the performance and operation of the sensor nodes significantly [228].

To mitigate and overcomes the problem of malicious activities, various secure localization algorithms were developed [167][63][229] which are classified into three groups: (1) localization based on robust observation; (2) localization based on the separation of malicious beacon nodes; and (3) localization is based on location verification. In the first group, the upper-bound limitation of distance among inter-sensor nodes disables the attacker to degrade the performance of localization process. In the second group, malicious node or fraud nodes are identified with the help of checkpoints for monitoring which avoid the fraud in the localization process. In third group, a set of sensor nodes are deployed with pre-scheduled locations to detect whether the localization process is trustworthy or not. However, all the groups have their own shortcomings and weakness [230].

The secure localization algorithms in the first group are unable to avoid malicious attacker which enlarge the measured distances between sensor nodes and also not capable to confirm exactly where unknown nodes lie. In the second group, the process of localization depends on the BS. Therefore, the processing of a large amount of information overloads the BS. Finally, in the third group, the deployments of all sensor nodes affect the performance of the localization algorithms significantly. The inadequacy of the above mentioned secure localization algorithms is known for some time and mitigation of the problem is slowly advancing in WSNs. Localization in WSNs plays a crucial role in various applications as we discussed earlier. It is most difficult to determine the positions of sensor nodes in the presence of malicious nodes and non-trusted environments. Hence, the accuracy of the localization process is a challenging issue in the presence of malicious nodes and attackers. To overcome this problem, secure localization approaches and trusted schemes based on blockchain technology are the two emerging techniques for localization. Due to rapid advancement in technology, the concept of blockchain has an emerging and great impact in the Internet of Things (IoT) which provides decentralization, interaction in a distributed manner, enabling new models and immutable data [186][231][189]. Blockchain and reinforcement-based trusted routing scheme has been proposed recently to provide additional security in

WSNs. Routing information of nodes is stored in the blockchain to make the tampering hard and reinforcement learning selects more trusted routing links [232].
The blockchain technology has been adopted to provides privacy to healthcare data in cloud computing. Blockchain consensus is decentralized in nature which reduces the influence of attacks and ensures the integrity and accountability of patient data [233]. Hence, it is interesting to test a trust evaluation based secure localization model using blockchain technology and that form the seed of this chapter.
The remaining parts of this chapter are organized as follows; the proposed network and attack model are described in section 6.2. Research methodology of the chapter is discussed in section 6.3. In section 6.4 the simulated results of the chapter are discussed with conclusion of the chapter explained in section 6.5.

6.2 Network and Attack Model

In this section, we have discussed the network model and attack model of the proposed algorithm. The network model represents the environments, roles, responsibility, and capability of sensor nodes utilized for the proposed algorithm and the perceptive of the attacker and malicious nodes are discussed in the attack model.

6.2.1 Network model

In the proposed network model, two types of sensor nodes such as beacon nodes or benign nodes and unknown nodes are considered for the localization process. For the network model, some assumptions are considered as follows:

- A set B having M beacon nodes are considered for localization. The locations of such nodes are prior known with the help of Global Positioning System (GPS).
- A set U having n unknown nodes are also considered and the locations of these nodes to be estimated using beacon nodes information.

- Therefore, the overall size of the proposed network model is given as follows:

$$|N| = |B| + |U|$$

- The beacon nodes can play one of the following roles i.e. Applicant and Validator. An applicant is a node who claims its location and a validator is one who verifies the claimed locations.

- Initially, the locations of beacon nodes are forwarded to their neighbor sensor nodes and the format for the broadcasted packets are as follows:

$$packet_i = \{Id_i, location_i^c, timestamp, E_{residual}^i\}$$

  where Id_i is the identification of i^{th} beacon node, $location_i^c$ is the measured position using beacon nodes, $timestamp$ represents the time stamp for each node and $E_{residual}^i$ is the residual energy of the beacon node.

- All the beacon nodes are able to find their position $location_{true}$ with GPS having no localization error.

- The beacon node reports its location $location^c$ and it is identical to $location_{true}$.

6.2.2 Attack model

An attacker or adversary can compromise or tamper the information of any beacon nodes and the compromised beacon node is called malicious beacon node. The main motive of the adversary or malicious node is to accomplish the position of bacon nodes and tamper the true identity of that particular beacon node. An attacker can perform the following behavior to benign nodes:

- The total $Malicious_i$, where $(i = 1, 2, ., k \ll M)$ nodes are considered as malicious beacon node in the network. M represents the total number of beacon nodes present in the network.

- Compromised beacon nodes can report false location packet intentionally to the neighbors as following:

$$packet_i^{false} = \{Id_i, location_i^c, timestamp, E_{residual}^i\} \therefore \text{where}$$
$$location_i^c \neq loctaion_{true}$$

- Malicious beacon nodes can receive information from all the nodes that lie in their communication area.
- Malicious beacon nodes can intentionally tamper the data and its integrity
- Selfish beacon nodes can broadcast or reports false energy information Malicious node intentionally reports false reputation of well-behaving nodes

6.3 Proposed Methodology

To prevent malicious activities and adversaries, the localization algorithm must be capable of countermeasure various types of attacks. If the malicious nodes or compromised nodes are identified by sensor nodes, they can easily handle the location information and estimates the location of unknown nodes precisely. Therefore, an effective trusty reputation localization algorithm is proposed to achieve more secure localization with high accuracy in WSNs. The main steps of the proposed algorithm are shown in Figure 6.1.

6.3.1 Trust evaluation

A trust model with blockchain technology is employed for secure localization to mitigate the compromised beacon nodes problem and to establish more trusty localization. The trust value of each beacon node is computed on the basis of different parameters i.e. reputation value, mobility, residual energy, and neighbor node list of beacon nodes. The distribution of malicious activities and forged information can be prevented by selecting highly trusty nodes for the localization. In trust evaluation,

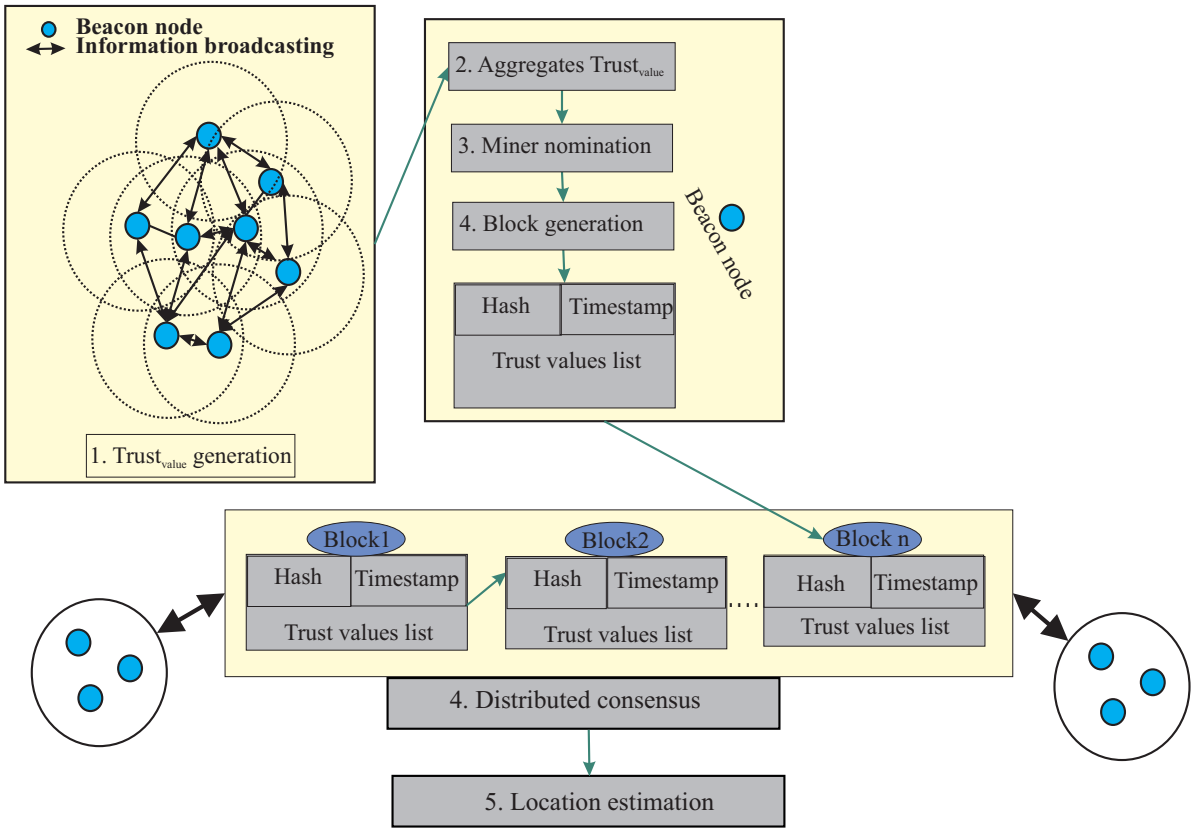

FIGURE 6.1: *Procedure of the proposed algorithm.*

beacon nodes evaluate each other based on the perception of positions and distribute the results to all beacon nodes. After trust evaluation, ranking to each beacon nodes are provided on the basis of received trust values. Different assumptions for trust evaluation are considered as follows:

1. Beacon and unknown nodes are mobile in nature.
2. Reputation value for each beacon nodes varies from 0 to 1 and indicating the lowest to highest reputation.
3. A medium value 0.5 is assigned to each beacon node as initial reputation value.
4. Beacon nodes evaluate the reputation values only for its one-hop neighbored beacon nodes.

6.3.1.1 Initialization:

Initially, all beacon nodes determine their one-hop neighbor nodes and enlist the nodes in Neighbor Node List (NNL). After that beacon node broadcasts its information to all neighbored beacon nodes with a timer T_{start}. The beacon node B_i which forwards the information towards the neighbor is represented by S^{BN} and the receiver node B_j is represented by destination node D^{BN}. The format of broadcasted packets is as follows:

$$S_j^{BN} \rightarrow D_i^{BN} : \{(x_j, y_j), Id_j, NNL, E_i^{residual}, T_j^{start}\}$$

In the aforementioned packet format, $E_i^{residual}$ represents the residual energy of S_j^{BN}. When the packets are received at D_i^{BN}, it stops the timer with (T_j^{stop}). d_{ij}^{co} represents the distance between nodes computed with the coordinates of nodes and d_{ij}^{sp} is the distance among nodes computed with speed or velocity of signal travelling. Further, the distance d_{ij}^{co} and d_{ij}^{sp} are computed between D_i^{BN} and S_j^{BN} with the help of coordinates information and velocity with One-Way Travel Time(OWTT), respectively. The procedure through which the distances are obtained is explained in Figure 6.2. Each beacon node evaluates the trust values of S_j^{BN} on the basis of various metrics like reputation value, NNL, residual energy, and mobility of nodes and these metrics are computed as follows:

1. Reputation value evaluation:

In this phase, the reputation values of each beacon node are computed. B1 and B2 represent the benign nodes and $B2$ is the malicious beacon node as shown in Figure 6.2. The distance d_{12}^{co} and d_{12}^{sp} among B2 and B1 are determined with the help of Equation 6.1 and 6.3 respectively. The honesty of beacon node B2 is ensured by B1 with comparing both distances d_{12}^{co} and d_{12}^{sp}. If both the distances are equal $d_{12}^{co} = d_{12}^{sp}$ that means B2 node is benign beacon node otherwise it is considered as a malicious node. In Figure 6.2, $B2$ is a malicious beacon node because of the distances d_{12}^{co} and d_{12}^{sp} are not same. The range of reputation value is depicted in Figure 6.3.

$$d_{ij}^{co} = \sqrt{(x_i - x_j)^2 + (x_i - y_j)^2} \ \ (i \neq j) \tag{6.1}$$

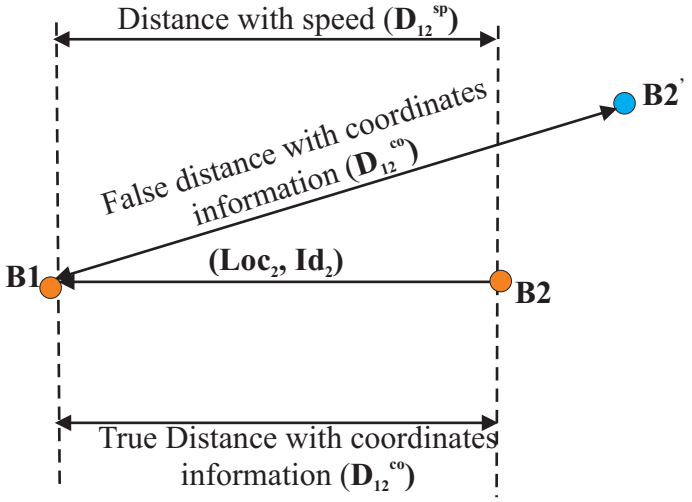

FIGURE 6.2: *Example of distance estimation.*

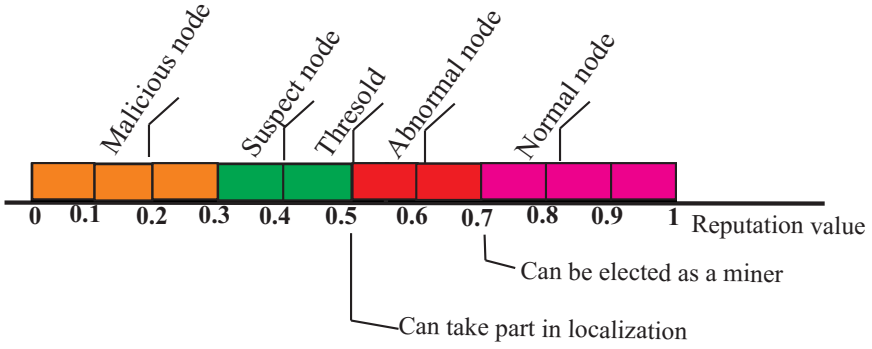

FIGURE 6.3: *Range of reputation value.*

$$\begin{cases} \text{Malicious node:} & 0 \leq R_P < 0.3 \\ \text{Suspect node:} & 0.3 \leq R_P < 0.5 \\ \text{Abnormal node:} & 0.5 \leq R_P < 0.7 \\ \text{Normal node:} & 0.7 \leq R_P \leq 1 \end{cases}$$

In the aforementioned equation, (x_j, y_j) and (x_i, y_i) are the coordinates of D_j^{BN} and S_i^{BN} respectively.

$$OWTT = T^{stop} - T^{start} \tag{6.2}$$

$$d_{ij}^{sp} = c \times OWTT, \quad \text{where c is the speed of light} \tag{6.3}$$

$$\begin{cases} (Rp)_{t+\Delta t}^{B_{ij}} = \varphi \times (Rp)_t^{B_{ij}} + (1-\varphi), \quad if|d_{co} - d_{sp}| \leq d_{Th} \\ (Rp)_{t+\Delta t}^{B_{ij}} = (1-\varphi) \times (Rp)_t^{B_{ij}}, \quad if|d_{co} - d_{sp}| > d_{Th} \end{cases} \tag{6.4}$$

In the above equation, $(Rp)_t^{(B_{ij})}$ and $(Rp)_{(t+\Delta t)}^{(B_{ij}}$) are the reputation values of B_i by B_j at times t and $(t + \Delta t)$ respectively, Δt is the time interval between reputations and d_{Th} represents the threshold distance.

$$\varphi = \frac{|d_{ij}^{co} - d_{ij}^{sp}|}{(d_{ij}^{co} + d_{ij}^{sp})} \tag{6.5}$$

The value of a reputation for each beacon nodes lies in the range of 0 to 1 ($R_P \in [0, 1]$).

2. Mobility:

Due to fast-emerging technology, the dynamicity of sensor nodes is highly desired in the localization process. Mobility is the most challenging concern in WSNs localization and plays a vital factor which disturbs the network topology and protocols. Therefore, in dynamic networks, selection of appropriate beacon nodes with low speed is most crucial in localization. The unknown nodes move out from the range of beacon nodes immediately, if the beacon nodes with higher speed are selected which may accomplish error-prone locations. Also, the high mobility of beacon nodes affects the stability and performance of the localization algorithm. Therefore, relative mobility ($RM_{i,j}$) of the sensor nodes is computed which delineates that the nodes are moving far or coming closer to each other. ($RM_{i,j}$) is determined as follows:

$$d_{ij}^t = \sqrt{(x_i^t - x_j^t)^2 + (y_i^t - y_j^t)^2} \tag{6.6}$$

$$d_{ij}^{t-1} = \sqrt{(x_i^{t-1} - x_j^{t-1})^2 + (y_i^{t-1} - y_j^{t-1})^2} \tag{6.7}$$

$$RM_{ij} = d_{ij}^t - d_{ij}^{t-1} \tag{6.8}$$

In the aforementioned equation, (x_i^t, y_i^t) and $(x_i^{(t-1)}, y_i^{(t-1)})$ are the coordinates of Bi and coordinates of Bj are represented by (x_j^t, y_j^t) and $(x_j^{(t-1)}, y_j^{(t-1)})$ at time t and $(t-1)$ respectively. The relative mobility can be positive or negative but it must be small.

3. Residual energy

For trust evaluation, the residual energy of beacon nodes is also an important parameter. The energy model considered in the proposed algorithm is same as [234] for computing the residual energy. The cost of transmission of the k-bit packet to a distance D is computed as follows:

$$E_{Tx}^{j}(k, D) = kE_{elec} + kE_{amp}D^2 \tag{6.9}$$

In the aforementioned equation, E_{elec} and E_{amp} are the required energy for electronic circuitry and amplification respectively.

$$E_{Rx}^{j}(k) = kE_{elec}, \quad where(j = 1, 2, 3, , m) \tag{6.10}$$

where $E_{Rx}^{i}(k)$ represents the required energy to receive k-bit information within the transmission range. Hence, the total energy consumption of the beacon node is computed by the following equation:

$$E_{consumption}^{j}(k) = E_{Tx}^{j}(k, D) + E_{Rx}^{j}(k) \tag{6.11}$$

Now the residual energy is computed as follows:

$$E_{residual}^{j}(k) = E_{Initial}^{j} - E_{consumption}^{j} \tag{6.12}$$

4. Neighbors Node List (NNL)

In the proposed algorithm, we have considered the transmission up to one hop and set of neighbors nodes $N(j)$ is computed as follows:

$$N(j) = \sum_{(i \in N, i \neq j)} \{i | d_{ij} < R|\} \tag{6.13}$$

The set $N(j)$ defines the degree of connectivity of B_j and is computed as:

$$Degree_j = |N(j)| \tag{6.14}$$

After discovering the neighbor nodes, B_j constructs an NNL list with all its neighbors.

5. Trust value Evaluation:

Each beacon node B_j evaluates the trust value for B_i on the basis of $(Rp)^{B_{ij}}_{(t+\Delta t)}, RM_{ij}, E^j_{residual}$ and NNL. The trust value is computed according to a weighted sum decision model, given by the following Equation:

$$Trust^j_{value} = \omega_1 \times (Rp)^{B_{ij}}_{t+\Delta t} + \omega_2 \times (\frac{1}{|RM_{ij}|}) + \omega_3 \times log(E^j_{residual}) + \omega_4 \times log(NNL) \tag{6.15}$$

where $\omega_1, \omega_2, \omega_3$ and ω_4 represents the weighting factors for the corresponding parameters of the algorithm. The weighting factors considered for the present model reflect the relative importance of the $(Rp)^{B_{ij}}_{(t+\Delta t)}, RM_{ij}, E^j_{residual}$ and NNL.

$$\{\omega_1 + \omega_2 + \omega_3 + \omega_4 = 1\} \tag{6.16}$$

The weights considered for evaluating trust value are $\omega_1 = 0.4, \omega_2 = 0.2, \omega_3 = 0.3$ and $\omega_4 = 0.1$. Finally, the trust value of B_i is broadcasted across the network by B_j. The format of the packet is $\{B_j$broadcast trust value : $(Id_j, Id_i, Trust^j_{value}, msg_{id}\}$, where Id_i is the identification of D_{BN}, Id_j and $Trust^i_{value}$ are the identification and trust value of S_{BN} and P_{id} is the identifier of the packet. Each beacon node gets the trust value of every beacon nodes in the network and constructs a matrix of trust value at time t as follows:

$$M^t_{trust} = \begin{pmatrix} Trust^{11}_{value} & Trust^{12}_{value} & .... & Trust^{1m}_{value} \\ Trust^{21}_{value} & Trust^{22}_{value} & .... & Trust^{2m}_{value} \\ .... & .... & ..... & .... \\ .... & .... & .... & .... \\ Trust^{m1}_{value} & Trust^{m2}_{value} & .... & Trust^{mm}_{value} \end{pmatrix} \tag{6.17}$$

$Trust^{ij}_{value}$ is the trust value of B_j to its neighbor node B_i, where $i, j \in m$ and the trust value to itself $Trust^{jj}_{value}$ is discarded to maintain fairness. Finally, beacon nodes put all these trust values in the matrix and try to add it into the blockchain.

6. Miner election and block generation

Blockchain technology is an emerging technology with decentralized or distributed network structure. It was invented by Satoshi Nakamoto to abstract the well digital currency i.e. the Bitcoin [235]. It utilized the peer to peer technology for different transactions. Due to decentralized attributes of blockchain, it provides transparency, trust, and immutability to transactions. The information stored in the blockchain is publicly available to the networks [236][237][238]. In blockchain technology, there is no central control to manage the transactions because of its decentralized nature. All the participants in the blockchain technology have equal rights and position and they have same copy of all transactions. Therefore, because of immutability attributes no one can alter the recorded information in blockchain unless he has obtained strong enough capacity to confuse the crowds. It ensures the more privacy, reliability, and security to the information due to which it has been widely applied in different applications recently [239]. The blockchain consists of a list of blocks to store the transaction, where each block have a number of transactions. For secure localization, a blockchain of trusted values is generated in this chapter. The trust values of each beacon nodes are stored in blocks and a miner is periodically is elected among all beacon nodes to generate blocks. For miner selection, the concept of Proof of Work (PoW) is generally used in blockchain which confirms the transaction to generate new blocks in blockchain [240]. In PoW consensus mechanism, a complicated mathematical puzzle is given and miners try to solve that particular puzzle. The miners who solve the puzzle first would be elected as a miner and add the transaction in the block. All the transactions must be validated carefully. The PoW process consumes a lot of power and resources in solving the complicated mathematical puzzle. Therefore, the concept of Proof of stake (PoS) is used in proposed algorithm for validating the transactions. The PoS works in a similar way to PoW, but the method to accomplish the objective is totally different. The miners for block generation are elected in deterministic way

on the basis of $Trust_{value}$. The beacon node with highest $Trust_{value}$ is selected as a miner and adds blocks to the blockchain. The verification of the block is done by other beacon nodes and structure of the block is depicted in Figure 6.4. In the proposed algorithm, the trustworthiness of the node is used in place of reward or transaction fee as incentives. However, the trustworthiness of the node cannot be spent or transferred which is totally different to coins and higher $Trust_{value}$ beacon nodes can offer superior services.

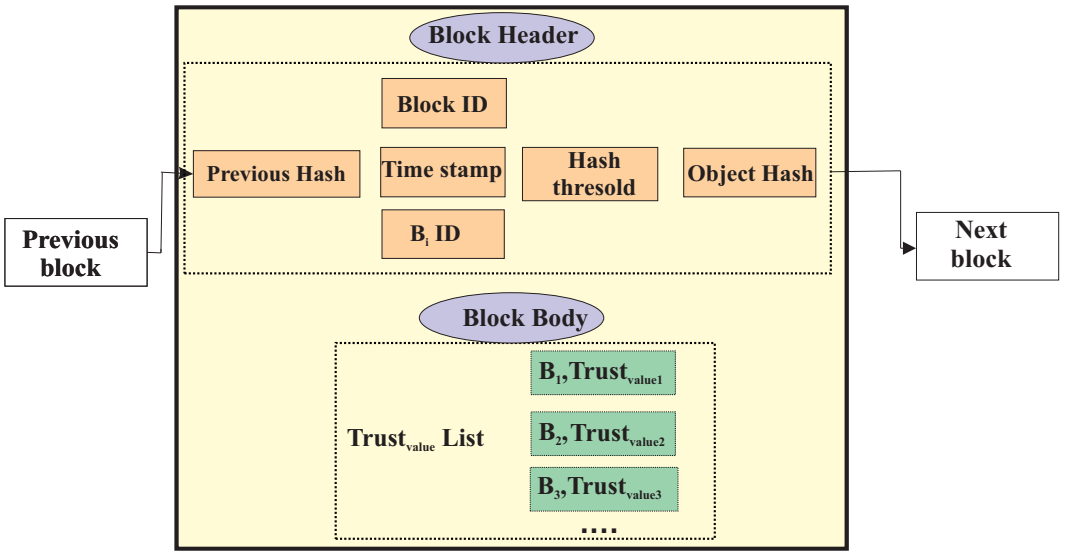

FIGURE 6.4: *Blockchain structure.*

7. Distributed consensus

After generating a block, the validity of the block is ensured by beacon nodes. After verification, the block is added to the blockchain. Sometimes, it may happen that two or more blocks are generated at the same time and broadcasted across the network. The beacon nodes receive two or more blocks at a time. In such situations, blockchain starts fork and one of the forks is randomly selected to continue adding a new block. Finally, the longest chain becomes the distributed consensus and remaining forks of the chain are eliminated from the network. In this way, each beacon nodes store the blockchain which ensures the consistency of the network.

6.3.2 Localization process:

After the blockchain generation of trust values, the process of localization is initialized for estimating the locations of unknown nodes. For the localization process, most trusty beacon nodes are selected. The beacon nodes with higher trust values ensure the more precise locations of unknown nodes. In the proposed algorithm, m beacon nodes and n unknown nodes are randomly deployed. The coordinates of beacon nodes are represented by $[(x_1, y_1), (x_2, y_2), ..., (x_m, y_m)]$. The geographical locations of unknown nodes $[(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)]$ are discovered by trustworthy beacon nodes. The distance between beacon node i and unknown node u is computed as follows:

$$D_{iu}^{est} = c \times OWTT \tag{6.18}$$

The estimated distance D_{iu}^{est} has some localization error due to system noise. Thus, the distance can be represented as follows:

$$D_i = D_{iu}^{est} + \xi \tag{6.19}$$

$$\xi \sim N(0, \sigma^2) \tag{6.20}$$

In the aforementioned equation, ξ is the normally distributed measurement error with mean 0 and variance σ^2 depending upon the existing environment [241]. As the distance among nodes increases, the localization error of unknown nodes decreases gradually. Also, the difference in actual distance (D_{iu}^{act}) and measured distance (D_{iu}^{est}) between beacon nodes and unknown nodes increases with distance.

$$D_{iu}^{act} = \| X_u - X_i \|_2 = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2)} \tag{6.21}$$

where $X_u = [x_u, y_u]^T$ and $X_i = [x_i, y_i]^T$ represents the coordinates of the unknown node u and beacon node i respectively. The estimated distance D_{iu}^{est} has some deviation from the actual distance d_{iu}^{act} due to noise or measurement.

$$\varepsilon = (\sqrt{(x_u - x_i)^2 + (y_u - y_i)^2}) - D_{iu}^{est}) \tag{6.22}$$

In localization, the difference between D_{iu}^{est} and d_{iu}^{act} in WSNs obeys the normal distribution [242], therefore the error function can be described as following:

$$\sigma_N(d^{est}) = ae^{\frac{-(d^{est}-d^{act})^2}{\sigma^2}} \tag{6.23}$$

where $\sigma_N(d^{est})$ refers to the Gaussian function of distance d^{est}. In the above Equation, $d^{est} = d^{act}$ represents the measurement location error reaches its maximal value. For location estimation of unknown nodes, a set of beacon nodes such as:

$$[(x_1, y_1, d_{1u}, trust_{value}^1), (x_2, y_2, d_{2u}, trust_{value}^2), ..., (x_i, y_i, d_{iu}, trust_{value}^i)]$$

where (x_i, y_i) indicates the set of coordinates of beacon node i, d_{iu} indicates the distance between i and unknown node u and $trust_{value}^i$ represents the set of trust values of beacon node i. The coordinates of the unknown node (x_u, y_u) is computed using the least square method, however, the estimation function of the localization process is defined as follows:

$$D_i^2 = \| X - X_i \|_2 + \lambda) \quad where(X = (x, y)) \tag{6.24}$$

$$(x, y) = argmin \sum_{i=1}^{m} (\sqrt{(x_i - x_u)^2 + (y_i - y_u)^2}) - D_i)^2 \tag{6.25}$$

where λ is the location error due to measurement and $\lambda \sim U(-\varepsilon, \varepsilon)$, while the maximal measurement error ε is represented as follows:

$$max|D_i - \sqrt{(x_i - x)^2 + (y_i - y)^2)} \mid \leq \epsilon \tag{6.26}$$

In the proposed network model, different types of security threats are considered

such as i) Broadcasting false location information, ii) Impersonation, iii) Tampering with the integrity of information, iv) Reports false energy information to misguide the trust evaluation process. Consequently, to improve localization accuracy and security, the proposed trust model must address potential problems resulting from the above-mentioned attacks.

6.4 Results and Discussion

For evaluating the performance of the proposed algorithm, the simulated results are presented in this section. The simulation parameters of the present study are described in Table 6.1. The performance of the proposed algorithm is compared with existing algorithms such as Reputation-based algorithm [243], Collaborative-secure algorithm [161], Colluders resistant algorithm [63] and RSS-based algorithm [178]. The simulated results are evaluated on various performance metrics such as average localization error, localization error variance, execution time and malicious node detection. For performance evaluation of all algorithms, the simulation is conducted in Matlab. All the sensor nodes including beacon nodes as well as unknown nodes are distributed in the area of $100 \times 100m^2$ as demonstrated in Figure 6.5. Total 100 sensor nodes with 25% beacon nodes, 5% malicious beacon nodes and remaining unknown nodes represented with green, red and black color respectively are considered in Figure 6.5.

TABLE 6.1: *Simulation parameters*

Simulation Parameters	**Value**
Sensing field	$100 \times 100m^2$
Total sensor nodes	100
Beacon nodes	$10 - 40\%$
Malicious node	$5 - 30\%$
Communication radius	$10 - 40$
Network topology	Random way point model
Hash algorithm	SHA-256
Initial energy	$5J$
Speed	$0 - 20m/s$

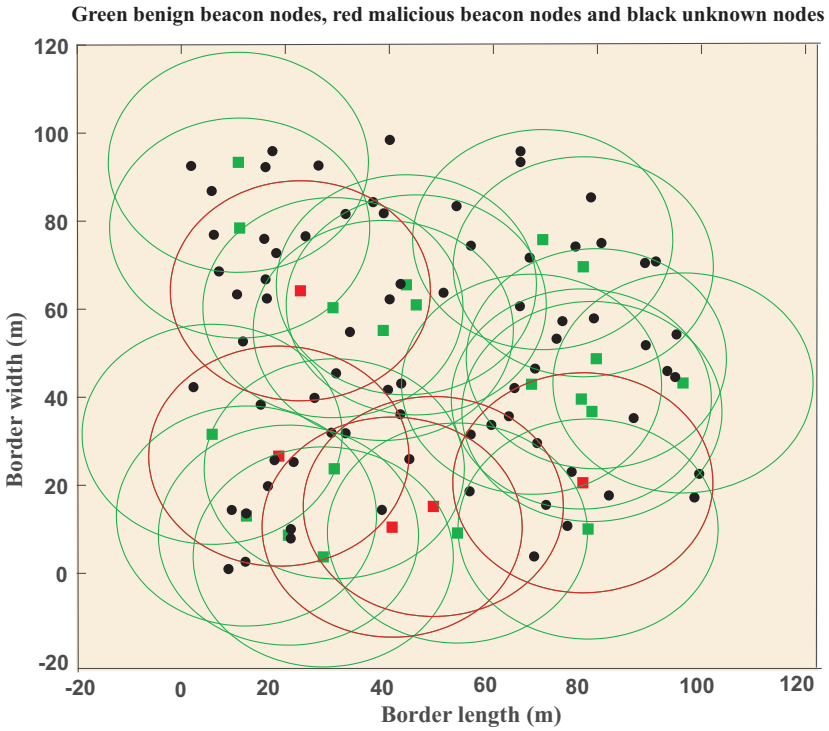

FIGURE 6.5: *Random Distribution of sensor nodes.*

6.4.1 Simulation Metrics

Various performance metrics are considered to measure the effectiveness of the proposed algorithm and these metrics are as follows:

6.4.1.1 Localization Error (LE):

The LE (ϕ) is the difference between the estimated position and the true position of the unknown node. The LE is computed using as following:

$$\phi = \sqrt{(x_i^{est} - x_j^{act})^2 + (y_i^{est} - y_j^{act})^2)} \tag{6.27}$$

where (x_j^{exp}, y_j^{exp}) and (x_j^{exp}, y_j^{exp}) represents the estimated coordinates and true coordinates of the unknown nodes respectively.

6.4.1.2 Average Localization error (ALE):

Another metric for results evaluation is ALE (Avg_error) and computed by using as follows:

$$Avg\_error = \frac{\sum_{i,j=1}^{n} \sqrt{(x_i^{est} - x_j^{act})^2 + (y_i^{est} - y_j^{act})^2)}}{n \times R} \tag{6.28}$$

6.4.1.3 Localization error variance (LEV):

LEV is another metric that is used for performance evaluation of different algorithms and it is denoted by $loc\_variance$. LEV is enumerated by using the following equation:

$$loc\_variance = \sqrt{\frac{\sum_{i,j=1}^{n} (\sqrt{(x_i^{est} - x_j^{act})^2 + (y_i^{est} - y_j^{act})^2} - (Avg\_error \times R))^2}{n \times R^2}} \tag{6.29}$$

6.4.2 Simulation results

In this section, the simulated results of the proposed algorithm are presented and compared with different existing algorithms. For the performance evaluation, different simulated tests are conducted as follows:

- **Test 1:** *Localization error with and without trust evaluation*
- **Test 2:** *Effect of ratio of malicious and benign beacon nodes on ALE*
- **Test 3:** *Effect of ratio of malicious and benign beacon nodes on the probability of true location*
- **Test 4:** *Effect of sensor nodes on ALE and LEV*
- **Test 5:** *Effect of simulation time on ALE and LEV*

- **Test 6:** *Effect of simulation time on detection ratio*
- **Test 7:** *Comparision of residual energy with simulation time*

6.4.2.1 Test 1: Localization error with and without trust evaluation

The impact of trust evaluation scheme on localization error is examined in Test 1. For the simulation, 100 sensor nodes are randomly deployed with 20% benign beacon and 5% malicious beacon nodes. The localization error for each unknown nodes with and without trust evaluation are illustrated in Figure 6.6. From the simulated results, it is perceived that the localization errors with trust evaluation significantly decrease.

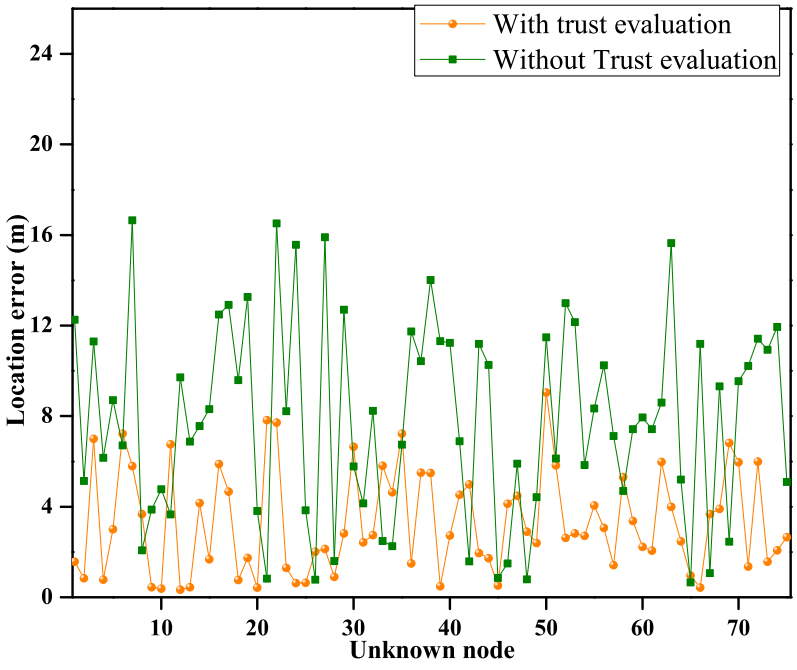

FIGURE 6.6: *Location error of every unknown node at any point for a specific simulation.*

6.4.2.2 Test 2: Effect malicious and benign beacon nodes on ALE

In Test 2, the impact of the ratio of benign beacon node and malicious beacon nodes on ALE is evaluated. For test 2, benign nodes ratio varies from 10 to 40% and malicious nodes ratio varies from to 30% of benign nodes. The simulated results are illustrated in Figure 6.7. The impact of ratio of malicious nodes on ALE is shown in Figure 6.7(a) which expressed that the ALE increases as the ratio of malicious nodes increases. The effect of ratio of benign beacon nodes on ALE is presented in Figure 6.7(b). From the simulated outcomes it was demonstrated that ALE reduces for all algorithms when the proportion of benign nodes increases and proposed algorithm gives more precise localization in contrast to existing ones. The performance comparison of various algorithm with proposed algorithm is terms of ALE is tabulated in Table 6.2. Reputation-based algorithm [243], Collaborative-secure algorithm [161],

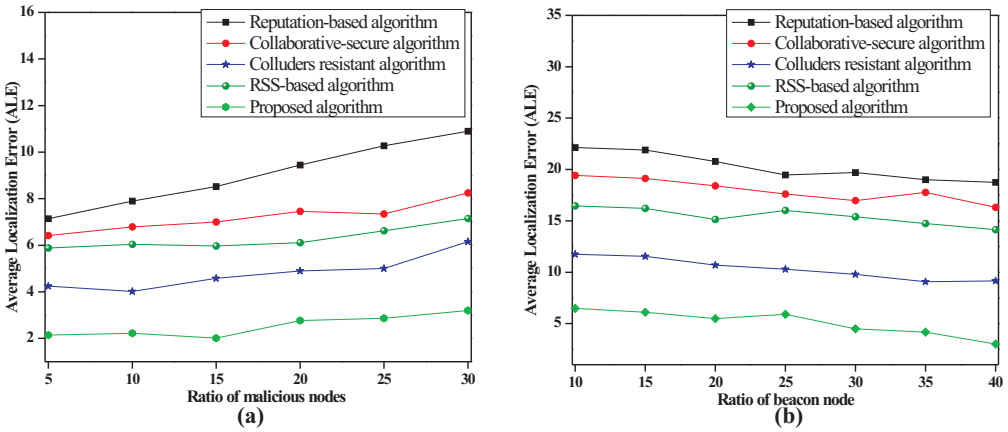

FIGURE 6.7: *Comparison of ALE: (a) Effect of malicious nodes and (b) Effect of benign nodes.*

Colluders resistant algorithm [63] and RSS-based algorithm [178]

TABLE 6.2: *Localization error comparison with varying ratio of malicious nodes*

Localization algorithm	% of benign beacon nodes	% of malicious beacon nodes	ALE
Reputation-based algorithm	40	5	16.875
		10	17.426
		15	17.998
		20	18.756
		25	19.758
		30	20.785
Collaborative-secure algorithm	40	5	7.478
		10	8.125
		15	8.997
		20	9.1498
		25	10.478
		30	11.175
Colluders resistant algorithm	40	5	8.124
		10	8.786
		15	9.391
		20	10.701
		25	10.998
		30	11.763
RSS-based algorithm	40	5	12.103
		10	12.804
		15	13.555
		20	14.142
		25	15.107
		30	16.119
Proposed algorithm	40	5	2.782
		10	3.897
		15	3.992
		20	4.0114
		25	4.887
		30	5.598

6.4.2.3 Test 3: Effect of ratio of malicious and benign beacon nodes on the probability of true location

In test 3, the impact of the ratio of malicious nodes and benign beacon nodes on the probability to find true locations of unknown nodes is examined. The simulated results of all algorithms by varying ratio of malicious beacon nodes are demonstrated in Figure 6.8(a) and it is observed that the probability decreases as the ratio of malicious

beacon nodes increases. In Figure 6.8(b), the effect of ratio of benign beacon nodes on the probability of finding true locations is illustrated and it is examined from the simulated results that the probability increases as the ratio of benign beacon nodes increase for all algorithms. However, the proposed algorithm performs excellent as compared to existing ones.

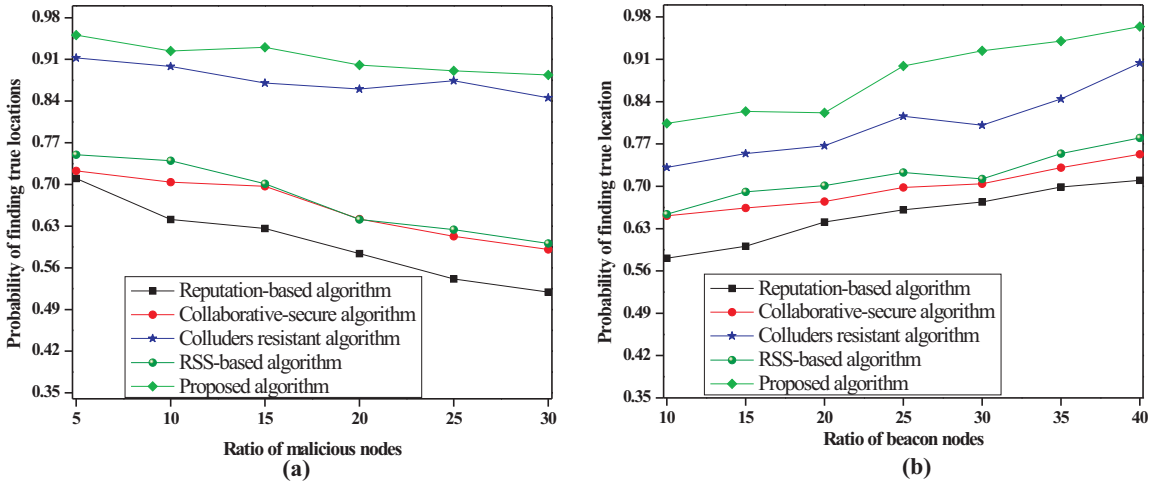

FIGURE 6.8: *Probability of localization by varying (a) ratio of malicious nodes (b) ratio of beacon nodes.*

6.4.2.4 Effect of sensor nodes density on ALE and LEV

To examine the impact of node density on ALE and LEV, Test 4 is conducted. The simulated results of all algorithms are demonstrated in Figure 6.9 by varying node density. The impact of node density on ALE is illustrated in Figure 6.9(a) and on LEV is shown in Figure 6.9(b). The simulated results illustrate that as the node density increases both ALE and LEV for all algorithms decreases significantly. It happens due to fact that the additional location information can be collected when the node density increases. From the simulated results, it is observed that the proposed algorithm performs effectively and efficiently as compared to existing ones.

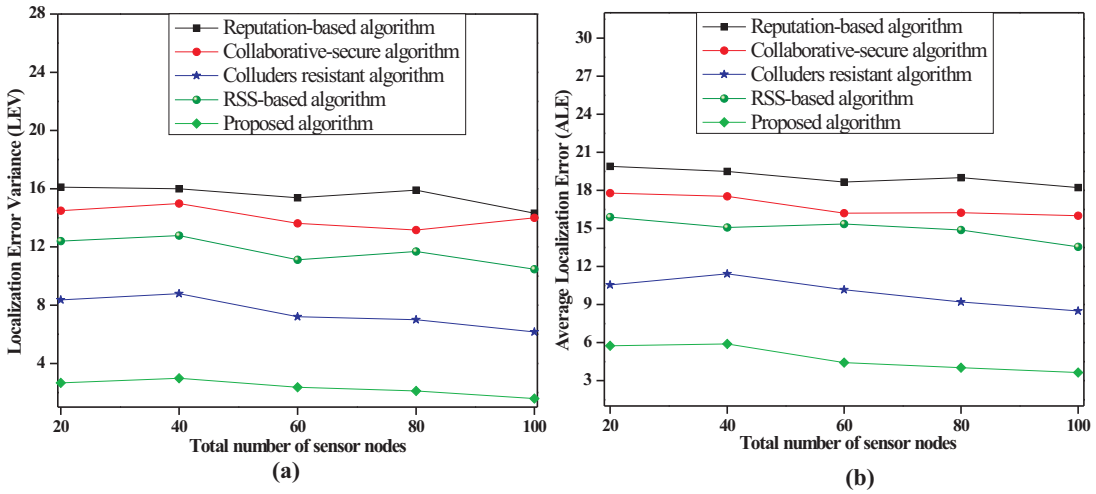

FIGURE 6.9: *Effect of sensor node density on (a) LEV (b) ALE.*

6.4.2.5 Test 5: Effect of simulation time on ALE and LEV

The number of simulation rounds defines the number of times of network deployment. The impact of simulation time on ALE and LEV is examined in Test 5. The simulated results of all algorithms are demonstrated in Figure 6.10. Impact of simulation time on LEV and ALE are illustrated in Figure 6.10(a) and 6.10(b) respectively. It is observed from the simulated results that LEV and ALE are almost the same with an increasing number of simulation time. Therefore, it is concluded from the simulated results that the localization process does not affect by a variety of network topology.

6.4.2.6 Test 6: Effect of simulation time on detection ratio

Impact of simulation time on detection ratio is examined in Test 6 and the simulated results are presented in Figure 6.11. It is observed from the simulated results that the detection ratio increases as the simulation time of the algorithms increases. Figure 6.11 shows that the proposed algorithm detects malicious attacks with least simulation time to simulate than existing algorithms effectively.

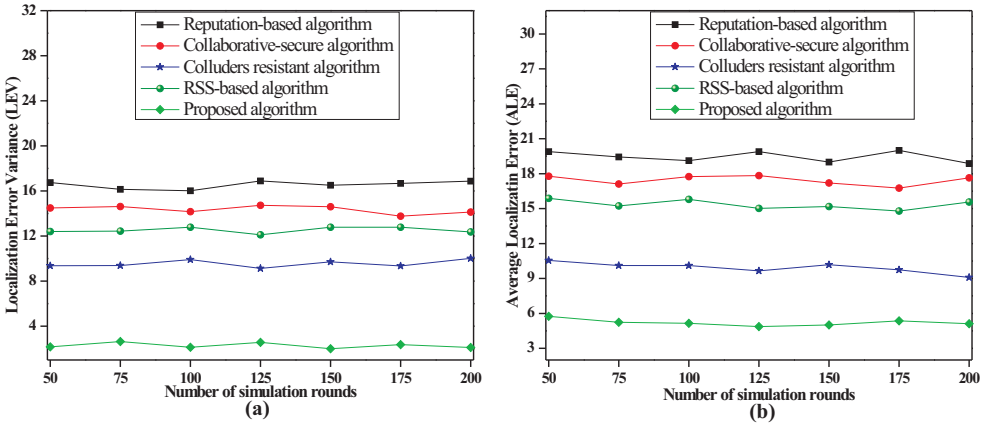

FIGURE 6.10: *Impact of simulation rounds on (a) LEV (b) ALE.*

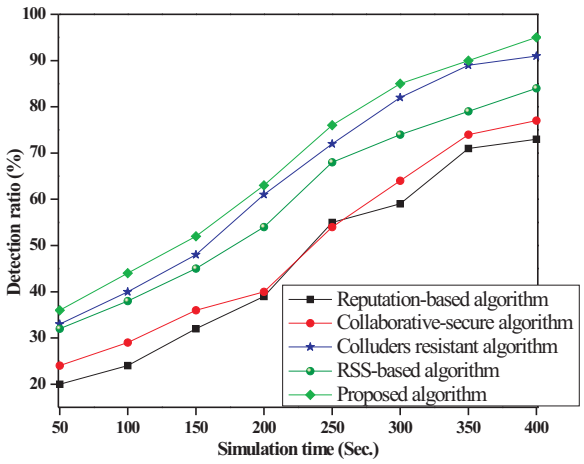

FIGURE 6.11: *Comparison of malicious detection ratio with simulation time.*

6.4.2.7 Test 7: Comparision of residual energy with simulation time

The percentage of residual energy with respect to simulation time is evaluated in Test 7 and is compared to existing algorithms such as Reputation-based algorithm [243], Collaborative-secure algorithm [161], Colluders resistant algorithm [63] and RSS-based algorithm [178]. From the simulated results shown in Figure 6.12, it is concluded that the Reputation-based algorithm [243] consumes the least power as compared to other algorithms. The proposed algorithm consumes more energy as compared to Reputation-based algorithm [243], Collaborative-secure algorithm [161] and

RSS-based algorithm [178]. For blockchain generation and trust evaluation, the proposed algorithm needs more energy and introduces more communication overheads. However, it ensures more security and privacy to the networks. Further, the proposed algorithm performs effectively and efficiently in terms of security, localization ratio, and accuracy. So, we can sacrifice the energy of the network to improve the localization accuracy and performance of the secure localization algorithm.

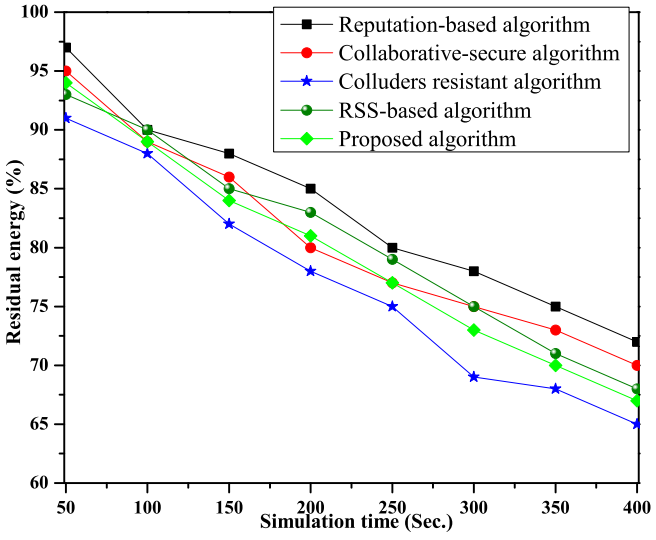

FIGURE 6.12: *Comparison of residual energy with simulation time.*

6.5 Conclusion

In this chapter, a trust-based range-free algorithm is proposed for secure localization in WSNs. Blockchain technology is utilized for sharing the trust values of beacon nodes with neighboring beacon nodes. The trust values of each beacon node are evaluated on the basis of different metrics such as reputation value, mobility, residual energy, and neighbor node list. The evaluated trust values of each beacon node are stored in the chain for security purpose. For adding the blocks, the beacon node with higher trust value is selected as a miner for mining of blocks. Further,

the localization process is performed by most trusty nodes so that more precise location can be accomplished. To analyze the effectiveness of the proposed algorithm, different simulations are performed in Matlab and the simulated results are compared with existing algorithms. The simulated results prove the efficacy of the proposed algorithm which discriminates malicious beacon nodes significantly and improves the performance in terms of localization accuracy with resist network topology variety and localization ratio.

CHAPTER 7

Conclusion & Future Scope

The organizations of this chapter as follows: In Section 7.1 general descriptions about proposed algorithms are discussed. Section 7.2 summarizes the research work of the thesis by emphasizing the major contributions of the proposed algorithms in localization. The future research direction of the research work is discussed in Section 7.3.

7.1 General

Wireless Networks are growing rapidly over the past few decades and it becomes an emerging and fast technology with lots of exciting actions and communication technologies. There are a number of ways to describe a wireless network and it can be defined as a global network of interconnected objects based on conventional communication protocols that are only addressable. It includes various typologies of fixed, mobile, two-way radios, portable, mobile, laptop, wireless network and personal digital assistant (PDAs). Recent advancements have introduced new networks called Wireless Sensor Networks (WSNs), including a wide range of concepts to satisfy multiple

human wishes. The growth in low-power and highly-integrated electronic equipment has resulted to the growth of micro-sensors which are capable to perform sensing tasks. The primary focus of the thesis is on WSNs which consists of a big amount of sensor nodes that allow physical phenomena in different environmental circumstances to be observed.

WSNs are considered as enabling technology of an emerging field which is envisaged to solve the different problems, thus facilitating the accommodation of new advanced services and providing efficient solution to the ever-increasing user demands. The WSNs make the association between the physical world and the digital world by seizing and exposing the phenomena of the real world. These phenomena can be converted into a form that can be easily assessable, storable and actable. These networks can support to evade terrible infrastructures failures, conserve exquisite natural resources, improve productivity, provide more secure communication, and also enable various smart applications such as smart home technologies. The happening events of surroundings are generally important for sensor nodes in WSNs and without knowledge of locations of an event, the information gathered by sensing devices are inadequate. The process of assigning the geographical locations to sensor nodes is termed as localization and it is a challenging concern in WSNs. Also, several challenges are faced during the location estimation process such as network lifetime, security, cost-complexity, and performance, etc. Therefore, the localization process should be capable to locate sensor nodes with minimum resources utilization to improve the performance. It should be accomplished to perform location estimation process more precisely.

In this context, the main motive of this thesis is to study range-free localization approach with energy-efficiency and security. This thesis is structured into three key sections which cover three major objectives of the research are as follows:

1. *To develop an optimized DV-Hop algorithm for minimizing the localization error.*
2. *To develop an energy-efficient framework for localization algorithm on Media Access Control layer.*

3. *To address the security concerns in the localization algorithm under the presence of adversary nodes.*

For each objective mentioned above, a unique solution is provided by considering random network scenario with mobility having limited resources. The first two objectives are based on the accuracy and energy-efficiency of the localization process. In the third objective, the security issues of the localization algorithm are addressed. In the next section, we have summarized the crucial findings for each objective.

7.2 Summary of Important Findings

1. To develop an optimized DV-Hop algorithm for minimizing the localization error.

WSNs are generally employed in several IoT applications. These networks are comprised of tiny sensing devices for capturing physical phenomena. To interpret the detected information significantly, the location of sensor nodes are essential in WSNs. Hence, location sensor nodes are the most important and crucial issue of concern because precise locations of nodes are required in functioning of several applications. Different localization algorithms have been proposed for precise localization in recent past. An advanced DV-Hop algorithm is proposed for computing accurate locations of nodes by utilizing minimum resources as described in Chapter 4. Firstly, a virtual backbone of the beacon nodes is constructed for efficient localization termed as Energy-Efficient Connected Dominating Set (EECDS). The beacon nodes are prioritized for EECDS on the basis of their degree of connectivity with one-hop neighbored unknown nodes and residual energy. Further, the localization error of the proposed algorithm is reduced by utilizing modified hop-size. The concept of collinearity is also considered which ensures that only non-collinear beacon nodes take part in localization process. The main motive of the proposed algorithm is To localize the unknown nodes effectively and efficiently by optimizing the energy of beacon nodes is the main motive of the proposed algorithm.

Extensive simulations are performed to analyze the effect of the proposed algorithm by considering different network scenarios and the comparative analysis with existing algorithms are performed. From the simulated results it is observed that the proposed algorithm gives 50%, 42%, 35%, and 22% more accurate localization as compared to other previously used algorithms.

2. To develop an energy-efficient framework for localization algorithm on Media Access Control layer.

In WSNs, localization plays a vital role for determining the locations of sensor nodes. Although numerous localization algorithms have utilized various principles to reduce the localization error, but the energy-conservation at MAC layer is not much addressed by the researchers. A range-free Power Efficient Cooperative-MAC (PECo-MAC) localization algorithm is proposed by considering the concept of cooperative communication among beacon nodes as discussed in Chapter 5. In the proposed algorithm, a novel concept of cooperative communication in localization is introduced to diminish the overall energy consumption instead of traditional direct communication. An energy factor is also introduced which helps to reduce the energy consumption of beacon nodes. The location information of beacon nodes is broadcasted through cooperative communication to Base Station (BS) to maximize the residual energy of nodes. The selection of cooperative beacon nodes is accomplished on the basis of least-energy consumption.

To evaluate the performance of the proposed algorithm, the simulations are conducted in MATLAB. The performance of the algorithms is compared with recent localization algorithms and found superior in terms of accuracy and energy efficiency. It is perceived from the simulated results that the proposed algorithm accomplishes about 65%, 62%, 51%, and 42% better accuracy as compared to IDV-HOP, NDV-Hop, Modified DV-Hop, and Improved DV-Hop respectively.

3. To address the security concerns in the localization algorithm under the presence of adversary nodes.

In WSNs, it is very challenging to discovers the locations of unknown nodes in the

presence of malicious nodes and harsh environments. Chapter 6 focuses on the trust-based range-free algorithm for secure localization in WSNs. In the proposed algorithm, firstly the trust values of beacon nodes are evaluated on the basis of various metrics such as reputation value, mobility, residual energy, and neighbor node list. After that, evaluated trust values of each beacon node are shared among all beacon nodes across the network to construct a blockchain and these values are stored in a particular block of blockchain. For adding blocks to the blockchain, the most trusty beacon node is elected as miner for mining of blocks. Further, the localization process is performed by most trusty nodes so that more precise location can be accomplished. The proposed algorithm ensures an updated blockchain with reliability and consistent trust values of all beacon nodes.

The effectiveness of the proposed algorithm is analyzed by performing various simulations and the simulated results are compared with recent secure existing algorithms. The efficacy and significance of the proposed algorithm are proved by simulated results. It discriminates malicious beacon nodes significantly and improves the performance in terms of localization accuracy with resist network topology variety and localization ratio. The salient features of the proposed algorithms addressing the existing problems is shown in Table 7.1.

TABLE 7.1: *Salient features of the proposed algorithms which address the existing problems*

Issue	**Existing Algorithms**	**Problems**	**Proposed Algorithm**	**Salient Features of the proposed algorithm**

Localization accuracy	Basic DV-Hop [76], Weighted DV-Hop [198], Enhanced DV-Hop [201] and Improved DV-Hop [97]	Poor localization accuracy and mobility of nodes is not considered	Advanced DV-hop algorithm	It provides more accuracy to localization with minimum energy consumption. The network scenario is considered as mobile.
Energy conservation	IDV-HOP [204], NDV-Hop [92], Modified DV-Hop [107] and Improved DV-Hop [123]	These algorithms provide poor location estimations and the concept of energy conservation at MAC is not considered.	Power Efficient Cooperative-MAC (PECo-MAC)	The concept of cooperative communication at MAC is incorporated with mobile network scenario. The proposed algorithm is energy-efficient.

Security	Reputation-based secure algorithm [243], collaborative secure localization algorithm [161], Secure localization [63] and Attack-resistant RSS-based Localization [178].	Validation for the overall mobile environment is not considered	Trust-based range-free algorithm	The decentralized blockchain technology is included for secure localization with mobile network scenario.

7.3 Future Scope

Due to the increasing advancement in technology, WSNs play a crucial role in various real-time applications. WSNs attract the attention of researchers and academia over the past few decades to resolve different problems using exciting actions and advance communication technology. By considering the importance of WSNs, the future direction of the present research is as follows:

- WSNs have limited resources to perform various tasks. Limited storage or memory is also a challenging issue of concern. Therefore, in the future, effective memory utilization can be considered with accuracy and energy-efficiency in localization. Also, the framework can be extended to three-dimensional networks instead of two-dimensional.

- Blockchain is an emerging technology which proves its effectiveness in various fields. But, incorporation of blockchain with resources constrained WSNs require large storage, more power for operation, and heavy bandwidth due to control overheads. Hence, the concept of memory and computation in WSNs with blockchain will be considered in future work. Further, the framework can be extended to handle all types of multimedia information securely in Multimedia Wireless Sensor Networks.

- In the current era, WSNs are one of the most popular, useful, and dominant technologies for communication and information processing in the Internet of Things (IOTs). Hence, the concept of cloud computing will be considered for data storage to handle the large amount of data in WSN enabled IoTs. In WSN enabled IoTs, it is also important to maintain trade-off in data transmission, data processing, and data storage. The future research scope of proposed research in this dissertation should be in that direction

BIBLIOGRAPHY

[1] M. M. Zanjireh, A. Shahrabi, and H. Larijani, "ANCH: A new clustering algorithm for wireless sensor networks," in *Proceedings - 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA* 2013, 2013, pp. 450-455.

[2] N. Herscovici and C. Christodoulou, "Wireless communications and networking: An overview," *IEEE Antennas and Propagation Magazine*, vol. 44, no. 1. pp. 185-193, 2002.

[3] M. M. Abdul, "Wireless sensor networks: Technology and protocols," *BoD-Books on Demand*, 2012.

[4] O. Yalgashev, M. Bakhouya, A. Nait-Sidi-Moh, and J. Gaber, "Wireless sensor networks: Basics and fundamentals," in *the book Cyber-Physical System Design with Sensor Networking Technologies*, pp. 1-20, 2016.

[5] M. A. Marsan, C. F. Chiasserini, and A. Nucci, "Forming optimal topologies for Bluetooth-based wireless personal area networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 4, pp. 763-772, 2006.

[6] F. Zhao and W. Hua, "Compact size microstrip-line-fed antenna for WLAN application," in *2012 IEEE International Workshop on Antenna Technology, iWAT 2012*, 2012, pp. 249-252.

[7] K. Sharma and N. Dhir, "A study of wireless networks: WLANs , WPANs , WMANs , and WWANs with Comparison," *International Journal of Computer Science & Information Technology*, vol. 5, no. 6, pp. 7810-7813, 2014.

[8] W. Baluja, T. O. Ledesma, and L. Coya, "New solution for the creation of MANETs based on personal devices," *IEEE Latin America Transactions*, vol. 14, no. 3, pp. 1480-1487, 2016.

[9] C. Prabha, D. S. Kumar, and D. R. Khanna, "Wireless Multi-hop Ad-hoc Networks: A Review," *IOSR Journal of Computer Engineering*, vol. 16, no. 2, pp. 54-62, 2014.

[10] S. V. Manisekaran and R. Venkatesan, "Cluster-based architecture for range-free localization in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[11] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *Journal of Supercomputing*, vol. 68, no. 1, pp. 1-48, 2014.

[12] N. Jiang, S. Jin, Y. Guo, and Y. He, "Localization of wireless sensor network based on genetic algorithm," *International Journal of Computers, Communications and Control*, vol. 8, no. 6, pp. 825-837, 2013.

[13] F. Erbas, "Wireless Ad Hoc Networking," in *Encyclopedia of Information Science and Technology, First Edition*, 2011, pp. 3090-3094.

[14] A. Shaikh and S. Pathan, "Research on Wireless Sensor Network Technology," *International Journal of Information and Education Technology*, pp. 476-479, 2013.

[15] E. Gurses and O. Akan, "Multimedia communication in wireless sensor networks," *Annales des telecommunications*, pp. 1-8, 2005.

[16] I. F. Akyildiz and E. P. Stuntebeck, Wireless underground sensor networks: Research challenges, *Ad Hoc Networks*, vol. 4, no. 6, pp. 669-686, 2006.

[17] U. I. Minhas, I. H. Naqvi, S. Qaisar, K. Ali, S. Shahid, and M. A. Aslam, "A WSN for Monitoring and Event Reporting in Underground Mine Environments," *IEEE Systems Journal*, vol. 12, no. 1, pp. 485-496, 2018.

[18] L. Ghelardoni, A. Ghio, and D. Anguita, "Smart underwater wireless sensor networks," in *2012 IEEE 27th Convention of Electrical and Electronics Engineers in Israel, IEEEI* 2012, 2012.

[19] C. Uribe and W. Grote, "Radio communication model for underwater WSN," in *3rd International Conference on New Technologies, Mobility and Security, NTMS* 2009, 2009.

[20] E. P. Stuntebeck, D. Pompili, and T. Melodia, "Wireless underground sensor networks using commodity terrestrial motes," in 2006 *2nd IEEE Workshop on Wireless Mesh Networks, WiMESH 2006*, 2007, pp. 112-114.

[21] S. A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, and J. Ma, "Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing," in *Proceedings - 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW'07*, 2007, vol. 1, pp. 113-120.

[22] R. Berger, "Introduction to Wireless Sensor Networks," *INI Technical Symposiom*, 2009.

[23] U. Pesovic, J. Mohorko, K. Benkic, and Z. Cucej, "Single-hop vs. Multi-hop - Energy efficiency analysis in wireless sensor networks," in *Telekomunikacioni forum TELFOR 2010* , 2010.

[24] M. H. Anisi, A. H. Abdullah, and S. A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks," *Wireless Sensor Network*, vol. 3, no. 10, pp. 329-333, 2011.

[25] T. Bala, V. Bhatia, S. Kumawat, and V. Jaglan, "A survey: issues and challenges in wireless sensor network," *International Journal of Engineering & Technology*, vol. 7, no. 2-4, p. 53, 2018.

[26] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in *Proceedings - 2013 International Conference on Machine Intelligence Research and Advancement, ICMIRA 2013*, 2014, pp. 58-62.

[27] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware trojan design and implementation," in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2009*, 2009, pp. 50-57.

[28] M. Winkler, K. Tuchs, K. Hughes, and G. Barclay, "Theoretical and practical aspects of military wireless sensor networks," *Journal of Telecommunications and Information Technology (JTIT)*, pp. 37-45, 2008.

[29] F. Khakestani and S. Balochian, "A Survey of Military Application of Wireless Sensor Networks For Soldiers," *International Journal Of Engineering And Computer Science*, vol. 4, no. 4, pp. 13205-13210, 2015.

[30] I. Ahmad, K. Shah, and S. Ullah, "Military Applications using Wireless Sensor Networks: A survey," *International Journal of Engineering Science and Computing*, vol. 6, no. 6, pp. 7039-7043, 2016.

[31] M. P. Durisic, Z. Tafa, G. Dimic, and V. Milutinovic, "A survey of military applications of wireless sensor networks," *Mediterranean Conference on Embedded Computing (MECO)*, pp. 196-199, 2012.

[32] X. Shen, Z. Wang, and Y. Sun, "Wireless sensor networks for industrial applications," in *Proceedings of the World Congress on Intelligent Control and Automation (WCICA)*, 2004, vol. 4, pp. 3636-3640.

[33] F. A. Silva, "Industrial Wireless Sensor Networks: Applications, Protocols, and Standards [Book News]," *IEEE Industrial Electronics Magazine*, vol. 8, no. 4, pp. 67-68, 2014.

[34] L. Zheng, "Industrial wireless sensor networks and standardizations: The trend of wireless sensor networks for process autometion," in *Proceedings of the SICE Annual Conference*, 2010, pp. 1187-1190.

[35] M. Antoniou, M. C. Boon, P. N. Green, P. Green, and T. A. York, "Wireless sensor networks for industrial processes," in *SAS 2009 - IEEE Sensors Applications Symposium Proceedings*, 2009, pp. 13-18.

[36] A. A. Kumar S., K. Ovsthus, and L. M. Kristensen., "An industrial perspective on wireless sensor networks-a survey of requirements, protocols, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1391-1412, 2014.

[37] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, "Environmental wireless sensor networks," in *Proceedings of the IEEE*, 2010, vol. 98, no. 11, pp. 1903-1917.

[38] L. M. L. Oliveira and J. J. P. C. Rodrigues, "Wireless sensor networks: A survey on environmental monitoring," *Journal of Communications*, vol. 6, no. 2. pp. 143-151, 2011.

[39] B. S. Sathish, P. Ganesan, L. Bharathi, V. Suryanarayana, and A. Ranganayakulu, "Advanced Design of Wireless Communication Network for Building Monitoring," in *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 2019, pp. 194-197.

[40] V. Tsetsos, O. Sekkas, and E. Zervas, "A Forest Fire Detection System," in *Crisis Management*, 2013, pp. 1088-1098.

[41] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292-2330, 2008.

[42] A. Knaian, "A wireless sensor network for smart roadbeds and intelligent transportation systems," *Electrical Science and Engineering, Massachusets Institute of Technology*, no. 1999, 2000.

[43] A. Chehri, P. Fortier, and P. M. Tardif, "UWB-based sensor networks for localization in mining environments," *Ad Hoc Networks*, vol. 7, no. 5, pp. 987-1000, 2009.

[44] M. Li and Y. Liu, "Underground coal mine monitoring with wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 5, no. 2, pp. 1-29, 2009.

[45] G. Werner-Allen et al., "Deploying a wireless sensor network on an active volcano," *IEEE Internet Computing*, vol. 10, no. 2, pp. 18-25, 2006.

[46] P. Kulkarni and Y. ztrk, "Requirements and design spaces of mobile medical care," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 3, pp. 12-30, 2007.

[47] M. Morris, "Technologies for Heart and Mind: New Directions in Embedded Assessment," *Intel Technology Journal*, vol. 11, no. 1, 2007.

[48] I. Stoianov, L. Nachman, S. Madden, and T. Tokmouline, "PIPENETa wireless sensor network for pipeline monitoring," in *Proceedings of the 6th international conference on Information processing in sensor networks-IPSN 07*, 2007, p. 264.

[49] N. Mohamed, I. Jawhar, J. Al-Jaroodi, and L. Zhang, "Sensor network architectures for monitoring underwater pipelines," *Sensors*, vol. 11, no. 11, pp. 10738-10764, 2011.

[50] I. A. Essa, "Ubiquitous sensing for smart and aware environments," *IEEE Personal Communications*, vol. 7, no. 5, pp. 47-49, 2000.

[51] Y. Cho, J. Choi, and J. Choi, "A context-aware workflow system for a smart home," in *2007 International Conference on Convergence Information Technology, ICCIT 2007*, 2007, pp. 95-100.

[52] G. Kumar, M. K. Rai, R. Saha, and H. J. Kim, "An improved DV-Hop localization with minimum connected dominating set for mobile nodes in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 1, 2018.

[53] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-105, 2002.

[54] J. J. Lotf, S. H. H. Nazhad, and R. M. Alguliev, A survey of wireless sensor networks, in *2011 5th International Conference on Application of Information and Communication Technologies, AICT 2011*, 2011.

[55] A. Dana, A. K. Zadeh, and B. Hekmat, "Localization in Ad-Hoc networks," in *Proceeding - 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, ICT-MICC 2007*, 2007, pp. 313-317.

[56] X. Ji and H. Zha, "Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling," in *Proceedings - IEEE INFOCOM*, 2004, vol. 4, pp. 2652-2661.

[57] J. N. Ash, S. Kyperountas, A. O. H. Iii, R. L. Moses, and N. S. Correal, "Locating the Nodes," *IEEE Signal Processing Magazine*, vol. 22, no. July, pp. 54-69, 2005.

[58] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 54-69, 2005.

[59] S. Das, I. Banerjee, and T. Samanta, "Sensor localization and obstacle boundary detection algorithm in WSN," in *Proceedings - 2013 3rd International Conference on Advances in Computing and Communications, ICACC 2013*, 2013, pp. 412-415.

[60] R. Divya and R. Gunasundari, "Node Localization in Wireless Sensor Network Under Non-Line-Of-Sight Scenario," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy*, vol. 3297, no. 3, p. 309-312, 2007.

[61] M. Nicoli, S. Gezici, Z. Sahinoglu, and H. Wymeersch, "Localization in mobile wireless and sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, 2011.

[62] K. . Lu, J. . Zhang, G. . Wang, and L. . Ma, "Localization for mobile node based on sequential Monte Carlo," *Beijing Hangkong Hangtian Daxue Xuebao/Journal of Beijing University of Aeronautics and Astronautics*, vol. 33, no. 8, pp. 886-889, 2007.

[63] W. Shi, M. Barbeau, J. P. Corriveau, J. Garcia-Alfaro, and M. Yao, "Secure localization in the presence of colluders in WSNs," *Sensors (Switzerland)*, vol. 17, no. 8, 2017.

[64] S. M. Mazinani and M. Safari, "Secure Localization Approach in Wireless Sensor Network," *International Journal of Machine Learning and Computing*, vol. 5, no. 6, pp. 458-461, 2016.

[65] Y. Zhang, W. Liu, and Y. Fang, "Secure localization in wireless sensor networks," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2005, vol. 2005.

[66] W. Huang, H. Fang, Y. Chen, B. Yuan, and X. Zhou, "GPS-based positioning for autonomous underwater vehicle," in *International Conference on Space Information Technology*, 2005, vol. 5985, p. 598-556.

[67] N. M. Drawil, H. M. Amar, and O. A. Basir, "GPS localization accuracy classification: A context-based approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 262-273, 2013.

[68] S. Hwang and D. Yu, "GPS localization improvement of smartphones using built-in sensors," *International Journal of Smart Home*, vol. 6, no. 3, pp. 1-8, 2012.

[69] X. Q. Li and G. R. Chen, "A Sensor Node Localization Algorithm Based on Fuzzy RSSI Distance," *Applied Mechanics and Materials*, vol. 543-547, pp. 989-992, 2014.

[70] H. Wang, J. Wan, and R. Liu, "A novel ranging method based on RSSI," in *Energy Procedia*, 2011, vol. 12, pp. 230-235.

[71] A. Mesmoudi, M. Feham, and N. Labraoui, "Wireless Sensor Networks Localization Algorithms: A Comprehensive Survey," *International journal of Computer Networks & Communications*, vol. 5, no. 6, pp. 45-64, 2013.

[72] S. M. A. Bettencourt, "A Taxonomy of Localization Schemes for Wireless Sensor Networks," in *ICWN*, vol. 9, no. 8, 2007, pp. 1754-1757.

[73] X. Zhang et al., "Performance comparison of localization techniques for sequential WSN discovery," in *IET Seminar Digest*, 2012, vol. 2012, no. 3.

[74] S. Ravindra and S. N. , Jagadeesha, "Time of Arrival Based Localization in Wireless Sensor Networks: A Linear Approach," *Signal & Image Processing: An International Journal*, vol. 4, no. 4, pp. 13-30, 2013.

[75] J. Songbo, "A time difference of arrival-based localization algorithm for wireless sensor networks," *International Journal of Online Engineering*, vol. 12, no. 11, pp. 80-83, 2016.

[76] D. Niculescu and B. Nath, "DV Based Positioning in Ad Hoc Networks," *Telecommunication Systems*, vol. 22, no. 1-4, pp. 267-280, 2003.

[77] R. Nagpal, H. Shrobe, and J. Bachrach, "Organizing a global coordinate system from local information on an ad hoc sensor network," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2634, pp. 333-348, 2003.

[78] L. Kleinrock and J. Silvester, "Optimum transmission radii for packet radio networks or why six is a magic number," *Proceedings of National Telecommunications Conference (NTC 78)*, vol. 1, p. 431-435, 1978.

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

[80] R. V Kulkarni, S. Member, A. Frster, and G. K. Venayagamoorthy, "Computational Intelligence in Wireless Sensor Networks: A Survey," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 1, pp. 68-96, 2011.

[81] T. Adnan, S. Datta, and S. MacLean, "Efficient and accurate sensor network localization," *Personal and Ubiquitous Computing*, vol. 18, no. 4, pp. 821-833, 2014.

[82] O. Yalgashev, M. Bakhouya, A. Nait-Sidi-Moh, and J. Gaber, "Wireless sensor networks: Basics and fundamentals," in *Cyber-Physical System Design with Sensor Networking Technologies*, 2016, pp. 1-20.

[83] N. A. Alrajeh, M. Bashir, and B. Shams, "Localization techniques in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[84] Y. Hu and X. Li, "An improvement of DV-Hop localization algorithm for wireless sensor networks," *Telecommunication Systems*, vol. 53, no. 1, pp. 13-18, 2013.

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

[86] D. Ma, M. Joo, E. Bang, and W. Hock, "Range-free wireless sensor networks localization based on hop-count quantization," pp. 199-213, 2012.

[87] S. Tomic and I. Mezei, "Improvements of DV-Hop localization algorithm for wireless sensor networks," 2015.

[88] X. Chen and B. Zhang, "Improved DV-hop node localization algorithm in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, 2012.

[89] S. Lee, C. Park, M. J. Lee, and S. Kim, "Multihop range-free localization with approximate shortest path in anisotropic wireless sensor networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2014, 2014.

[90] S. Kumar and D. K. Lobiyal, "An advanced DV-Hop localization algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 71, no. 2, pp. 1365-1385, 2013.

[91] Y. Chen, X. Li, Y. Ding, J. Xu, and Z. Liu, "An improved DV-hop localization algorithm for wireless sensor networks," *Proceedings of the 13th IEEE Conference on Industrial Electronics and Applications, ICIEA 2018*, vol. 64, no. 3, pp. 1831-1836, 2018.

[92] T. Li, F. Liu, X. Li, and J. Wang, "A novel DV-Hop localization based on improved ABC algorithm," *Journal of Computational Information Systems*, vol. 10, no. 14, 2014.

[93] Y. Liu, J. Chen, and Z. Xu, "Improved DV-hop localization algorithm based on bat algorithm in wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 1, pp. 215-236, 2017.

[94] X.Wu, F. Zhang, and F.Sheng, "A Range-free Localization Algorithm for WSN based on Error Correction and Multi-Hop," *International Journal of Computer Applications*, vol. 151, no. 3, pp. 27-31, 2016.

[95] M. Peyvandi and A. A. Pouyan, "An Improved DV-Hop Localization Algorithm in Wireless Sensor Networks," pp. 16-17, 2015.

[96] A. Kaur, P. Kumar, and G. P. Gupta, "A weighted centroid localization algorithm for randomly deployed wireless sensor networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 1, pp. 82-91, 2019.

[97] G. Sharma and A. Kumar, "Improved DV-Hop localization algorithm using teaching learning based optimization for wireless sensor networks," *Telecommunication Systems*, vol. 67, no. 2, pp. 163-178, 2018.

[98] W. Kun, T. Yuzhen, Z. Zhen, and S. Yinhua, "An Improved DV-Hop Distributed Active Multihop Localization Algorithm," in *Proceedings - 2016 International Computer Symposium, ICS 2016*, 2017, pp. 221-226.

[99] G. Li, S. Zhao, J. Wu, C. Li, and Y. Liu, "DV-Hop Localization Algorithm Based on Minimum Mean Square Error in Internet of Things," *Procedia Computer Science*, vol. 147, pp. 458-462, 2019.

[100] P. Wang, F. Xue, H. Li, Z. Cui, and J. Chen, "A Multi-Objective DV-Hop Localization Algorithm Based on NSGA-II in Internet of Things," *Mathematics*, vol. 7, no. 2, p. 184, 2019.

[101] G. A. L. Zodi, G. P. Hancke, and A. B. Bagula, "Enhanced centroid localization of wireless sensor nodes using linear and neighbor weighting mechanisms," in *ACM IMCOM 2015 - Proceedings*, 2015, pp. 1-8.

[102] S. Liu, C. Liu, W. Zhang, and D. Zhao, "Hybrid localization algorithm based on APIT and DV-HOP in Wireless Sensor Networks," in *2015 IEEE/CIC International Conference on Communications in China-Workshops, CIC/ICCC 2015*, 2017, pp. 164-168.

[103] D. Zhang, Z. Fang, H. Sun, and J. Cao, "HTCRL: A range-free location algorithm based on homothetic triangle cyclic refinement in wireless sensor networks," *Information (Switzerland)*, vol. 8, no. 2, 2017.

[104] D. Qiao and G. K. H. Pang, "Localization in wireless sensor networks with gradient descent," in *IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing - Proceedings*, 2011, pp. 91-96.

[105] W. Zhang, Q. Yin, H. Chen, F. Gao, and N. Ansari, "Distributed angle estimation for localization in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 527-537, 2013.

[106] S. Tomic, M. Beko, and R. Dinis, "Distributed RSS-AoA Based Localization with Unknown Transmit Powers," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 392-395, 2016.

[107] G. Sharma and A. Kumar, "Modified Energy-Efficient Range-Free Localization Using Teaching-Learning-Based Optimization for Wireless Sensor Networks," *IETE Journal of Research*, vol. 64, no. 1, pp. 124-138, 2018.

[108] F. Shahzad, T. R. Sheltami, and E. M. Shakshuki, "DV-maxHop: A Fast and Accurate Range-Free Localization Algorit*hm for Anisotropic Wireless Networks," IEEE Transactions on Mobile Computing*, vol. 16, no. 9, pp. 2494-2505, 2017.

[109] S. Zhang, J. Li, B. He, and J. Chen, "LSDV-Hop: Least squares based DV-Hop localization algorithm for wireless sensor networks," *Journal of Communications*, vol. 11, no. 3, pp. 243-248, 2016.

[110] C. Li, P. Zhao, and Y. Zeng, "Improved DV-Hop localization algorithm for wireless nodes in the smart grid," in *26th Chinese Control and Decision Conference, CCDC 2014*, 2014, pp. 4535-4540.

[111] S. Dong and Y. Qi, "MPDV-HOP: An improved localization algorithm for wireless sensor networks," *WSEAS TRANSACTIONS on COMMUNICATIONS*, vol. 14,pp.390-398, 2015.

[112] J. Mass-Sanchez, E. Ruiz-Ibarra, J. Cortez-Gonzlez, A. Espinoza-Ruiz, and L. A. Castro, "Weighted Hyperbolic DV-Hop Positioning Node Localization Algorithm in WSNs," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5011-5033, 2017.

[113] G. Sharma and A. Kumar, "Improved range-free localization for three-dimensional wireless sensor networks using genetic algorithm," *Computers and Electrical Engineering*, vol. 72, pp. 808-827, 2018.

[114] S. Phoemphon, C. So-In, and N. Leelathakul, "Fuzzy Weighted Centroid Localization with Virtual Node Approximation in Wireless Sensor Networks," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4728-4752, 2018.

[115] F. Darakeh, G. R. Mohammad-Khani, and P. Azmi, "DCRL-WSN: A distributed cooperative and range-free localization algorithm for WSNs," *AEU - International Journal of Electronics and Communications*, vol. 93, pp. 289-295, 2018.

[116] L. Cui, C. Xu, G. Li, Z. Ming, Y. Feng, and N. Lu, "A high accurate localization algorithm with DV-Hop and differential evolution for wireless sensor network," *Applied Soft Computing Journal*, vol. 68, pp. 39-52, 2018.

[117] Y. Sun, S. Yin, and J. Liu, "Novel DV-hop Method Based on Krill Swarm Algorithm Used for Wireless Sensor Network Localization," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 14, no. 4, p. 1438-1445, 2016.

[118] S. K. Gharghan, R. Nordin, M. Ismail, and J. A. Ali, "Accurate Wireless Sensor Localization Technique Based on Hybrid PSO-ANN Algorithm for Indoor and Outdoor Track Cycling," *IEEE Sensors Journal*, vol. 16, no. 2, pp. 529-541, 2016.

[119] C. Tao and L. Min, "Sensor node localization based on improved genetic algorithm," *International Journal of Smart Home*, vol. 9, no. 7, pp. 251-258, 2015.

[120] Z. Sun, X. Wang, L. Tao, and Z. Zhou, "Localization algorithm in wireless sensor networks based on multi-objective particle swarm optimization," in *Communications in Computer and Information Science*, 2015, vol. 501, pp. 223-232.

[121] R. Rajakumar, J. Amudhavel, P. Dhavachelvan, and T. Vengattaraman, "GWO-LPWSN: Grey Wolf Optimization Algorithm for Node Localization Problem in Wireless Sensor Networks," *Journal of Computer Networks and Communications*, vol. 2017, p. 10, 2017.

[122] Z. Cui, B. Sun, G. Wang, Y. Xue, and J. Chen, "A novel oriented cuckoo search algorithm to improve DV-Hop performance for cyber-physical systems," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 42-52, 2017.

[123] M. Mehrabi, H. Taheri, and P. Taghdiri, "An improved DV-Hop localization algorithm based on evolutionary algorithms," *Telecommunication Systems*, 2016.

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

[125] C. Vimalarani, R. Subramanian, and S. N. Sivanandam, "An Enhanced PSO-Based Clustering Energy Optimization Algorithm for Wireless Sensor Network," *Scientific World Journal*, vol. 2016, 2016.

[126] X. Luo, X. Chang, and H. Liu, "A Taylor based localization algorithm for wireless sensor network using extreme learning machine," *IEICE Transactions on Information and Systems*, vol. E97D, no. 10, pp. 2652-2659, 2014.

[127] S. Phoemphon, C. So-In, and D. (Tao) Niyato, "A hybrid model using fuzzy logic and an extreme learning machine with vector particle swarm optimization for wireless sensor network localization," *Applied Soft Computing Journal*, vol. 65, pp. 101-120, 2018.

[128] J. Zheng and A. Dehghani, "Range-Free Localization in Wireless Sensor Networks with Neural Network Ensembles," *Journal of Sensor and Actuator Networks*, vol. 1, no. 3, pp. 254-271, 2012.

[129] Y. Xu, X. Luo, W. Wang, and W. Zhao, "Efficient DV-HOP localization for-wireless cyber-physical social sensing system: A correntropy-based neural network learning scheme," *Sensors (Switzerland)*, vol. 17, no. 1, 2017.

[130] S. Sivakumar and V. Venkatesan, "Error Minimization in Localization of Wireless Sensor Networks using Fish Swarm Optimization Algorithm," *International Journal of Computer Applications*, vol. 159, no. 7, pp. 39-45, 2017.

[131] V. Gupta and B. Singh, "Study of range free centroid based localization algorithm and its improvement using particle swarm optimization for wireless sensor networks under log normal shadowing," *International Journal of Information Technology*, 2018.

[132] L. Jian Yin and M. Elhoseny, "A New Distance Vector-Hop Localization Algorithm Based on Half-Measure Weighted Centroid," *Mobile Information Systems*, vol. 2019, 2019.

[133] S. Amri, F. Khelifi, A. Bradai, A. Rachedi, M. L. Kaddachi, and M. Atri, "A new fuzzy logic based node localization mechanism for Wireless Sensor Networks," *Future Generation Computer Systems*, vol. 93, pp. 799-813, 2019.

[134] H. M. Kanoosh, E. H. Houssein, and M. M. Selim, "Salp Swarm Algorithm for Node Localization in Wireless Sensor Networks," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1-12, 2019.

[135] G. Kumar et al., "Improved location estimation in wireless sensor networks using a vector-based swarm optimized connected dominating set," *Sensors (Switzerland)*, vol. 19, no. 2, 2019.

[136] N. Al-Nabhan, B. Zhang, M. Al-Rodhaan, and A. Al-Dhelaan, "Two connected dominating set algorithms for wireless sensor networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, vol. 7405 LNCS, pp. 705-713.

[137] T. Shi, S. Cheng, Z. Cai, and J. Li, "Adaptive connected dominating set discovering algorithm in energy-harvest sensor networks," in *Proceedings - IEEE INFOCOM*, 2016, vol. 2016-July.

[138] T. Pino, S. Choudhury, and F. Al-Turjman, "Dominating Set Algorithms for Wireless Sensor Networks Survivability," *IEEE Access*, vol. 6, pp. 17527-17532, 2018.

[139] C. W. Chou, C. H. Yang, J. H. Lin, H. L. Tsai, and Y. H. Ou, "Algorithms for Constructing Strongly Connected Dominating Set in Heterogeneous Wireless Sensor Networks," *Applied Mechanics and Materials*, vol. 311, pp. 87-92, 2013.

[140] J. P. Mohanty, C. Mandal, C. Reade, and A. Das, "Construction of minimum connected dominating set in wireless sensor networks using pseudo dominating set," *Ad Hoc Networks*, vol. 42, pp. 61-73, 2016.

[141] C. Luo, J. Yu, D. Li, H. Chen, Y. Hong, and L. Ni, "A Novel Distributed algorithm for constructing virtual backbones in wireless sensor networks," *Computer Networks*, vol. 146, pp. 104-114, 2018.

[142] Y. Wu, F. Wang, M. T. Thai, and Y. Li, "Constructing k-connected M-dominating sets in wireless sensor networks," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2007.

[143] H. Faheem, N. Ilyas, S. ul, and S. Tanvir, "Connected Dominating Set based Optimized Routing Protocol for Wireless Sensor Networks," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 11, 2016.

[144] N. Al-Nabhan, B. Zhang, X. Cheng, M. Al-Rodhaan, and A. Al-Dhelaan, "Three Connected Dominating Set Algorithms for Wireless Sensor Networks," *International Journal of Sensor Network*, vol. 21, no. 1, pp. 53-66, 2016.

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

[146] L. Cheklat, M. Amad, and A. Boukerram, "A Limited Energy Consumption Model for P2P Wireless Sensor Networks," *Wireless Personal Communications*, vol. 96, no. 4, pp. 6299-6324, 2017.

[147] A. Ali, M. Abo-Zahhad, and M. Farrag, "Modeling of Wireless Sensor Networks with Minimum Energy Consumption," *Arabian Journal for Science and Engineering*, vol. 42, no. 7, pp. 2631-2639, 2017.

[148] P. Nayak and B. Vathasavai, "Energy Efficient Clustering Algorithm for Multi-Hop Wireless Sensor Network Using Type-2 Fuzzy Logic," *IEEE Sensors Journal*, vol. 17, no. 14, pp. 4492-4499, 2017.

[149] M. Abo-Zahhad, M. Farrag, A. Ali, and O. Amin, "An energy consumption model for wireless sensor networks," in *5th International Conference on Energy Aware Computing Systems and Applications, ICEAC 2015*, 2015.

[150] D. Apiletti, E. Baralis, and T. Cerquitelli, "Energy-saving models for wireless sensor networks," *Knowledge and Information Systems*, vol. 28, no. 3, pp. 615-644, 2011.

[151] Z. Zhu, S. O. Oyadiji, and H. He, "Energy awareness workflow model for wireless sensor nodes," *Wireless Communications and Mobile Computing*, vol. 14, no. 17, pp. 1583-1600, 2014.

[152] A. Damaso, D. Freitas, N. Rosa, B. Silva, and P. Maciel, "Evaluating the power consumption of Wireless Sensor Network applications using models," *Sensors (Switzerland)*, vol. 13, no. 3, pp. 3473-3500, 2013.

[153] H. W. Kim, T. H. Im, and H. S. Cho, "UCMAC: A cooperative MAC protocol for underwater wireless sensor networks," *Sensors (Switzerland)*, vol. 18, no. 6, 2018.

[154] H. R. Shamna and J. Lillykutty, "An energy and throughput efficient distributed cooperative MAC protocol for multihop wireless networks," *Computer Networks*, vol. 126, pp. 15-30, 2017.

[155] Y. I. Joo and K. Hur, "Cooperative Distributed MAC design for cross-layer link adaptation of UWB WPAN devices," *Wireless Personal Communications*, vol. 71, no. 1, pp. 137-150, 2013.

[156] H. Shan, W. Zhuang, and Z. Wang, "Distributed cooperative MAC for multihop wireless networks," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 126-133, 2009.

[157] K. Liu, S. Wu, B. Huang, F. Liu, and Z. Xu, "A power-optimized cooperative MAC protocol for lifetime extension in wireless sensor networks," *Sensors (Switzerland)*, vol. 16, no. 10, 2016.

[158] J. Lin and M. A. Weitnauer, "Range extension cooperative MAC to attack energy hole in duty-cycled multi-hop WSNs," *Wireless Networks*, vol. 24, no. 5, pp. 1419-1437, 2018.

[159] M. Sami, N. K. Noordin, F. Hashim, S. Subramaniam, and A. Akbari-Moghanjoughi, "An Energy-Aware Cross-Layer Cooperative MAC Protocol for Wireless Ad Hoc Networks," *Journal of Network and Computer Applications*, vol. 58, pp. 227-240, 2015.

[160] X. Wang and J. Li, "Improving the network lifetime of MANETs through cooperative MAC protocol design," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1010-1020, 2015.

[161] G. Han, L. Liu, J. Jiang, L. Shu, and J. J. P. C. Rodrigues, "A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks," *Sensors (Switzerland)*, vol. 16, no. 2, 2016.

[162] R. Garg, A. L. Varna, and M. Wu, "An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks," in *IEEE Transactions on Information Forensics and Security*, 2012, vol. 7, no. 2, pp. 717-730.

[163] N. Yu, L. Zhang, and Y. Ren, "BRS-based robust secure localization algorithm for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[164] T. Bao, J. Wan, K. Yi, and Q. Zhang, "A game-based secure localization algorithm for mobile wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, 2015.

[165] G. Kumar, M. K. Rai, H. Kim, and R. Saha, "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks," *Mobile Information Systems*, vol. 2017, pp. 1-12, 2017.

[166] R. Garg, A. L. Varna, and M. Wu, "A gradient descent based approach to secure localization in mobile sensor networks," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2012, pp. 1869-1872.

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

[168] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xi, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, no. PA, pp. 22-35, 2015.

[169] X. Liu, R. Yang, and Q. Cui, "An efficient secure DV-Hop localization for wireless sensor network," *International Journal of Security and its Applications*, vol. 9, no. 7, pp. 275-284, 2015.

[170] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, "Wormhole Detection Based on Ordinal MDS Using RTT in Wireless Sensor Network," *Journal of Computer Networks and Communications*, vol. 2016, pp. 1-15, 2016.

[171] C.C. Chang, W.Y. Hsueh, and T.F. Cheng, "A Dynamic User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks," *Wireless Personel Communication*, vol. 89, no. 2, pp. 447-465, 2016.

[172] T. Shu, Y. Chen, and J. Yang, "Protecting multi-lateral localization privacy in pervasive environments," *IEEE/ACM Transactions on Networking*, vol. 23, no. 5, pp. 1688-1701, 2015.

[173] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 5, pp. 938-950, 2013.

[174] P. Bao and M. Liang, "A security localization method based on threshold and vote for wireless sensor networks," in *Procedia Engineering*, 2011, vol. 15, pp. 2783-2787.

[175] Y. Choi, "Weaknesses of temporal credential-based mutual authentication with a multiple-password scheme for wireless sensor networks," *International Journal of Applied Engineering Research*, vol. 12, no. 17, pp. 6962-6969, 2017.

[176] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp. 263-277, 2015.

[177] O. AlFarraj, A. AlZubi, and A. Tolba, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-11, 2018.

[178] D. Chen, Q. Zhang, N. Wang, and J. Wan, "An Attack-resistant RSS-based Localization Algorithm with L1 Regularization for Wireless Sensor Networks," in *Proceedings of 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2018*, 2018, pp. 1048-1051.

[179] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655-45664, 2018.

[180] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things Journal*, 2018.

[181] S. Kushch and F. Prieto-Castrillo, "Blockchain for dynamic nodes in a smart city," in *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings*, 2019, pp. 29-34.

[182] R. J. ul Hussen Khan, Z. Noshad, A. Javaid, M. Zahid, I. Ali, and N. Javaid, "Node Recovery in Wireless Sensor Networks via Blockchain," *in Lecture Notes in Networks and Systems*, vol. 96, 2020, pp. 94105.

[183] S. Ali, N. Javaid, D. Javeed, I. Ahmad, A. Ali, and U. M. Badamasi, "A Blockchain-Based Secure Data Storage and Trading Model for Wireless Sensor Networks," *in Advances in Intelligent Systems and Computing*, 2020, vol. 1151 AISC, pp. 499511.

[184] T.H. Kim, R. Goyat, M.K. Rai, G. Kumar, W.J. Buchanan, R. Saha, and R. Thomas, "A Novel Trust Evaluation Process for Secure Localization Using a

Decentralized Blockchain in Wireless Sensor Networks," *IEEE Access*, vol. 7, pp. 184133184144, 2019.

[185] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6. pp. 32979-33001, 2018.

[186] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Security and Communication Networks*, vol. 2018, pp. 1-27, 2018.

[187] Y.P. Lin et al., "Blockchain: The Evolutionary Next Step for ICT E-Agriculture," *Environments*, vol. 4, no. 3, p. 50, 2017.

[188] S. Goka and H. Shigeno, "Distributed management system for trust and reward in mobile ad hoc networks," in *CCNC 2018 - 2018 15th IEEE Annual Consumer Communications and Networking Conference*, 2018, vol. 2018-Janua, pp. 1-6.

[189] A. Reyna, C. Martn, J. Chen, E. Soler, and M. Daz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173-190, 2018.

[190] A. Lei et al., "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Generation Computer Systems*, 2019.

[191] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Generation Computer Systems*, vol. 92, pp. 357-373, 2019.

[192] O. Kanoun and H. R. Trankler, "Sensor technology advances and future trends," *IEEE Transactions on Instrumentation and Measurement*, vol. 53, no. 6, pp. 1497-1501, 2004.

[193] X. Li, A. Nayak, D. Simplot-Ryl, and I. Stojmenovic, "Sensor Placement in Sensor and Actuator Networks," in *Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication*, 2010, pp. 263-294.

[194] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," *IEEE Personal Communications*, vol. 7, no. 5, pp. 28-34, 2000.

[195] J. Wang, R. K. Ghosh, and S. K. Das, "A survey on sensor localization," *Journal of Control Theory and Applications*, vol. 8, no. 1, pp. 2-11, 2010.

[196] P. Singh and S. Agrawal, "TDOA based node localization in WSN using Neural networks," in *Proceedings - 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013*, 2013, pp. 400-404.

[197] H. Chen, K. Sezaki, P. Deng, and H. C. So, "An improved DV-Hop localization algorithm with reduced node location error for wireless sensor networks," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 8, pp. 2232-2236, 2008.

[198] D. D. Liu, S. Peng, K. C. Lin, and J. Zhang, "A weight-based DV-HOP improved localization algorithm for wireless sensor networks," *International Journal of Online Engineering*, vol. 10, no. 4, pp. 22-27, 2014.

[199] C. L. Tseng, F. Y. Liu, C. H. Lin, and C. Y. Lee, "Boundary-improved distance vector-hop localization method with multipower correction for wireless sensor networks," *Sensors and Materials*, vol. 29, no. 6, pp. 675-687, 2017.

[200] L. Gui, T. Val, A. Wei, and R. Dalce, "Improvement of range-free localization technology by a novel DV-hop protocol in wireless sensor networks," *Ad Hoc Networks*, vol. 24, no. PB, pp. 55-73, 2015.

[201] W. Z. Ping and C. Xuan, "Node Localization of Wireless Sensor Networks Based on DV-hop and Steffensen Iterative Method," *International Journal of Future Generation Communication and Networking*, vol. 8, no. 2, pp. 1-8, 2015.

[202] J. Yu, Z. Kuang, B. Zhang, W. Zhang, D. Lin, and J. Fan, "Leveraging Content Sensitiveness and User Trustworthiness to Recommend Fine-Grained Privacy

Settings for Social Image Sharing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1317-1332, 2018.

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

[204] Y. Hu and X. Li, "An improvement of DV-Hop localization algorithm for wireless sensor networks," *Telecommunication Systems*, vol. 53, no. 1, pp. 13-18, 2013.

[205] C. Yu, L. Yu, J. Tan, R. Li, D. Xiao, and Q. He, "DV-Hop localization algorithm in WSN based on weighted of correction in hop distance," in *Applied Mechanics and Materials*, 2013, vol. 303-306, pp. 143-148.

[206] M. Mehrabi, H. Taheri, and P. Taghdiri, "An improved DV-Hop localization algorithm based on evolutionary algorithms," *Telecommunication Systems*, vol. 64, no. 4, pp. 639-647, 2017.

[207] S. P. Singh and S. C. Sharma, "Implementation of a PSO Based Improved Localization Algorithm for Wireless Sensor Networks," *IETE Journal of Research*, pp. 1-13, 2018.

[208] Z. Cui, B. Sun, G. Wang, Y. Xue, and J. Chen, "A novel oriented cuckoo search algorithm to improve DV-Hop performance for cyber-physical systems," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 42-52, 2017.

[209] O. Cheikhrouhou, G. M. Bhatti, and R. Alroobaea, "A hybrid DV-hop algorithm using RSSI for localization in large-scale wireless sensor networks," *Sensors (Switzerland)*, vol. 18, no. 5, 2018.

[210] R. Raj Priyadarshini and N. Sivakumar, "Cluster head selection based on Minimum Connected Dominating Set and Bi-Partite inspired methodology for energy conservation in WSNs," *Journal of King Saud University - Computer and Information Sciences*, 2018.

[211] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The anatomy of a context-aware application," *Wireless Networks*, vol. 8, no. 2-3, pp. 187-197, 2002.

[212] A. Kaur, P. Kumar, and G. P. Gupta, "Analysis on DV-hop algorithm and its variants by considering threshold," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 4, pp. 79-83, 2017.

[213] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325-349, 2005.

[214] O. K. Tonguz and G. Ferrari, "A communication-theoretic approach to ad hoc wireless networking," in *2006 3rd Annual IEEE Communications Society on Sensor and Adhoc Communications and Networks, Secon 2006*, 2006, vol. 2, pp. 715-722.

[215] K. Chen, M. Ma, E. Cheng, F. Yuan, and W. Su, "A survey on MAC protocols for underwater wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1433-1447, 2014.

[216] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "The evolution of MAC protocols in wireless sensor networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 101-120, 2013.

[217] R. A. M. Khan and H. Karl, "MAC protocols for cooperative diversity in wireless LANs and wireless sensor networks, *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 46-63, 2014.

[218] P. Ju, W. Song, and D. Zhou, "Survey on cooperative medium access control protocols," *IET Communications*, vol. 7, no. 9, pp. 893-902, 2013.

[219] H. Shan, H. T. Cheng, and W. Zhuang, "Cross-layer cooperative MAC protocol in distributed wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2603-2615, 2011.

[220] T. Aguilar, S. J. Syue, V. Gauthier, H. Afifi, and C. L. Wang, "CoopGeo: A beaconless geographic cross-layer protocol for cooperative wireless ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2554-2565, 2011.

[221] J. Seo, M. Kim, I. Hur, W. Choi, and H. Choo, "DRDT: Distributed and reliable data transmission with cooperative nodes for lossy wireless sensor networks," *Sensors*, vol. 10, no. 4, pp. 2793-2811, 2010.

[222] C. Y. Oh and T. J. Lee, "Cooperative MAC protocol using active relays for multi-rate WLANs," *Journal of Communications and Networks*, vol. 13, no. 5, pp. 463-471, 2011.

[223] S. Phoemphon, C. So-In, and N. Leelathakul, "Optimized Hop Angle Relativity for DV-Hop Localization in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 78149-78172, 2018.

[224] B. Chopard and M. Tomassini, "Particle swarm optimization," in *Natural Computing Series*, 2018, pp. 97-102.

[225] D. Ganesan, A. Cerpa, W. Ye, Y. Yu, J. Zhao, and D. Estrin, "Networking issues in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 64, no. 7, pp. 799-814, 2004.

[226] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *Journal of Network and Computer Applications*, vol. 60. pp. 192-219, 2016.

[227] D. Pescaru and D. I. Curiac, "Anchor node localization for wireless sensor networks using video and compass information fusion," *Sensors (Switzerland)*, vol. 14, no. 3, pp. 4211-4224, 2014.

[228] P. R. Vamsi and K. Kant, "Trust and Location-Aware Routing Protocol for Wireless Sensor Networks," *IETE Journal of Research*, vol. 62, no. 5, pp. 634-644, 2016.

[229] W. Liang, Z. Ruan, Y. Wang, and X. Chen, "RESH: A secure authentication algorithm based on regeneration encoding self-healing technology in WSN," Journal of Sensors, vol. 2016, 2016.

[230] W. W. Chang et al., "A smart medication system using wireless sensor network technologies," in *Sensors and Actuators, A: Physical*, 2011, vol. 172, no. 1, pp. 315-321.

[231] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, 2018.

[232] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors (Switzerland)*, vol. 19, no. 4, 2019.

[233] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511-521, 2019.

[234] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660-670, 2002.

[235] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Consulted*, pp. 1-9, 2008.

[236] V. K. M. Crosby, Nachiappan, P. Pattanayak, S. Verma, "Blockchain Technology Explained," *Blockchain Technologies*, pp. 1-27, 2015.

[237] O. Badreddin, A. G. Rivera, and A. Malik, "Blockchain Fundamentals and Development Platforms," *Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, pp. 377-379, 2018.

[238] M. P. Heinrich, M. No, J. Waldman, and E. Akpinar, "Blockchain - Blockchain Fundamentals," *MSDN Magazine Blog*, vol. U608438, no. 3, p. 218, 2018.

[239] M. Iansiti and K. R. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, vol. 95, no. January-February, pp. 118-127, 2017.

[240] T. Duong, A. Chepurnoy, L. Fan, and H. S. Zhou, "TwinsCoin: A cryptocurrency via proof-of-work and proof-of-stake," in *BCC 2018 - Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Co-located with ASIA CCS 2018*, 2018, pp. 1-13.

[241] M. Ye and Y. P. Wang, "A new malicious nodes attack-resistant security location method in wireless sensor network," *Jisuanji Xuebao/Chinese Journal of Computers*, vol. 36, no. 3, pp. 532-545, 2013.

[242] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Fingerprinting localization in wireless networks based on received-signal-strength measurements: A case study on wimax networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 283-294, 2010.

[243] J. He, J. Xu, X. Zhu, Y. Zhang, T. Zhang, and W. Fu, "Reputation-based secure sensor localization in wireless sensor networks," *Scientific World Journal*, vol. 2014, 2014.

PUBLICATIONS

[1] Rekha, Gulshan Kumar and Mritunjay Kumar Rai, "An Advanced DV-Hop Localization Algorithm for Random Mobile Nodes in Wireless Sensor Networks," *Arabian Journal for Science and Engineering*, vol. 44, no. 11, pp.1-17, 2019. DOI: https://doi.org/10.1007/s13369-019-04082-4 (SCI/SCIE Indexed with Impact Factor 1.518).

[2] Rekha Goyat, Gulshan Kumar, Mritunjay Kumar Rai, Rahul Saha and Tai-Hoon Kim, "Energy Efficient Range-Free Localization Algorithm for Wireless Sensor Networks," *Sensors*, vol. 19, no. 16:3603, 2019. DOI: https://doi.org/10.3390/s1916 3603 (SCI/SCIE Indexed with Impact Factor 3.031).

[3] Rekha Goyat, Gulshan Kumar, Mritunjay Kumar Rai, Rahul Saha, Reji Thomas and Tai Hoon Kim,"Blockchain Powered Secure Range-Free Localization in Wireless Sensor Networks, *Arabian Journal for Science and Engineering*, pp.1-17, 2020. DOI:https://doi.org/10.1007/s13369-020-04493-8 (SCI/SCIE Indexed with Impact Factor 1.518).

[4] Tai-Hoon Kim, Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar, William J. Buchanan, Rahul Saha, and Reji Thomas, "A Novel Localization Algorithm with Cooperative Communication for Wireless Sensor Networks", *IEEE Access*, vol. 7,

pp.184133-184144. DOI: 10.1109/ACCESS.2019.2960609 (SCI/SCIE Indexed with Impact Factor 4.098)

[5] Tai-Hoon Kim, Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar, William J. Buchanan, Rahul Saha, and Reji Thomas, "A Blockchain-based Scheme for Privacy Preserving Authentication with Fog Computing in Wireless Multimedia Sensor Networks", *IEEE Security & Privacy*, Accepted. (SCI/SCIE Indexed with Impact Factor 1.598)

[6] Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar and Hye jin Kim, "Improved DV-Hop Localization Scheme for Randomly Deployed WSNs," *International Journal of Sensors, Wireless Communications and Control*, 2019. DOI:10.2174/2210327909666190208161350 (Scopus Indexed with Impact Factor 0.36).

[7] Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar and Se-Jung Lim, "A structured review on security and energy efficient protocols for wireless sensor networks," *International Journal of Advanced Science and Technology*, vol. 122, no.2019, pp. 49-74, (2019). DOI: http://dx.doi.org/10.14257/ijast.2019.122.05 (Scopus Indexed with Impact Factor 0.42).

[8] Rekha Goyat, Mritunjay Kumar Rai and Gulshan Kumar, "Recent Advances in DV-hop localization algorithm for Wireless Sensor Networks, *Conference on Intelligent, Interactive Systems and Applications*, Accepted .

[9] Rekha Goyat, Mritunjay Kumar Rai and Gulshan Kumar, "Trust-based Secure Localization for Wireless Sensor Networks with Blockchain Technology, *ACM Transactions on Multimedia Computing Communications and Applications*, Communicated. (SCI/SCIE Indexed with Impact Factor 2.2518).

[10] Rekha Goyat, Mritunjay Kumar Rai and Gulshan Kumar, "A Range-free Power Efficient Cooperative MAC Localization Algorithm in mobile Heterogeneous WSNs", *ACM Transactions on Internet Technology*, Communicated. (SCI/SCIE Indexed with Impact Factor 1.498).

[11] Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar, Rahul Saha, and Reji Thomas, "Blockchain-based Data Storage for Privacy and Authentication in Internet-of-Things", *IEEE Internet of Things Journal*, DOI: 10.1109/JIOT.2020.3019074. (SCI/-SCIE Indexed with Impact Factor 9.515).