Addis Ababa University
Addis Ababa Institute of Technology
School of Graduate Studies
School of Electrical and Computer Engineering

Improving Energy Efficiency and Security of LEACH Routing Protocol against Black Hole Attack in Wireless Sensor Network

By

Zeru Kifle

Advisor

Yalemzewd Negash(PhD)

A Thesis Presented to School of Graduate Studies of Addis Ababa University in partial fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering

Addis Ababa, Ethiopia

December 29, 2021

Declaration

I, Zeru Kifle , hereby declare that all the information submitted by me in the report is correct ,true and valid. All sources of materials used for the thesis have been duly acknowledged. I further confirm that the thesis has not been submitted either in part or in full to any other higher learning institution for the purpose of earning any degree. I will present the supporting documents as and when required.

Zeru Kifle
(Roll No. GSE/1772/10)

December 29, 2021

Acceptance Certificate

School of Electrical and Computer Engineering

Addis Ababa institute of Technology
Addis Ababa University

The thesis report entitled **Improving Energy Efficiency and Security of LEACH Routing Protocol against Black Hole Attack in Wireless Sensor Network** Submitted by Mr. Zeru Kifle is carried under my supervision and guidance and fulfilling the nature and standard required for the partial fulfilment of requirements of masters of science degree in Computer Engineering. The work encapsulated in this thesis has not been submitted somewhere for degree.

Dr. Yalemzewd Negash
School of Electrical and Computer Engineering
Addis Ababa Institute of Technology
Addis Ababa University

Signature

December 29, 2021

Approval Sheet

School of Electrical and Computer Engineering

Addis Ababa Institute of Technology
Addis Ababa University

This MSc thesis entitled **"Improving Energy Efficiency and Security of LEACH Routing Protocol against Black Hole Attack in Wireless Sensor Network"** by **Zeru Kifle** is approved for the degree of Master of Science in Computer Engineering.

Name	**Signature**	**Date**
Yalemzewud Negash(PhD)		
(Advisor)		
Fitsum Assamnew (PhD)		
(Program Chairman)		
Sosina Mengistu(PhD)		
(Internal Examiner)		
(Bisrat Derebssa (PhD)		
(Dean, School of Electrical and Computer Engineering)		

December 29, 2021
Place : Addis Ababa Institute of Technology, Addis Ababa University
Addis Ababa, Ethiopia

Abstract

A Wireless sensor network (WSN) consists of masses of tiny sensor nodes working in a cooperative manner that sense the physical or environmental circumstances and send this information to the base station. WSN has different constraints due to limited sensor nodes resources, lack of central control, and unreliable communication of routing protocol used in WSN. Sensor nodes in WSN have limited resources such as memory capacity, storage space, and energy. These resource constraints in WSN lead to the limitations to implement the most commonly used cryptography algorithm to secure WSNs. Nowadays, secured data transferring and reducing energy dissipation of sensor nodes is the main challenge in WSNs. A black hole attack is one of the security challenges in WSN at the network layer in Low-Energy Adaptive Clustering Hierarchy (LEACH) routing protocol.

Several scholars proposed energy-efficient and security schemes that enhanced the LEACH routing protocol. But there is a gap in addressing both energy efficiency and and black hole attack issues at the same time in the LEACH routing protocol during cluster head(CH) selection. This paper improves the energy efficiency and security of the LEACH routing protocol when CH is selected. The energy efficiency improved by modifying the parameters of the cluster head selection algorithm for threshold function. And also, the security issue of the black hole attack detected and prevented based on the behaviors of the sensor node shown in the network when the sensor nodes request to participate in the CHs selection process at the setup phase in LEACH. Unlike LEACH routing protocol, the modified threshold function for CH selection algorithm of proposed routing protocol includes the parameters of residual energy of sensor node, the average residual energy of networks, and distance between the sensor node and base station (BS) to calculate the threshold value. The CH selection algorithm decides whether sensor nodes are selected as CHs or not in the network depending on the threshold value. This improvement extends the network lifetime and transmits reliable data in WSN. According to the simulation result, the proposed protocol reduces the energy usage of WSN and minimizes the probability of malicious nodes selected as cluster heads in the LEACH routing protocol.The proposed routing protocol improves the LEACH routing by an average of 34.67%, 28.43% 237.65% and 21.676% in terms of residual energy, network lifetime, packet sent to BS and throughput's respectively. After implementing security solution on the proposed LEACH it improved by 1.88% in terms number of packet sent to BS under malicious attack. The proposed routing protocol for WSNs simulation was conducted with MATLAB on two scenarios.

Key Words: - Energy-efficient and Secure LEACH, Cluster Head Selection Algorithm, Black Hole Attacks in WSN, Black Hole Attack Detection,Threshold Function.

Acknowledgment

In the first, place I want to forward my sincere thanks to God and Saint Mary. Next, I would like to give my grateful and sincere thanks to Dr. Yalemzewd Negash for his guidance, patience, and support during my graduate studies. I would also like to thank Dr.Bisrat Derebssa and his colleagues for their valuable feedback to this thesis during each phase of seminars presentation.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BS Base Station

BHA Black Hole Attack

DEEC Distributed energy-efficient clustering

DES Data Encryption Standard

ES-LEACH Energy Efficient and Secure Low Energy Adaptive Clustering Hierarchy

CDMA Code Division Multiple Access

CH Cluster Head

CHs Cluster Heads

FND First Node Die

IDS Intrusion Detection System

LEACH Low Energy Adaptive Clustering Hierarchy

NCH None Cluster Head

RSA Rivest -Shamir- Adleman is Crypto System Algorithm

TDMA Time Division Multiple Access

WSN Wireless Sensor Network

Chapter 1

Introduction

1.1 Introduction

A Wireless sensor network (WSN) contains many tiny sensor nodes which communicate with each other wirelessly from diverse directions.These sensor nodes are built from a semiconductor device, and they have limited resources due to their size[3]. The sensor node senses the event; sends the sensed data to the next node or the base station [4]. Sensor nodes consist of sensing, processing, and communication modules. WSN applications are found in different areas such as surveillance and motoring in the military field, environmental and agricultural monitoring, home appliances, traffic management, health care, manufacturing industry, mining, anti-terrorism disaster field, etc. [5].

In WSN, implementing a security mechanism is a challenging task due to the nature of building components of WSN; limited processing power, storage capacity, communication bandwidth, and energy of nodes [5, 6]. These weak entities make WSN easily vulnerable to a variety of attacks. These are the physical layer, data link layer, network layer, transport layer attacks [5]. From these attacks, routing protocol attacks at the network layer is one of the challenging attacks in WSN. Some of the routing protocol attacks at the network layer in WSNs are sinkhole, wormhole, Sybil, hello flood, and black hole attacks[3, 7]. Black hole attack is one of the active types of attacks in WSN and among the most destructive routing attack in

WSN [7].

In recent times, energy and security is the main issue in WSN design. Low Energy Adaptive Clustering Hierarchy (LEACH) is one of the cluster-based energy-efficient routing protocols used in WSN to overcome the problem of energy inefficiency in WSN design. But this protocol was vulnerable to black hole attacks, especially the CH in LEACH routing protocol is the main focus area for this type of attack. In addition to this, it has energy inefficiency problems when selecting CHs at the setup phase and data transmission at steady-state phases in LEACH.

Several variants of LEACH routing protocol have been proposed with energy-efficient CH selection for WSN. But there is limited research that has been done on both energy efficiency and security issue of black hole attack simultaneously on the LEACH routing protocol. The security mechanisms implemented for LEACH routing protocol are cryptography security algorithm and sensor node trusted-based mechanisms. The cryptography security mechanisms implemented for the LEACH routing protocol in WSN is not suitable for energy efficiency [8], and this security mechanism is unable to prevent and detect internal attacks such as black hole attacks in WSNs [9, 10]. In a black hole attack, the malicious node accepts the data packet from the source and drops or swallows it instead of forwarding it to the destination.

In this paper, we propose a modified LEACH routing protocol that enhances LEACH protocol in terms of energy-efficient and secure CH selection techniques against black hole attack in WSN. The proposed approach in this paper is called the name ES-LEACH routing protocol against black hole attack in WSN. In the proposed protocol, CH selection is based on a distance between the sensor node and base station, residual energy of each sensor node, and average energy of the network to make energy-efficient CH selection. In addition to enhancing CH selection algorithms using energy-efficient parameters, the proposed system also adopts a simple security mechanism based on sensor node behavior in the network during CH election. The security solution in this paper prevents the malicious nodes to becomes CH in the network, which improves data availability. ES-LEACH increases the number of data packets sends to the base station, and reduces the energy consumption of the WSN, and extends the network lifetime. In this paper, simulate the proposed routing protocol with MATLAB and evaluate the

performance of the proposed routing protocol with LEACH and previously designed cluster-based routing protocol.

1.2 Statement of the Problem

The energy constraint and security vulnerability is the main issue in WSN that affects the network lifetime and security of data transmitted using the routing protocol. These two issues occurred in WSN due to the nature of limited resources in the building components of WSN. The sensor node is one of the components that exist in WSN. It has limited resources such as limed memory capacity, storage space, and a non-replaceable battery source. Implementing the most commonly used traditional cryptography security schemes[11] in WSN on these resource-limited components is difficult. Even if we use a cryptography algorithm-based security solution to protect WSN routing from attack, it consumes more energy, and also it has limitations for preventing internal attacks such as black hole attack in the network[9].

The main goal in WSNs is utilizing limited energy sources effectively and securing routing protocol to extend the network lifetime and ensure the security of data packet transmission using a routing protocol in WSNs. One of the security issues in WSN is a black hole attack, which is an active and harmful network layer attack of routing protocol. LEACH routing protocol is one of the cluster-based routing protocols affected by this type of attack during CH selection. Today, improving both energy efficiency and security of routing protocol in WSN is the main hot research topic area. To overcome the problem of inefficient energy utilization in WSNs, using a cluster-based routing protocol is most effective than using a flat routing protocol in WSNs. LEACH is an energy-efficient routing protocol, but it has its limitation on energy utilization and security. In recent times several techniques have been proposed to reduce the energy consumption of the LEACH routing protocol. However, research conducted on both energy efficiency with a security vulnerability regarding black hole attack protection is limited.

In LEACH and Variants of LEACH routing protocol, CH is selected based on one or more parameters at a time. Those parameters are sensor node residual energy, average residual energy of networks, number of neighbor nodes, the position of nodes from the base station, etc., which

improve the energy efficiency of routing protocol during CH selection and data transmission. But it has a limitation that does not consider both energy efficiency and security when selecting CH.

In this paper, propose improved LEACH routing protocol in terms of energy efficiency and security simultaneously. The energy efficiency of the LEACH routing protocol was handled by enhancing the parameters of the cluster head selection algorithm in the LEACH routing protocol for threshold value calculation. In this thesis, the threshold value calculation for the CH selection algorithm includes the parameters of average residual energy of network, residual energy of sensor node, and distance between the sensor node and BS. And also, the black hole attack issue in LEACH is handled by adopting the behavior of the sensor node shown in WSN during the CH selection process.

1.3 Objective

1.3.1 General objective

The main objective of this research is to propose an improved LEACH routing protocol based on energy-efficient and secure cluster head selection techniques against black hole attacks in WSN.

1.3.2 Specific objective

- To improve CH selection algorithm threshold function by considering sensor node residual energy, average residual energy of network, and distance between the sensor node and BS
- To improve the energy efficiency of LEACH routing protocol using improved cluster head selection algorithm threshold function
- Modeling black hole attack and injecting into the network for simulating black hole attack scenario in WSN
- To identify and prevent malicious nodes selected as CH in the network based on its residual energy level shown at the CH selection phase
- To simulate proposed routing protocol in MATLAB and compare with existing related routing protocols in terms of various network performance metrics presented in chapter 5 section 5.2.

1.4 Scope of the project

The scope of this thesis focuses on improving the energy efficiency and security of the single hope LEACH routing protocol. The energy efficiency of the LEACH routing protocol improved by modifying the basic threshold function of the LEACH routing protocol using different parameters. Those parameters for energy-efficient CH selection are listed in section 1.2. The security mechanisms adopted in this paper for LEACH routing protocol are intended to prevent the compromised node with black hole attack selected as CH in the network.

1.5 Contribution

The main contribution of the proposed energy-efficient and secure LEACH routing protocol against black hole attack in WSN are:

- Improve LEACH routing protocol energy utilization and security
- Provide energy-efficient and secure cluster head selection algorithm
- Minimize the energy consumption of each sensor node in WSN and increase the network lifetime and number of packets sent to BS
- Provide a secure subsystem for the Internet of things (IoT)
- Reduce the number of packet drops due to black hole attack

1.6 Research Methodology

Wireless sensor networks are created with a lot of sensor nodes that communicate with each other using a wireless medium. Energy constraints in WSN are the main issue so that, sensor nodes must arrange themselves into the energy-efficient cluster-based routing to reduce the energy consumption in WSNs. On the other hand, due to the nature of WSNs, routing protocol in WSN is vulnerable to different attacks during the routing process. To avoid this problem, enhancing security solutions within WSNs routing protocol.

Inefficient utilization of limited energy resources and black hole attacks are the problems in the LEACH routing protocol in WSN. This problem in LEACH routing protocol is due to random CH selection without considering the sensor node remaining energy, distance between sensor node selected as CH and BS, and BS position in the networks, which are directly related factors affecting the energy efficiency in WSN. In addition to this, the selected CH in the network becomes inactive due to a black hole attack. This type of attack denies the service of WSN. To overcome the problems of the LEACH routing protocol mentioned above, we propose improving the energy efficiency and security of the LEACH routing protocol against black hole attacks in WSN. The following tasks and procedures have been conducting in this research.

1.6.1 Literature Review

Energy constraint and security issue is the main challenge for WSN design. The literature review conducted in this paper, mainly concerned with understanding, and identifying the gap on LEACH routing protocol energy efficient utilization techniques done by other scholars in WSN. In addition to this, the effect of black hole attack in LEACH routing protocol, black hole attack detection, and prevention algorithms efficiency in terms of energy utilization and attack reduction on LEACH, and variants of LEACH protocol.

1.6.2 Proposed Approach Algorithm Modeling

To improve the energy efficiency and security of the LEACH routing protocol, we identify the methodology used to improve the energy efficiency and black hole attack during the CH se-

lection process in LEACH. In this paper, we model algorithms for improving energy efficiency and security of LEACH routing protocol against black hole attacks in WSN. The detail of this model presented in chapter 4 at section 4.2

1.6.3 Simulation Environment Setup and Network Model Assumption

Energy efficiency and security of routing protocol in WSN such as LEACH routing protocol are affected by different factors. The parameters of the sensor network and assumptions of the network model, i.e., sensor node and base station characteristics in the network during simulating routing protocol in WSN, determine the result of the network as a whole. So that in this thesis, we identify the network model assumption and simulation parameters before the beginning of the proposed model simulation.

1.6.4 Proposed Approach Result Analysis and Evaluation

To evaluate the performance of the proposed approach, we used commonly used network performance metrics such as the number of packets sent to the base station, residual energy in the network, network lifetime, and throughput. These evaluation performance metrics are used to evaluate our approach relative to LEACH and similar routing protocol for WSN.

1.7 Thesis Outline

The remaining part of this document is organized as follows. In Chapter 1, introduction to WSN, challenges in WSN, research objective, and research methodology are presented. The statement of the problem and contribution of this thesis is also presented in this chapter. In Chapter 2, a detailed description of WSNs application, security threats, and security mechanism implementation challenges in WSN and also cluster-based routing protocol and black hole attack in WSN especially LEACH routing protocol operation principle, advantage, factors affecting LEACH routing protocol performance, limitation of LEACH and variant LEACH routing protocol, and the black hole attack issue in LEACH are presented. In Chapter 3, a literature review focus on LEACH routing protocol energy-efficient CH selection and security

solutions regarding black hole attacks are presented. In Chapter 4, the proposed routing protocol model and requirements for the model are presented. In chapter 5 and chapter 6, discussion on simulation result, conclusion and future recommendation of this thesis are presented.

Chapter 2

Theoretical Background

2.1 Wireless Sensor Network Application and Security Threats in Wireless Sensor Network

2.1.1 WSN Application area

In recent times, WSN widely used in different industry sectors. The purpose of using WSNs technology in a different area is not the same. The application of WSNs is different based on the type of application required in each industry. WSN technology is applicable for several areas [12, 13, 14, 15, 16] as presented in the following subsections.

2.1.1.1 Environmental and Agriculture

WSN is used to monitor environmental and agricultural activities. Environmental and agricultural activities controlled with different types of sensors such as RF sensors, water sensors, gas sensors, humidity sensors, seismic sensors, smoke sensors, etc. These sensors are used to build WSNs that used to monitor environmental and agriculture activities[17]. WSNs application in environmental and agricultural monitoring activities are grouped into different classes. Those classes are precision agriculture, cattle or habitat monitoring, environment monitoring, and forestry monitoring. Each class is further sub-divided into different groups. The preci-

sion agriculture divides into irrigation control, diseases prediction, crop monitoring [17] and greenhouse monitoring [17]. The cattle or habitat monitoring includes the activities of animal localization and diseases detection. On the other hand, environmental monitoring classes focus on air quality monitoring, water control, and active volcano monitoring, and the final class is forestry monitoring which monitors the activities in the forest.

2.1.1.2 Health Care

WSN is applicable in health care to monitor patients in hospital or their homes [17]. Sensors that used as sensor nodes to build WSN for health care application may be biomedical sensors, motion sensors and temperature sensors used in the form of patient wearable monitoring, biomedical sensors, position sensors, and seismic sensors used as home assisting systems and seismic sensors humidity sensors and RF sensors used as hospital patients monitoring[17]. In health care industry WSNs applications are categorized into vital status monitoring and remote health care surveillance groups. The vital status monitoring focuses on cardio monitoring and sudden falling, while the remote health care surveillance handles the elderly monitoring and rehabilitation supervision activity controlling with WSNs in the health industry.

2.1.1.3 Public Safety and Military Systems

WSN is used in the field of the military for the purpose of battlefield surveillance, combat monitoring, and intruder detection. In order to achieve the specified activities required in public safety and military system, the type of sensor node also different for building WSNs for the required application. In public and military systems WSNs “may use biomedical sensors, acoustic sensors sonars, seismic sensors and visual sensors for combat monitoring, battlefield surveillance and intrusion detection and soon [17]. WSN in public safety and military systems is grouped as active intervention and passive supervision. The active intervention includes the activities of firefighter monitoring, soldier supervision, and border surveillance. The passive supervision of public safety and the military system uses WSNs for fire detection, perimeter protection, and structural health monitoring.

2.1.1.4 Industry

WSN deployed in the industry for monitoring different activities and materials within the industry. Position sensor, motion sensor, visual sensor, vibration sensor, RF sensor, optical sensors, corrosion sensors, heat sensors, etc., which used to build WSNs systems to monitor activities and material in industry [17]. Some of the activities and material monitored with the help of WSNs application in different systems. WSNs are used in SCADA systems for pipeline monitoring and production line control, in smart grids, used for voltage monitoring and home energy management, in the manufacturing industry used for monitoring explosive materials and industrial process monitoring.

2.1.1.5 Transportation System

WSNs applied in transportation systems for traffic control, providing safety systems indicators, providing traffic information, diplomatic monitoring, and air traffic control. Acoustic sensors, accelerators, visual sensors are some of the sensors used by WSNs in transportation systems [17]. The application of WSN in transport systems for traffic control purposes such as vehicle counting, traffic light control, for safety systems such as collision avoidance and accident signaling, for service such as traffic jam information, parking space assistance, and diplomatic communication, e-learning, and air traffic control [12].

2.1.2 Security Threats in WSN

Wireless Sensor networks are easily exposable to "security attacks due to" their nature of dynamic topology, open wireless medium, lack of central infrastructure, etc. Some of the security threats in WSN are listed and described below in different categories. Categorizing and putting a single security issue in WSN into a single type category is difficult shown by several scholars in their work.

A. An External or physical: Attacker does not have the control of sensor nodes. It could overhear or eavesdrop on information in the network or disrupt physically, the service of a wireless network [18]. The external or physical attack done in the form of jamming,

eavesdropping, node tampering, and hardware hacking [19]

B. Internal or network attacks : "Attacker can capture the sensor nodes by injecting faulty data to control their activity. It uses the attacked nodes to disturb the network traffic[18]."

C. Passive Attacks : Passive attacks are run to collect and "analyses information about the environment [18]" that used to show suitable loopholes in the environment for performing an active attack. To achieve this objective passive attacker uses eavesdropping, monitoring, knowledge of confidential information/ Camouflage Adversaries, and traffic analysis [18, 20] techniques in the network.

D. Active attack : The objective of this attack in WSN is to alter the proper functioning of the routing protocol. To achieve this objective, the active attacker in the network uses packet modification, overloading, energy depletion, reducing traffic, and data loss techniques in WSNs [18, 20]. Sometimes this type of attacks called as network layer or routing attack which discussed bellow[18, 20].

Selective Forwarding: a malicious node in the network collect packet from its neighbors and some selected packet rather than transmit to the required destination or refuse some sensor node data during the transmission process.

Black hole Attack: This type of attack creates false information about the route from the source to the destination for data transmission. This malicious node under black hole attack advertises itself as the best route from sensor node to BS, such as it has much more energy than other nodes, it is near to the BS, etc.

HELLO flood attacks: A malicious node sends or replays a routing protocol's HELLO flood packets from one sensor node to sensor another with more energy. This attack increases energy degradation and collisions, creating false transmission routes in the network.

Wormholes Attacks: This type of attack is a critical attack in which the attacker records the packets sent from one node to the other in another place in the network and tunnels those to another sensor node that is not part of that communication process or false data destination.

Sinkhole Attack: This type of attack creates by advertising false information to create a center of attraction for other nodes in the network.

Replay Attack: A type of network layer attack is created by repeating a valid data transmission in the network. The network performance is disrupted by generating false error messages, disrupting the routes, increasing congestion and interference.

Sybil Attack: the future of this attack is presenting multiple identities in the network and Compromise of transmission routes.

Spoofed, altered, information: The main future of this attack is creating non-existent information or partially modifying data. This type of attack reduces the performance of the network by attracting/repelling network traffic, creating routing loops in the network.

2.1.2.1 Challenges for Security Mechanism Implementation in WSN

Including the security mechanisms used in a wired sensor network for WSN design is a challenging task. The components that build WSN are resource-constrained and very small in size. WSNs are built from hundreds to thousands of tiny sensor nodes that are made up of semiconductor devices powered with a non-replaceable battery. So that to implementing standard security mechanisms such as RSA, DES, etc. as a wired network for energy and resource-limited components of WSN is difficult. Generally, WSN faces the following challenges due to its nature and the type of components that exist within it. Some of the challenges in WSNS are energy constraint, limitation of bandwidth,dynamic typologies, hostile deployment environment, scalability, availability and reliability, Ad-Hoc deployment and nature of wireless medium in WSN[18, 20]. From the above listed issue, this thesis focus on the security issue regarding the back hole attack and the energy constraint issue handling techniques in WSNs routing protocol design.

2.1.2.2 Main Security Objectives in WSN

The security objective of WSN mainly dived into two groups. These are primary and secondary or supplementary goals of security [11, 18, 19, 20]. Confidentiality, data integrity and availability are grouped under the primary goal of security [11, 18, 19, 20] and also authentication, data freshness ,anonymity, self-organization, time synchronization, robustness/resiliency / survivability, secure localization, transparency, authorization and nonrepudiation grouped un-

der secondary or supplementary goal of security in WSN [11, 19, 20]. Tomić and McCann in[19] further divides the secondary goal of security in WSN into data level requirements (anonymity, data freshness), access level requirements (authentication, authorization, accessibility) and network level requirements(self-organization, time synchronization, robustness/resiliency).

2.2 Cluster Based Routing Protocol and Black Hole Attack in WSN

2.2.1 Routing Protocol in WSN

Routing protocols are a set of rules and communication standards in the network to be followed by the source and destination to send and receive data between them.The routing protocol can be classified based on routing protocol function or target of applications, sensor node participation, and network structure in WSNs into different categories. There are three types of routing protocols based on the communication route establishment within the network during data transmission from source to destination; those are proactive, reactive and hybrid protocols [21]. Based on the network structure, there are three groups of routing protocol in WSN which are flat network routing protocol ,hierarchical network routing protocol and location based routing protocol[22]. Figure (2.1) shows the classification of WSNs routing protocols adapted from[21, 23].

a. Flat Network Routing Protocol: In this type of routing protocol, all sensor nodes in the network collect the information from their surroundings, and also they have the responsibility to send the collected data to the destination.

b. Hierarchical Network Routing Protocol: In this type of network, the sensor nodes arranged in hierarchically structure in a sensing field. In this structure there are two types of nodes, which are the member sensor node and the CH sensor node. If the member sensor node wants to send data to BS it can not send directly to BS. First member node send the sensed data to its respective cluster and then each CH aggregate the revived data from ts

member and finally sent it to BS. This paper focus LEACH routing protocol, it is one of hierarchical routing protocol in WSN.

c. **Location Based Routing Protocol**: To establish the communication in location-based routing protocol in WSN position of each sensor node in the network must be known. This protocol is named position-based routing or geographic routing protocol.

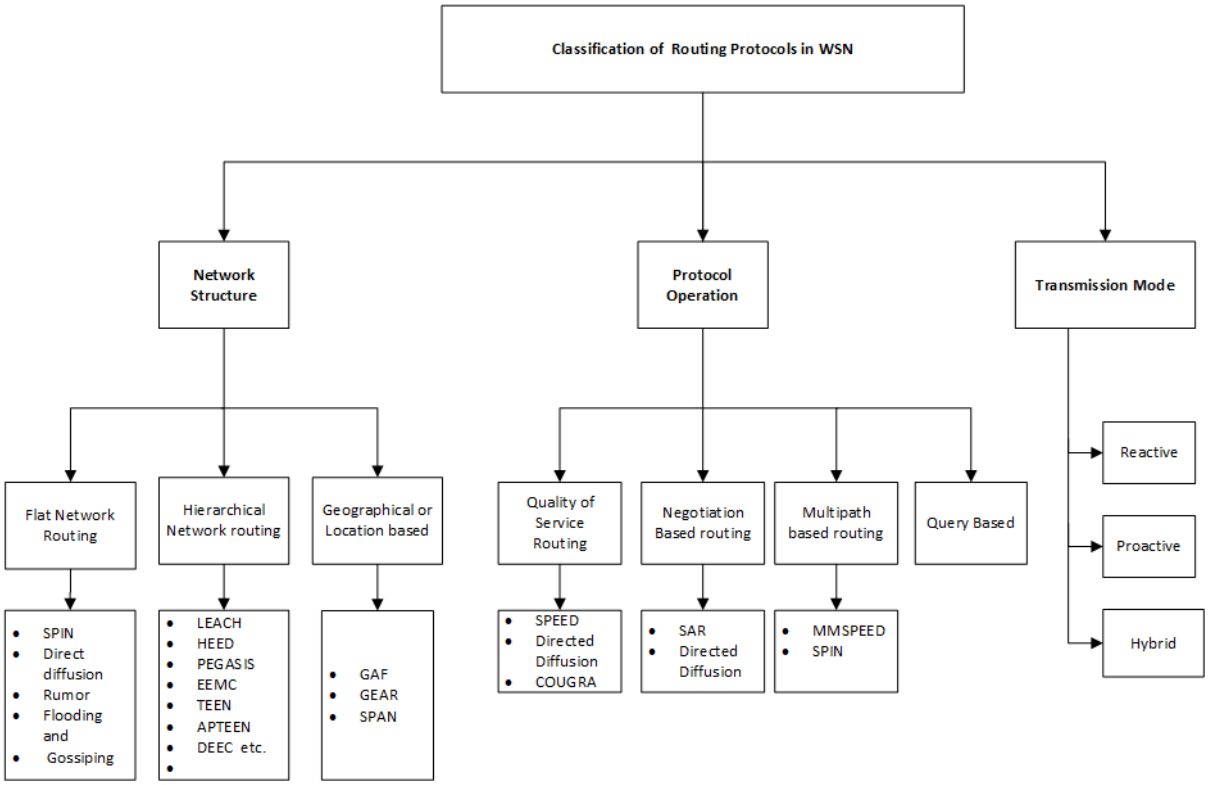


Figure 2.1: Routing protocols classification in WSN

2.2.1.1 Clustering Algorithm in WSN

"Clustering refers to a grouping of sensor nodes into cluster [24]." Clustering is a critical mission in Wireless Sensor Networks for energy efficiency and network constancy [25]. Clustering in WSNs is very important to solve many problems like scalability, energy, and lifetime issues of sensor networks [24]. Some advantages of clustering in wireless sensor networks (WSNs) are it increases the energy efficiency of sensor nodes, facilitates lower energy consumption, supports scalability, is used to reduce the routing table stored at each sensor node, and conserving communication bandwidth. In cluster based WSN, the sensor nodes in the network grouped into different clusters and each cluster have its cluster head that is responsible

to transfer the collected data from the sensor node to BS. The general architecture of cluster based WSNs presented in figure (2.2) that is adopted from [26]. To create clusters in WSN different clustering algorithms create a cluster by making different clustering criteria that are used to select CHs in the network.

LEACH routing protocol is one of the routing protocol in WSN using clustering techniques. Cluster based routing protocol like LEACH routing protocol used to overcome the problem of energy inefficiency problem than flat routing protocols[27], but it has a limitation on energy efficient and secure CH selection due to different parameters consideration during cluster head selection and data transmission period. So that several researchers improve cluster based routing protocol by using different parameters based on the required application; LEACH routing protocol is one of those types of routing protocol that have been improved with several researchers to improve the energy efficiency and security of routing protocols in WSNs, but there is a limitation on both energy efficiency and security simultaneously.Nowadays, these two issues are an open research area on LEACH routing protocol.

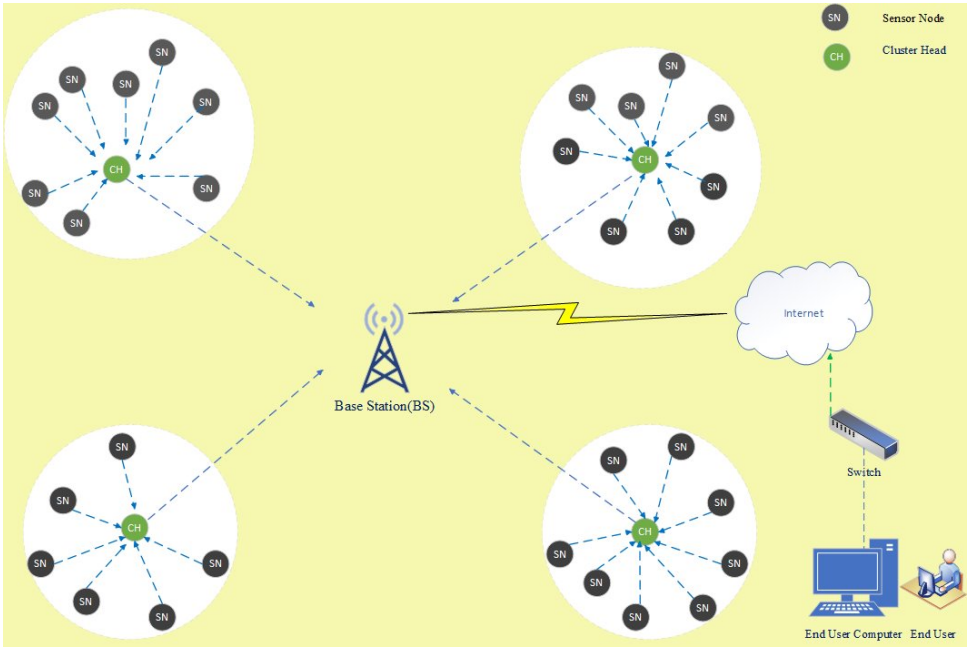


Figure 2.2: General architecture of cluster based Wireless sensor network

2.2.1.2 LEACH Routing Protocol

LEACH protocol is the first cluster based routing protocol developed by Heinzelman et al.[28] for WSN. LEACH (Low-Energy Adaptive Clustering Hierarchy) is a "self-organizing, adaptive clustering protocol that uses randomization to distribute the energy load among the sensor in the network." The main aim of this protocol is to extend the network lifetime by minimizing energy utilization of the network using a random distribution of energy load among the sensor node in the network [1].

2.2.1.3 LEACH Operation Principle

LEACH routing performs its task by dividing into several rounds. Each round in LEACH consists of two phases. Those are the setup phase and steady-state phase as shown in figure 2.3 [1] on page 2.

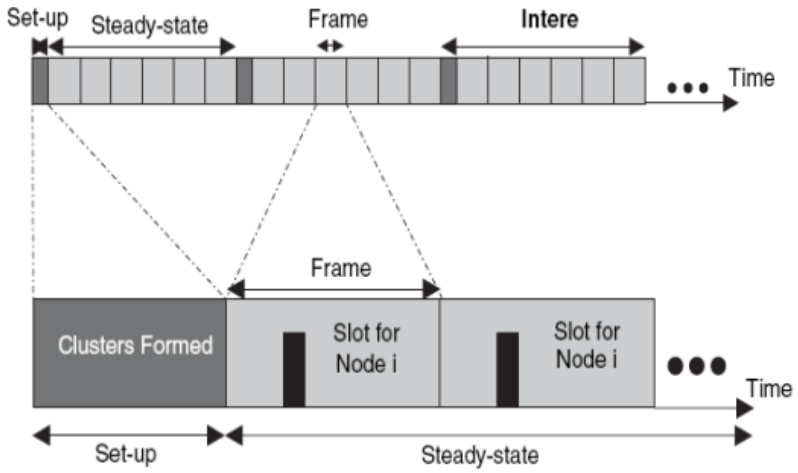


Figure 2.3: LEACH routing phase [1]

I. Setup Phase

The main goal of this phase is "cluster-head selection and cluster formation"[1]. Under setup phase there exists three sub-phases. These are the advertisement phase, cluster setup phase,and schedule creation phase.

Advertisement

In this phase the sensor node before making an advertisement it must be selected as cluster head based on the calculated threshold value[28]. The threshold value depends on the

threshold function parameters consideration during threshold value calculation such as: residual energy, mobility, and distance from base station,initial energy of sensor nodes, average energy of network, e.t.c [27, 28]." After calculating the threshold value using one or more parameters and if sensor node satisfies the criteria seated by threshold value then sensor node selected as CH and sends advertisement message to the other nodes in WSN. Equation(2.1) is the LEACH routing protocol threshold function algorithm based on only the pre-determined CH selection probability parameter.

$$T_{(n)} = \begin{cases} \frac{p_{opt}}{1-p_{opt}\times\left(r\times mod\,\frac{1}{p_{opt}}\right)}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{2.1}$$

where :- $T_{(n)}$ = threshold value

p_{opt} = the initial desired percentage of CHs probability(e.g., p_{opt}= 0.1)

r= the current round, and

G= is the set of nodes that have not been CH in the last $1/p_{opt}$ rounds

For each sensor node n in the network is assigned a randomly generated value between 0 and 1. Then randomly generated value assigned for each sensor node compared with the calculated threshold value T(n) in equation (2.1) to decide sensor node is CH or not. If the randomly assigned value of the sensor greater than the T(n) value, that sensor node is selected as CH at that round. LEACH consists of several rounds, in each round new cluster head is selected. But sensor nodes selected at each round don't participate CH selection process until $1/p_{opt}$ rounds while sensor nodes participate CH selection after $1/p_{opt}$ rounds [28]. After the sensor nodes are selected as cluster heads (CHs), each CHs send an advertisement message with non-persistent CSMA MAC protocol within the network and waiting join request message[28]. The non-cluster head node in the network accepted the CH advertisement and make a decision based on the signal strength non cluster node send a join message with CSMA MAC protocol for their selected CH.

Cluster Setup Phase

In this phase, the clusters Heads (CHs) accept join request messages from member nodes.

A member node uses CSMA MAC protocol to send a join message to its preferred CH. Then the CHs send acceptance for join request message for their member node and finally, the required number of cluster for that round is created.

Schedule Creation

Based on the number of member nodes in the cluster, cluster heads (CHs) allocate time for their member node using TDMA scheduling. Then the member node for each CH sends their data to its CH on the given time on the other had the sensor node turnoff their radio until its allocated time starts but CHs radio units always turn on to receive and transmit data. [28, 29].

II. Steady State Phase

The main task in this phase is gathering data, fusing or aggregating gathered data and finally, delivery to the base station [1]. In this phase, member nodes send "their data to the cluster head" within the allocated time slot. The first task of CH after collecting data from their cluster member is data fusion (data aggregation or compress the data into a single signal), which reduce the number of data packets to BS and the second task is sending the aggregate data directly to the base station using CDMA techniques; this is in the case of single hop LEACH [1, 28, 29]. In the case of multi-hop LEACH the aggregated data at CH may not only transmitted directly to the base station it may be transmitted to other CH for further data aggregation. After the end of steady state phase the network starts again from setup phase for several rounds as shown in figure(2.4) [30] on page 531.

2.2.1.4 Advantage of LEACH Routing Protocol

LEACH routing protocol is one of the routing protocol in WSN using clustering techniques. Cluster based routing protocol like LEACH routing protocol used to overcome the problem of energy inefficiency problem than flat routing protocols. The main advantage of LEACH routing protocol in WSN arrange the sensor node into cluster and each cluster deliver data to BS with its cluster head(CH), which reduce the bandwidth usage and energy consumption of each sensor node for direct delivery of data to BS. Here is some of the advantages of LEACH

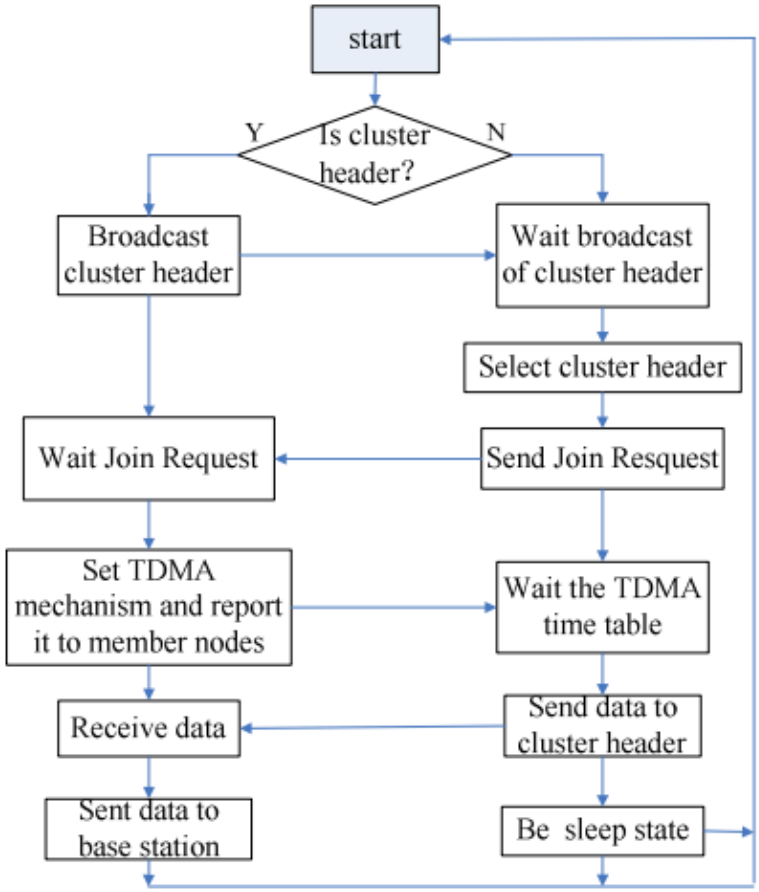


Figure 2.4: Flowchart Model of LEACH Protocol Operation Principle

routing protocol in WSN[8].

- LEACH routing protocol use only CH sensor node for data transmission to BS, which reduces communication between each sensor node directly to BS, this is used to reduce the energy consumption and increase the network lifetime.
- In LEACH CH aggregate the data collected from its member this reduce correlated data transmission to BS so that it can save energy for wasting for correlated data transmission.
- CH member node in LEACH turns on its radio module only to send data to CH based on the allocated TDMA schedule with by its CH; otherwise, go to sleep mode. TDMA reduces the energy consumption and intracluster collisions in CH.
- In LEACH protocol every sensor node have the same probability to become CH at once in the network. Because the CH selection algorithm only set random probability parameter there is no other criteria put on sensor node to become CH. This is used to distribute load

on each sensor node in the network and to improve network lifetime.

2.2.1.5 Limitation of LEACH Routing Protocol

LEACH routing protocol is an energy-efficient routing protocol for WSNs, but it has its limitations. Several researchers have been done researches on LEACH routing protocol and improve LEACH routing protocol limitations on energy utilization and security schemes. Research on cluster-based routing protocol as LEACH routing protocol is an open and hot research area in WSN routing protocol. Some of the limitations exist in LEACH and variants of LEACH routing protocol listed as follows. In this research,

- CH selection algorithm of LEACH routing protocol does not consider remaining energy of sensor node, location between the sensor node and BS during CH selection [31, 32, 33] CH selection and cluster formation in each round in LEACH increases the overhead on the network and leads to loss of unnecessary energy [32].
- Only support for single-hope communication from CH to BS and it poor scalability for larger networks [34] and applicable for continuous monitoring [35]
- CHs are not uniformly distributed, and the size of the cluster created with CH is also variable. Some CHs have a large number of members; others have small members and also in the sensing field, some CH is near or far from BS, or on the other hand, arranged in a concentrated manner at some point. This creates improper energy utilization and loads distribution on sensor nodes makes the network short[34, 35, 36, 37].
- The number of CH selected in LEACH is extremely fluctuated [38].
- In case of the CH becomes inactive, all stored data in the CH never reaches the BS [39].

LEACH and variants of LEACH routing protocols have different limitations as shown above. The focus on this thesis is regarding optimizing the energy utilization and security vulnerability based on LEACH routing protocol .

2.2.1.6 Factors affecting LEACH Routing Protocol Performance

LEACH is one of the energy-efficient routing protocols mostly used in WSN. The performance of this routing protocol is affected by different conditions such as the CH selection algorithm, security mechanisms, an optimal number of clusters, cluster formation, and position of BS [40] in the network.

To select CH in LEACH several researchers have been considered different parameters for threshold function or CH selection algorithm to reduce the energy cost of CH selection process and data transmission process to the BS. The researcher uses one or more parameters at a time to calculate the threshold value using threshold function. Some of the parameters considered during threshold calculation are the distance between nodes, initial, residual and average energy of sensor nodes, mobility, the distance between CH and BS, optimal number of clusters, number of cluster members in the cluster, etc. To reduce the energy consumption in WSNs, the original threshold function used for the LEACH routing protocol was enhanced by one or more parameters in the process of threshold value calculation that used to select energy-efficient CHs in the network. It is used to balance the load distribution in the network and extends the network lifetime in WSN.

The position of BS in the network under LEACH routing has a great effect on the network lifetime in WSN. If the BS placed far from sensor node deployment area or CH energy depleted in a short period and the network stability period is less than base station positioned near to CH [41]. LEACH routing protocol performance is affected by the number of clusters that exist in the network. If the number of clusters exist in the network is large in number, which expends much energy for communication between CH and BS. On the other hand, if the number of clusters in the network is very less in number, then CH loses more energy for data aggregation and it creates many overloads on the network, which leads to dies early. So that implementing an optimal number of cluster numbers in LEACH routing protocols minimizes the above-listed issue and is also used to maintain the performance of the routing protocol in WSN.

2.2.2 Black hole Attack in LEACH Routing Protocol

In the previous section, we disused factors affecting the performance of LEACH routing protocol related to energy utilization. Now in this section, we will see the effect of black on LEACH routing protocol. Black hole attack in WSN is a malicious node that introduces itself as the correct path from source to destination by "generating false routing information" and attracts all network traffic from the surrounding node towards itself [42]. The malicious node capturing the traffic from its neighbors and swallows or drops the packet rather than transferring the captured packet to the specified destination or base station. The main focus area for the malicious attack in a hierarchical structure-based network is the cluster head nodes(CHs). To achieve this attack the malicious node shows itself it fulfills the required criteria to be selected as CH in the network. One of the techniques most of the time used in cluster-based WSN; during CH selection the malicious node adverts itself, it has the highest residual energy [13, 42, 43]. By these false advertisements, the malicious node becomes cluster head several times in the network and drops the data accepted from the member node rather than transferring to the base station as shown in figure (2.5). LEACH routing protocol is one of cluster-based routing in WSN and is affected by this type of attack. Due to this routing attack, the WSN network does not perform its task with full of its capability, and also security level of the data transmitted over the channel is not fully confidential.

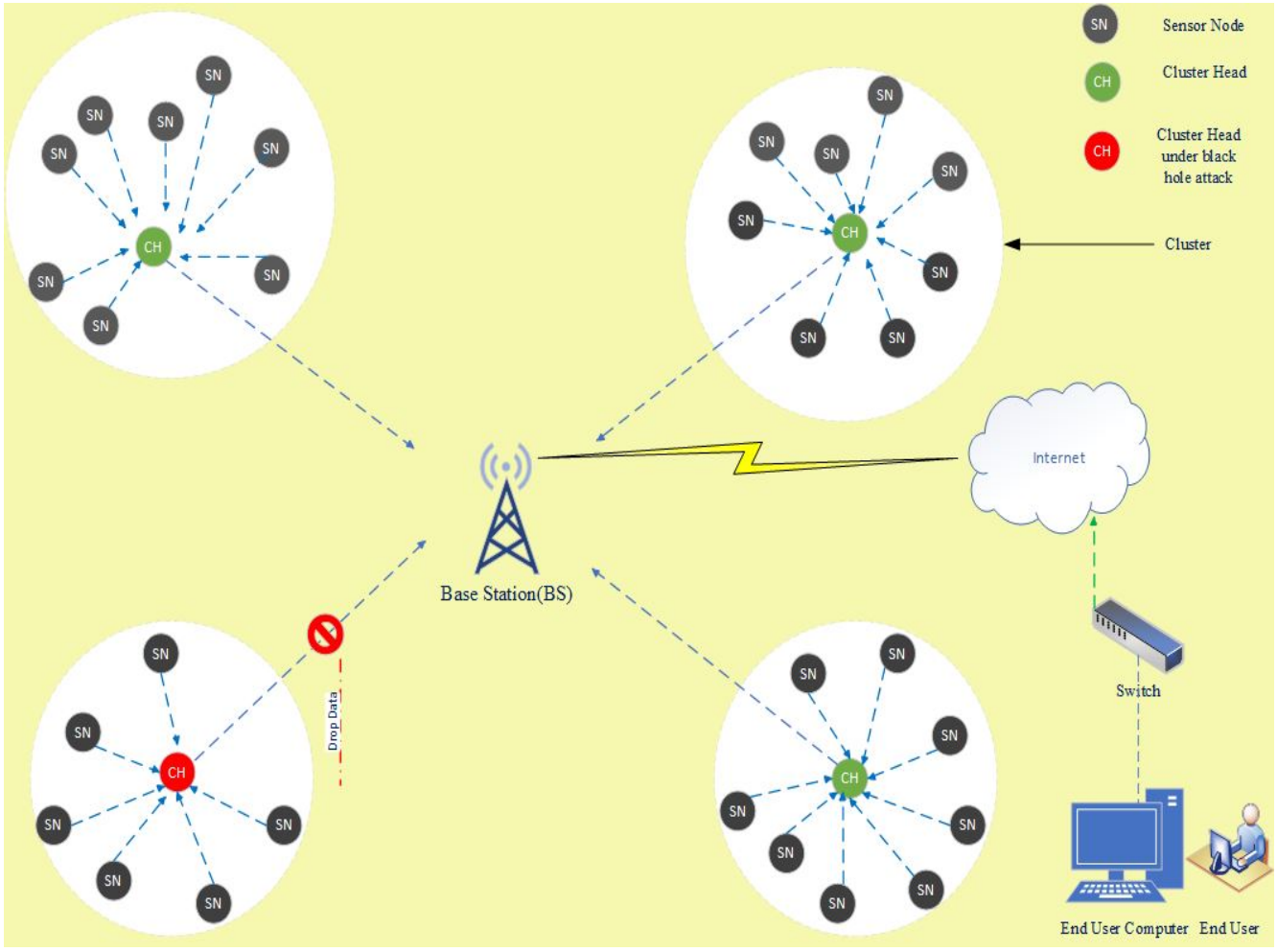


Figure 2.5: Cluster based WSN under Black Hole Attack

Chapter 3

Review of Literature

This section describes energy efficient and secure CH selection in cluster based WSN, especially LEACH and variants of LEACH routing protocols and also black hole attack detection and prevention mechanisms reviewed related to present work. In this section, several researchers' work is presented on effective energy utilization mechanisms and black hole attack detection and prevention mechanisms in cluster based WSN routing protocols, especially on LEACH routing protocol.

In [44] proposes a hierarchical energy efficient intrusion detection system that is used to protect sensor network from black hole attack. The proposed technique to detect black hole attacks in [44] is based on control packet exchange between sensor nodes and the base station(BS). The BS compares the amount of control packet received from the secondary cluster head (SCH) and the corresponding CH to make decisions for the sensor node is malicious or not. The proposed IDS system in[44] consumes little energy, but it is a secure network and energy-efficient compared to a previously conducted research result. The CH selection in [44] considers only residual energy of sensor node so that it needs improvement on the CH selection parameters to make it more energy-efficient.

In [42], the authors only investigated the effect of black hole attack and sinkhole attack on LEACH and LEACH-C routing protocol. In addition to this, the proposed detection mechanism for the attack is in progress. The proposed approach in[42] simulated with and without a black

hole and sink whole attack. The simulation result shows that both LEACH and LEACH-C routing protocols are affected by the attack but, LEACH is more affected than LEACH-C.

Bansal and Saluja [13] proposed an anomaly-based black hole attack detection algorithm and analyzed the effect of black hole attack on leach routing protocol in WSN. In[13] the black hole attack detection algorithm depends on the number of iteration that sensor node to be selected as cluster head in the network. The number of sensor nodes exists in the network grouped into a maximum of six clusters, and one of the sensor nodes performs malicious or black hole attack activity in the network. Simulation results in [13] show that packets sent to the base station under black hole attack decrease while the general remaining energy and packet delivery ratio increases. In [13] Bansal and Saluja suggests simulating the proposed system with different simulators and more parameters, in addition, to use by them. The limitation in [13] is the black hole attack detection algorithm has not been included in their simulation work, and the CH selection doesn't consider the optimal probability number of CH for energy distribution balance in the network.

Kaur et al. in [43] proposed black hole attack detection and prevention algorithm in WSN. The black hole attack was detected based on the sensor node behaviors in the network. If the sensor node is selected as CH previously and its residual energy ratio is not decreased relative to other CH is considered as a black hole attack. Then BS assigns a new cluster head to the member node associated with the cluster head declared as a black hole attack. The proposed system in [43] simulated on QualNet 5.02 Network simulator with a network model that contains a single base station and six clusters. One of the cluster heads maintained to perform a black hole attack in the network. The limitation shown in [43] is the number of clusters is not flexible and malicious CH is predefined, the energy distribution for each sensor node in the network is limited, and also applicable only to single hope WSN structure.

Das and Das [39] develops malicious node detection algorithm based on enhanced LEACH routing protocol. The proposed algorithms in[39] consists of five phases; cluster head selection phase, authentication check phase, detection phase, information dissemination phase, and elimination phase. At cluster election phase Das and Das[39] to calculate modified threshold value

that is used to decide to elect sensor node as clusters head. This modified threshold calculation takes into consideration of residual energy of the sensor node and distance from sensor node to base station rather than random cluster head (CH) selection. Black hole detection method in [39] detect based on sensor node behavior during packet transmission. If the marked node passes the test, it participates in the normal operation of the network starts otherwise this node is detected as a malicious cluster head and stored in a blacklisted table. After detecting the malicious node an alert message sends to the base station and the reverse order from the base station to the neighbor node about this node at the information dissemination phase. In the last phase of the proposed system in [39] cluster head sends the encrypted message to the neighbor's nodes and eliminates the blacklisted node from the network.

In [24] Dewal et al. proposed an approach for a black hole attack detection and prevention techniques based on a hierarchical based network in WSN using primary and secondary cluster heads within each cluster. From those cluster heads, one is active at a time. The cluster head maintains tables that contain IDs of member nodes. When member nodes start to send data to cluster head, cluster head start timers. The member nodes send all data packets within a given time to its CH marked as non-malicious nodes, while other nodes are marked as malicious nodes and removed from the network by the primary cluster head. In the same way, the cluster head that did not send the data packet to the base station was removed by the base station and the second cluster head activated and all nodes informed by the base station to send data to the secondary cluster head. But it has a limitation it does not consider[24] the black hole attack during the cluster head selection phase and implementation of the proposed system.

Alshowkan et al. in [45] provides a new energy-efficient and secure LEACH routing protocol for WSN, which is called LS-LEACH. LS-LEACH is a modified secure version of LEACH routing protocol by incorporating an authentication algorithm into LEACH routing protocol to grant data integrity, authenticity, and availability. LS-LEACH routing protocol simulated on NS-2 simulator with fixed cluster and fixed number of member nodes. The performance of the proposed system and LEACH routing simulation result evaluated with system throughput, network lifetime, and total energy consumption. In these performance metrics, LS-LEACH performs better than LEACH. However, the proposed system in[45] is capable of protecting

the network from attack only when new nodes requesting to join the network does not concern about the internal attack.

In[46], Krishnakumar and Anuratha proposed an energy-efficient cluster head selection of LEACH routing protocol for WSN by enhancing the threshold function of LEACH routing protocol. The enhancement of LEACH based on CH selection takes two parameters into considerations. The first parameter is the distance between cluster head and member node, and the second parameter is the "number of neighbor nodes." The enhanced threshold function is a combination of two score functions calculated with the above two parameters. The first score function is calculated with the distance between CH and neighbor nodes and the second score function is calculated based on the existence of the number of neighbor nodes for CH candidate nodes [46]. The proposed system in [46] compared with LEACH routing protocol improves the performance of the network by 65 % in terms of alive nodes in each round and average residual energy. The gap proposed approach in[46] applicable for the small size of the network, limited parameters of distance metrics, and security issues not taken into consideration.

Khadim et al. [2] proposed an energy-efficient clustering algorithm for WSN designed based on the LEACH-C routing protocol. The proposed system in [2] improved CH selection based on the energy level of the node, the distance between member node and CH, and an optimal number of cluster member node assignments for the selected CH. Member node assignment for the selected cluster head depends on the average sensor node calculated by total sensor nodes in the network, divided by the number of clusters that exist in the network. The performance of improved LEACH –C show the better result with different performance metric [2] than LEACH and LEACH-C routing protocol, but it indicates less performance on data packet sent to CH.

The energy utilization of the LEACH routing protocol in WSN is influenced by the cluster head position from the base station in the network and the remaining energy of the cluster head candidate node in the network. In DBLEACH [47] the sensor node is selected as cluster head in the network based on sensor node location from BS. When the sensor node nears equal to the average distance of sensor nodes in the network it is selected as CH. The distance and energy-aware cluster head selection proposed in [47] is called DBEA-LEACH, which is an

enhanced version of DB-LEACH. Geometric distance between sensor node to the base station and residual energy of sensor node parameters take into consideration to calculate threshold function that used to decide to select sensor node as CH or not in each round. The gap in [47] is the number of cluster heads selected is very small when the residual energy of the sensor node is very small compared to the initial energy of the sensor node. Sharma et al. in [48] proposed energy-efficient cluster head selection based on distance for LEACH routing protocol which is called DBCH Algorithm. Unlike LEACH routing protocol, to calculate the threshold function value for DBCH algorithm in[48] takes into consideration of maximum distance and minimum distance between the sensor node and base station in addition to this it considers residual energy of CH candidate node and distance between candidate CH and BS. Abidi and Ezzedine in [49] proposes an improved CH selection algorithm based on LEACH routing protocol for WSN. The proposed approach improves random cluster head selection of LEACH routing protocol by considering the remaining energy of nodes, the number of neighbors within the cluster range, and the distance between CH and BS. The probability of sensor node i to be cluster head determined by the output of original LEACH threshold function multiplied by cost function of node i, which is calculated with the summation of weighted probabilities each sensor node i of residual energy, number of neighbor nodes, and distance between the sensor node and BS. The simulation result in [49] shows reducing the energy consumption and the network lifetime extension. DE-LEACH in [50] divides the entire sensing area into two parts based on the average distance between the sensor node and base station. The region whose average distance is less or equal to from base station is considered as the first part, cluster head selection in this part is based on the distance between the sensor node and base station. The region whose distance is greater than the average distance from the base station is considered as the second part, cluster head selection in this based on the residual and initial energy of sensor node. The two optimal probabilities of the sensor node to be CH in DE- LEACH covers more than 6 % from the first part, and it covers more than 3 % from the second part in each round. The stability period and throughput of DE- LEACH routing protocols are better than the LEACH routing protocol. But the base station was not placed at the recommended position in the network. LEE et al. in [51] proposes an improved cluster head selection of LEACH routing protocols. Cluster

head selection was improved by modifying the threshold function of LEACH routing protocol by improving the threshold function parameters in terms of residual energy of the node, node distance from the base station, and "the number of cluster heads proximity." The proposed system in [51] addresses the problem of the lower number of cluster head selection occurred when selecting CH based on residual energy and also reduces the probability of adjacent node selected as CH. The improved system is simulated with Matlab and shows better performance in terms of FND evaluation compared with similar existing algorithms.

The main aim of Behera et al. in [52], develop an energy-efficient routing protocol in WSN parallel to enhance the energy limitation that occurred in IoT applications. Behera et al. in [52] proposed an energy-efficient cluster head selection based on LEACH routing protocol in WSN for IoT applications. In[52] cluster head selection algorithm includes the parameters of sensor node initial energy, residual energy, and an optimal number of clusters in the network to calculate the threshold value that is used to decide to select sensor node as CH. This new routing protocol for IoT applications is called R-LEACH. Throughput, residual energy in the network, and network lifetime improves in R-LEACH than LEACH with 60 %, 66 %, 64 % respectively and also packet sent to base station increase in R-LEACH. In addition to this, the Behera et al. in [52] shows the effect of initial energy variation with different network performance metrics. The comparative analysis is done in[52] R-LEACH with other routing protocols developed for IoT such as IGHND, GHND, and CBDAS. The Simulation result shows that R-LEACH was better than others in terms of half node died (HND), and final node died (FND) network life performance metric with varying initial energy of sensor node. The modified cluster head selection algorithm on LEACH routing in [52] has not considered the distance between the sensor node and security issue when CH election is done.

"To the best of our study, none of the previous works have shown" Improving energy efficiency and security of LEACH routing protocol against black hole attack in WSNs simultaneously.

Chapter 4

Proposed Routing Protocol Model

The energy consumption in WSN during communication reduces by using clustering techniques. LEACH protocol is one of the cluster-based routing protocols widely used in WSN that is used to reduce communication costs in the network. While the energy consumption of the LEACH routing protocol is also not an optimal solution by itself. LEACH routing protocol performance is affected by different factors. Some of the factors that affect the performance of cluster-based routing protocols in WSN are base station positioning in the network, an optimal number of clusters, black hole attacks, and energy consumption during CH selection.

Base station far from the center of sensing area, CH consumes more energy to transmit data to BS. If the number of clusters in the network is not optimal, it exposes unbalanced cluster formation and consumes more energy. On the other hand, the black hole attack in WSN reduces the security level of the network and drops the data before reaching the destination. So that to overcome the above-listed problem on LEACH routing protocol in this paper, improving the energy efficiency and security of LEACH routing protocol against black hole attacks in WSN is proposed.

The main objective of improving energy efficiency and security of LEACH routing protocol against black hole attack in WSN is to reduce the energy consumption of WSNs using energy efficient CH selection parameters that are used to distribute load for each sensor node and also reduce the possibility of the malicious node selected as CH in the network.

The basic idea in this paper is to improve LEACH protocol energy consumption and security to extend the network lifetime and prevent black hole attacks during the CH election in WSN. This improvement is carried on by modifying the threshold function for CH selection. In addition to this, the vulnerability of LEACH routing protocol to black hole attack during CH selection is handled based on the behavior of sensor nodes shown at the CH selection stage in each round. Generally, the flow chart model representation of the proposed system algorithm is presented in figure (4.1).

4.1 Proposed Routing Protocol Network Model Assumptions

- BS considers as free from black hole attacks and it has an unlimited energy source
- BS/sink is fixed and installed in the middle of the network
- Sensor nodes are static in position and homogeneous that have the same quality in terms of initial sensor node communication range, storage capacity, processing capabilities, and energy except energy level of malicious node [52, 53]
- Sensor nodes are deployed randomly in the given area[52]
- Sensor nodes always send sensed data with the given time slot or assigned transmission slot to CHs, then CHs sends to BS [52, 53]

4.2 ES-LEACH Routing Protocol against Black Hole Attack in WSN Algorithm

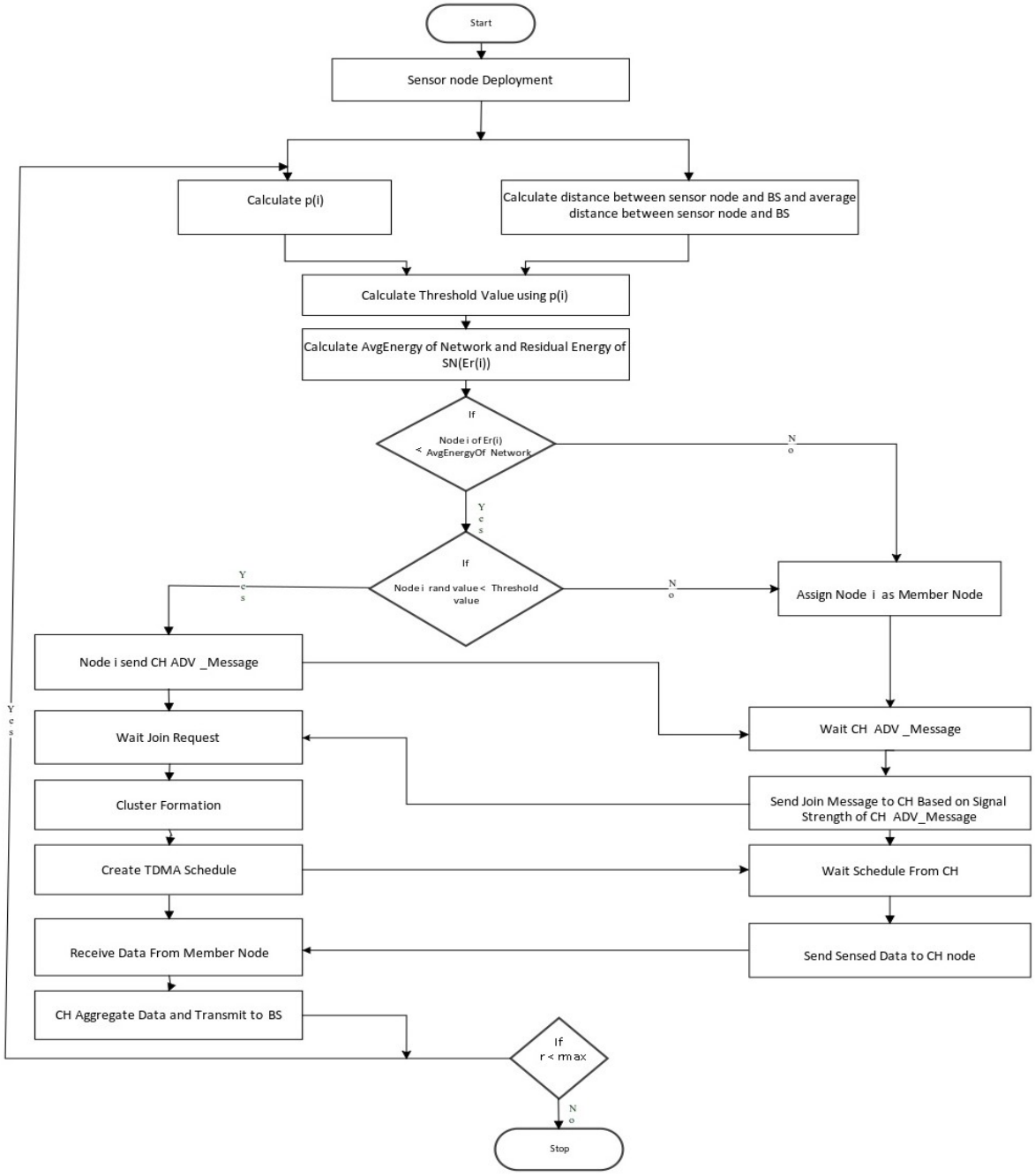


Figure 4.1: Proposed Routing Protocol Flow Chart Model

4.3 Energy Model Used for Proposed Routing Protocol

Sensor node energy in WSN is exhausted mainly during communication such as data receiving, data fusion, and data transmitting process. Energy exhausted for sensing and processing is much less compared to the energy consumed by communication, and it is neglected during the energy consumption calculation process [54]. Energy exhausted in this paper, during the cluster head data receiving, data fusion, and sending data to base station from member nodes[38]. In this paper adopt the first order radio energy model used in [2, 40, 55, 56]. Figure(4.2) shows the block diagram representation of first-order energy model.

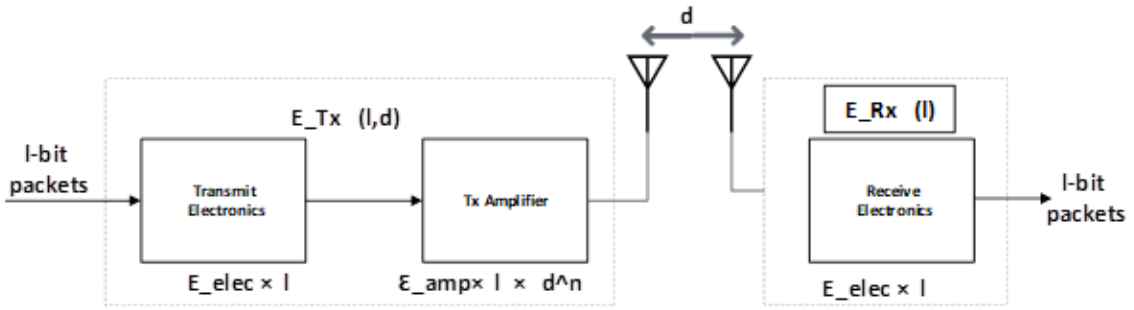


Figure 4.2: "Radio energy dissipation model" [2]

I. **Energy Consumption for l-bit Message Transmission**

The energy consumed by a transmitter during transmission of l-bits message over a distance d meters represented with general equation as shown in equation (4.1) [2]:

$$E_{Tx}(l,d) \quad = \quad E_{elec} \times l + \in_{amp} \times l \times d^{n} \tag{4.1}$$

The energy required to transmit the l-bit of data depends on the transmission distance. If the transmission distance is small compared to crossover distance, use free space propagation model ,otherwise use two-ray-ground model in the equation (4.2) as shown bellow

respectively.[2].

$$E_{Tx}(1,d) = \begin{cases} l \times E_{elec} + l \times \in_{fs} \times d^2, & \text{if } d < d_o \\ l \times E_{elec} + l \times \in_{amp} \times d^4, & \text{if } d \geq d_o \end{cases} \tag{4.2}$$

Where:

E_{elec}: − Is electronics energy of transmission/reception , l size of a message

$\in_{amp}$: − Is magnification times of amplifier

$\in_{fs}$: − Free space probation model

l: −Size of message data i.e number of bits in one packet

d: − Distance between transmitter and receiver

d_o: − Crossover distance or threshold distance

$$d_o = \sqrt{\frac{\in_{fs}}{\in_{amp}}}$$

The energy model parameter E_{elec} depends on the characteristics of the sensor node used in WSN. These characteristics of sensor nodes are expressed in terms of the digital coding, modulation, filtering, and spreading of sensor nodes.

II. **Energy Consumption for l-bit Message Receiving**

The energy required to receive l bits at the receiver computed with equation (4.3)[2]. Unlike energy consumption for transmitting data, the energy consumption for receiving data does not depend on the distance. E_{Rx} is the energy consumed by the receiver circuit.

$$E_{Rx} = E_{elec} \times l \tag{4.3}$$

III. **Energy Dissipation Estimation in WSN**

Assume the network model in this paper consists of N sensor nodes which are deployed uniformly and randomly in a sensing field of M × M dimensions. This network model contains average k clusters within each cluster (N/k -1) sensor node exists excluding CH. The energy dissipated by an NCH node for transmitting l bits of data to CH is estimated

using " equation (4.4)[40].

a. Energy dissipated by non-cluster head node

The energy dissipated in the non-cluster head node is only for transmitting data from its to CH in the network.

$$E_{nonCH} = l \times E_{elec} + l \times \in_{fs} \times d^2_{toCH} \tag{4.4}$$

Where:- d_{toCH} :- Is the euclidean distance from the member node to the CH node

b. Energy dissipated by Cluster Head

The energy dissipated in the CH in three cases. The first is energy dissipated for receiving data from member nodes, the second is energy dissipation for data aggregation, and in the third, energy dissipated for transmitting aggregated data to base station(BS).

$$E_{CH} = l \times E_{elec} \left(\frac{N}{k} - 1 \right) + \frac{lE_{DA}N}{k} + l \times E_{elec} + l \times \in_{amp} \times d^4_{toBS} \tag{4.5}$$

Where:-

$\frac{N}{k} - 1$: $-$ Is number of non-cluster head node with in the cluster

N: $-$ Number of sensor node in the sensing filed that distributed randomly

k: $-$ Is the average number of CH in the network

$l \times E_{elec} \left(\frac{N}{k} - 1 \right)$: $-$ Energy dissipated for receiving data from non- cluster node

$\frac{lE_{DA}N}{k}$: $-$ Energy dissipated for data aggregation or energy consumption for data processing

$l \times E_{elec} + l \times \in_{amp} \times d^4_{toBS}$: $-$ Energy dissipated by cluster head to transfer the aggregated data to BS i.e energy consumption for transmission

c. Total energy dissipation estimation inside a cluster

The total energy dissipated in the cluster is the sum of energy dissipated with the

non-cluster head node and energy dissipated with the CH as shown below [40].

$$E_{cluster} = E_{CH} + \left(\frac{N}{k} - 1\right) E_{nonCH} \tag{4.6a}$$

$$E_{cluster} \approx E_{CH} + \frac{N}{k} E_{nonCH} \tag{4.6b}$$

$$E_{Total} = k \times E_{cluster} + E_{round} \tag{4.6c}$$

$$E_{round} = L\left(2NE_{elec} + NE_{DA} + k \in_{amp} d_{toBS}^4 + N \in_{fs} d_{toCH}^2\right) \tag{4.6d}$$

E_{round}: − is the total energy dissipated in WSNs in a single round

IV. **Optimal Number of Cluster Estimation**

Mainly the lifetime of WSN is determined by the energy dissipation of each sensor node during the data transmission process in the network, and the number of cluster head(CH) exist in the network [57]. If the number of CHs in the network is small for dense sensor networks, CHs die early. If the number of cluster heads is a lot in number for less dense sensor nodes in the network, each CH dissipates more energy for data aggregation. So that using the optimal number of CHs in the network to reduce the energy consumption in WSN and extend the network lifetime. The optimal number of CH estimation in WSN depends on the energy dissipation model used in the network. In this paper, an optimal number of CHs calculation in the network based on the LEACH routing protocol energy dissipation at the data transmission phase. The optimal number of clusters calculate by the derivative of E_{round} in equation 4.6d with respect to k set equal to zero and the final result as shown below [56]:

$$k_{opt} = \frac{\sqrt{N}}{\sqrt{2}\pi} \sqrt{\frac{\in_{fs}}{\in_{amp}}} \frac{M}{d_{toBS}^2} \tag{4.7}$$

Where:-

$$E\left[d_{to}BS\right] = 0.765 \times \frac{M}{2}$$

$$E\left[d_{to}^2 CH\right] = \frac{M^2}{2 \times \pi \times k}$$

The optimal probability of sensor node to become CH in the WSN is also calculated as follows:-

$$p_{opt} = \frac{k_{opt}}{N} \tag{4.8}$$

Where: - N is the number of sensor nodes in the network

4.4 Modified Threshold Function for CH Selection

To calculate the threshold value for CH selection the modified threshold function in this research considers the residual energy of the sensor node, the average energy of the network at round r, and the distance between sensor node i to BS, which used to decide to select energy-efficient CH in the network. The threshold modification carried on the original LEACH threshold function in eq.(2.1) into eq.(4.14 and 4.19).

4.4.1 Cluster Head Selection Approach for Proposed Routing Protocol

4.4.1.1 Cluster Head Selection in Homogeneous Network Model

In this network model, both malicious and normal sensor nodes start with similar energy levels. This section identifies the optimal probability of each sensor node (p_i) based on its remaining energy at each round. After determining p_i calculate the threshold value($T_{n(i)}$) considering with and without distance between the CH candidate sensor node and BS.

a. Improved LEACH Cluster Head Section Based on Residual Energy

Let p_{opt} be the optimal probability of sensor node s_i selected as CH in n_i round cycle in the network. "Based on the current energy $E_{i(r)}$of the node s_i in the round r, the round cycle n_i is selected. Let $p_i = \frac{1}{n_i}$ that is, the average probability to be CH for the node s_i in the round n_i. If the energy in all sensor nodes is the same in every round, i.e., $p_i = p_{opt}$, which guarantees that all nodes die at the same time. The residual energy of the sensor node is different; the selection probability of the nodes with high energy is bigger than that with low energy, which can make the network uniformly consumes energy to prolong the lifetime of

networks. Assume $\overline{E_{(r)}}$ is the average energy of the network in the round r, then: [58]"

$$\overline{E_{(r)}} = \frac{1}{N}\sum_{i=1}^{N} E_{i(r)} \tag{4.9}$$

"Let the average energy $\overline{E_{(r)}}$ be the reference energy compared with the residual energy of node, then" the average probability of ith sensor node to be CH in the round presented with equation(4.10). $E_{(r)}$ is required to calculate the average probability of p_i.

$$p_i = p_{opt}\left[1 - \frac{\overline{E_r} - E_{i(r)}}{\overline{E_r}}\right] = p_{opt}\frac{E_{i(r)}}{\overline{E_{(r)}}} \tag{4.10}$$

The equation (4.10) [59] [prescribes] "that p_{opt} is the reference value of p_i." In a homogeneous network, the reference value of every node differs from each other after the first round in LEACH routing protocol due to the energy dissipation difference that comes from the distance between the transmitter and receiver and the role of the sensor node in the network. So that the optimal probability of the sensor node to become CH in the network based on its residual energy is determined with equation (4.10). As we have seen from equation(4.10), if the residual energy of the sensor node is greater than the average residual energy of the network, the probability(p_i) of the sensor node increase proportionally to p_{opt}. Otherwise, when the residual energy of the sensor node is smaller than the average residual energy of the network, the selection probability of the sensor node to be CH will reduce the corresponding proportion to p_{opt}. In the Eq.(2.1), the p_{opt} is replaced by p_i, then the threshold is obtained to determine whether s_i to be the CH or note in each round using equation(4.11):

$$T_{n(i)} = \begin{cases} \frac{p_i}{1-p_i\times\left(r\times mod\frac{1}{p_i}\right)}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{4.11}$$

If the value of $T_{n(i)}$ increases the probability of the sensor node selected as CH also increases. where: s_i :- Is the number of sensor nodes (i = 1, 2,3,....n)

Moreover, $\frac{1}{p_i}$ is the cycle n_i that the node becomes the CH. According to the residual energy of node to determine p_i , the different cycle n_i to be CH is selected for node s_i with different

residual energy:

$$n_i = \frac{1}{p_i} = \frac{\overline{E_{(r)}}}{p_{opt} E_{i(r)}} = n_{opt} \frac{\overline{E_{(r)}}}{E_{i(r)}} \tag{4.12}$$

where, $n_{opt} = 1/p_{opt}$ that is, the reference cycle of node to be the CH. In Eq.(4.12), the residual energy of the node is much greater than the average energy, the cycle of the node to be the CH will be smaller, and vice versa. So the more high-energy nodes will become CH easily so that the energy of all nodes will be used for almost the same time[58].

To estimate the $E_{(r)}$ of the network without global knowledge of network energy, take an ideal assumption of all sensor nodes and network energy distributed evenly in the environment, and all sensor nodes finished their energy and dead at the same time. With this assumption, the estimated average residual energy of the network is determined with equation (4.13) instead of estimating with equation (4.9) [60].

$$\overline{E_{(r)}} = \frac{1}{N} E_{Total} \left(1 - \frac{r}{R}\right) \tag{4.13}$$

Where:- $R = \frac{E_{Total}}{E_{round}}$

R:- is the maximum round of the network or estimated network lifetime

b. Improved LEACH Cluster Head Selection Based on Modified Threshold Function

The threshold function calculates the threshold value based on residual energy of sensor node and distance between the sensor node and base station, which used for CH selection for improved LEACH routing protocol presented as follows in equation (4.14).

The CH selection algorithm in equation(4.14) also implemented the network model under black hole attack. The black hole attack model for equation(4.14) has a similar energy level to the normal sensor node. In this network, the black hole attack model inserts into the network by assigning a unique ID for some sensor nodes and for these nodes to allow to

perform an attack in the network.

$$T_{(n)} = \begin{cases} \frac{p_i}{1-p_i \times \left(r \times mod \frac{1}{p_i}\right)} \times \left| \frac{d_{to}BS_{avg} - d(i,BS))}{d_{to}BS_{avg}} \right|, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{4.14}$$

Where:- The probability(p_i) based on the sensor node residual energy and the network average energy for selecting CH in WSNs [60].

$$p_i = p_{opt} \frac{E_{i(r)}}{\overline{E_{(r)}}}$$

4.4.1.2 Cluster Head Selection in Heterogeneous Network Model

In this network model, malicious and normal sensor nodes start with different initial energy. Initially, the sensor node used to model malicious attacks in this network model has more energy levels than another sensor node in the sensing area.

In this section, modeling the black hole attack and identify optimally weighted probabilities of a normal and malicious sensor node in the network. Then determine this weighted probability in terms of residual energy in each round. It is used to decide which sensor node becomes CH in the network. Finally, calculate the threshold value according to the modified threshold function.

a. Black Hole Attack Model and Optimal Probability of Normal and Malicious Node

There are two types of sensor nodes in our model that are normal nodes and malicious nodes, which performs black hole attack in the network. The malicious node is equipped with energy Eo (1+a) and the normal node is equipped with Eo energy. The network models have a total number of N sensor nodes and from which m times N malicious node and (1-m) times N normal node in the network. Where m is the fraction of malicious node in the network[60].

The number of normal and malicious node in the given network model determined by the

following equations respectively.

$$N_{nrm} = (1-m) \times N \tag{4.15a}$$

$$N_{mal} = m \times N \tag{4.15b}$$

The initial energy level of normal and malicious node in the network receptively.

$$E_{Nnrm} = N_{nrm} \times E_o \tag{4.15c}$$

$$E_{Nmal} = N_{mal} \times E_o(1+a) \tag{4.15d}$$

Total energy of the network is the sum of equation (4.15c and 4.15d)

$$E_{Total} = E_{Nnrm} + E_{Nmal} \tag{4.15e}$$

$$E_{Total} = N_{nrm} \times E_o + N_{mal} \times E_o(1+a) \tag{4.15f}$$

Substitute equation (4.15a and 4.15b) in to equation (4.15e) to get equation (4.15f)and simplified it as follows:

$E_{Total} = (1-m) \times N \times E_o + m \times N \times E_o(1+a)$

$E_{Total} = N \times E_o(1+am)$ "am" more virtual nodes created in the network due to malicious node energy. As shown in equation of $E_{Total} = N \times E_o(1+a \times m)$ this indicates, due to malicious node enhanced with more energy it creates $N \times (1+a \times m)$ virtual nodes that have equal initial energy with normal nodes. "To maintain energy consumption in each round within an epoch, the average number of clusters per round per epoch must be constant and equal" as shown in eq.(**??**) [58, 61]. The weighted probabilities of the heterogeneous network created due to advanced energy of malicious node than a normal node in the network must equal to initial energy of each node divided by initial energy of normal node, so that as those "two-level heterogeneous network is considered in this research we will use modified values of p_{opt}" for normal and malicious nodes of optimal weighted probabilities at each

round, r determined with equations(4.16 and 4.17) respectively.

$$p_{nrm} = \frac{p_{opt}}{1 + a \times m} \tag{4.16}$$

$$p_{mal} = \frac{p_{opt}}{1 + a \times m} \times (1 + a) \tag{4.17}$$

In order to calculate the optimal probabilities of malicious and normal node as shown in equation (4.18) the optimal probability (p_{opt}) in equation (4.10) substitute with the weighted probabilities in equation (4.16 & 4.17), which are the reference probabilities of p_i for malicious and normal node in the sensing area in the case of black hole attack model with energy enhanced sensor node.

b. Probability of Normal and Malicious Node to become CH Based on Residual Energy

The optimal probability of malicious and normal node identified based on the residual energy of sensor node and average residual energy of network denoted with equation (4.18) . The calculated value of p_i used as one of the parameters to calculate the threshold value of malicious and normal node to be cluster head when the network under black hole attack as shown in equation (4.19).

$$p_i = \begin{cases} \frac{p_{opt} E_{i(r)}}{(1+a\times m)\times \overline{E_r}}, & \text{if node i is normal node} \\ \frac{p_{opt}(1+a) E_{i(r)}}{(1+a\times m)\times \overline{E_r}}, & \text{if node i is malicious node} \end{cases} \tag{4.18}$$

Where:-

$Ei(r)$: - The residual energy of sensor node in the network [3, 59, 60]

$\overline{E_r}$:- The average energy of the network at round r [3, 59, 60]

m: - Percentage of malicious nodes in the network

a: - The factor of malicious node advance of a times more energy than normal node

c. Improved LEACH CH Selection Based on Modified Threshold Function

As shown in equation (4.15c and 4.15d) the initial energy of the normal node with E_o and the malicious node with $E_o \times (1 + a)$ energy, which indicates malicious nodes have more energy

than normal nodes in the model. The node that has higher residual energy in each round has more probability to be selected as CH in the network so that in this case the malicious node will have more probability to be selected as CH in the network. To prevent malicious node selected as CH repeatedly in the network, in this paper sensor node behavior based simple attack detection and prevention mechanism enhanced in proposed LEACH routing protocol. The threshold value for CH selection in the proposed routing protocol determined with CH selection algorithm in equation (4.19). In this algorithm the threshold function consider the parameters of the probabilities of malicious and normal node presented in equation(4.18) and distance between sensor node and BS to calculate the threshold value.

$$T_{(n)} = \begin{cases} \frac{p_i}{1-p_i \times \left(r \times mod \frac{1}{p_i}\right)} \times \left| \frac{d_{to}BS_{avg} - d(i,BS))}{d_{to}BS_{avg}} \right|, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{4.19}$$

Where :-

$d_{to}BS_{avg} = \frac{1}{n}\sum_{i=1}^{n} d_{(i,BS)}$

$d_{to}BS_{avg}$:- The average distance between sensor node and BS[47]

$d(i,BS)$:-Distance between the sensor node and BS [47] The distance between each sensor node is calculated with the Euclidean distance formula as shown below. x2,x1, y2, and y1 are the coordinates of X and Y-axis values of two sensor nodes in the network.

$d(i,BS) = \sqrt{(x2-x1)^2 + (y2-y1)^2}$

4.5 Black Hole Attack Detection and Prevention Algorithms

The black hole attack detection and prevention mechanism in this thesis is designed based on the behavior of sensor nodes on the residual energy level of the sensor node at each round that participates in CH selection in the network. If the residual energy level of each node in each round in the network is much greater than the average residual energy of the network considered a malicious node (back hole attack) with this algorithm. Then black hole attack detection and prevention algorithm exclude these malicious sensor nodes from CH selection, data reception, and transmission process. This algorithm is applied after the threshold value for CH selection determined with equation (4.14 and 4.19) in the case of the network under black hole attack. The black hole attack model with initially all sensor nodes equipped with similar energy levels and some sensor nodes enhanced with more energy which is simulated in scenario 1 and scenario 2 in chapter 5 respectively.

Chapter 5

Performance Evaluation and Analysis of Proposed Routing Protocol Result

5.1 Simulation Parameters

The proposed routing protocol network model parameters used for simulation with MATLAB are adopted from [2, 62] described in table 5.1. In this simulation from 100 sensor nodes, 10 of them have been considered to perform the malicious attack. The sensor node used in this simulation has a frequency of 914 k. Hz and a bit rate of 1Mbps [63].

5.2 Proposed LEACH Protocol Performance Metrics

In this paper, the performance of the proposed LEACH routing protocol is evaluated with the number of packets received at the base station, network lifetime (the first node dies, half of the node dies, and the last node dies or 90%), residual energy, and throughput. Using these system performance metrics, we evaluate the experimental result of the energy efficiency and security of the proposed routing protocol.

Number of packet received at base station: This will measure the total number of packet which are sent from CH to base stations(BS) [2] or packet received by BS

Network lifetime: This is the time interval between network operation start until the death of

Table 5.1: Simulation Parameters

Network surface(List of Parameters)	**Value**
Node Deployment Area (MxM)	$100 \times 100m^2$
BS location	Center ($0.5X_m$, $0.5Y_m$)
Total number of nodes	100
Sensor node initial energy	0.5J
Size of data packet	4000bits
Transmission /reception energy (ET_x/ER_x)	$5 \times 10^{-}9J$
Energy consumed by the amplifier to transmit at shorter distance ($d < d_o$) or free space signal ($\in_{fs}$)	$10 \times 10^{-}12J/bit/m^2$
Energy consumed by the amplifier to transmit at longer distance ($d > d_o$) or free space signal ($\in_{amp}$)	$0.003 \times 10^{-}12J/bit/m^4$
Aggregation Energy(E_{DA})	5nJ/bit/message
Routing protocol	LEACH
Number of Round	5000
Node Distribution	Randomly and uniformly distributed

the last node in WSN. Network lifetime is measured in terms of the number of rounds(time) which First Node Dies (FND), Half of Nodes Dies (HND), and Last Node Dies (LND) or 90 % node Dies.

- *First Node Dies*: Is the time interval from starting until the first sensor node runs out of energy in the WSN it also known as stability period[2, 11].
- *Half Nodes Dies* : The time or round in which half of the nodes in WSN out of energy
- *Last Node Dies*: The time or round in which all sensor nodes in WSN out of energy

Remaining energy: is defined as the residual energy of the sensor node in the network in each round after receiving and sending data to the base station[13].

Throughput : Throughput in the cluster-based routing protocol is defined as the sum of packets transmitted to the CH and base station over the network within the given time period or round.

5.3 Simulation Results and Discussion

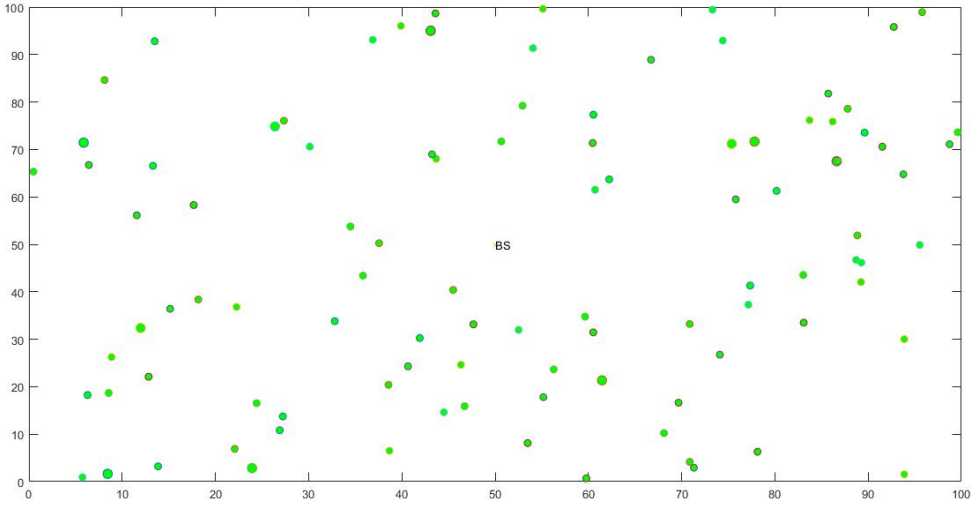
In this paper, simulation of the proposed routing protocol is done with two scenarios with and without a black hole attack. The first scenario experiment using a homogeneous sensor node in the network. In this scenario, the proposed LEACH routing protocol, cluster head(CH) selection algorithms consider the parameters of sensor node residual energy, average network energy, and distance between the sensor node and BS. The second scenario experiment is similar to the first scenario except energy enhanced sensor node used for the black hole attack model. In the first scenario, all malicious and normal sensor nodes have equal energy levels at the initial. But in the second scenario 10% of sensor nodes from a total number of nodes in the network are enhanced with more energy, and these sensor nodes perform the malicious activity in the network.

5.3.1 Random distribution of sensor node in simulation environment

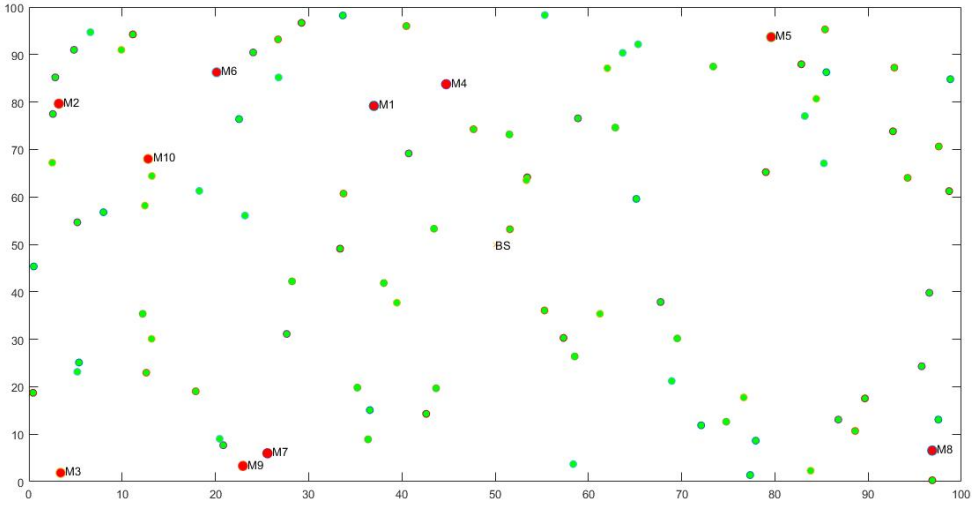
Figure (5.1a,5.1b and 5.1c) shows the random distribution of sensor node with and without malicious node and also cluster head distribution in the simulation area. The red circle in figure (5.1b and 5.1c) shows 10 % of malicious node distribution in the simulation area.

5.3.2 Scenario 1: Simulation result of malicious and normal node with similar energy level in network model

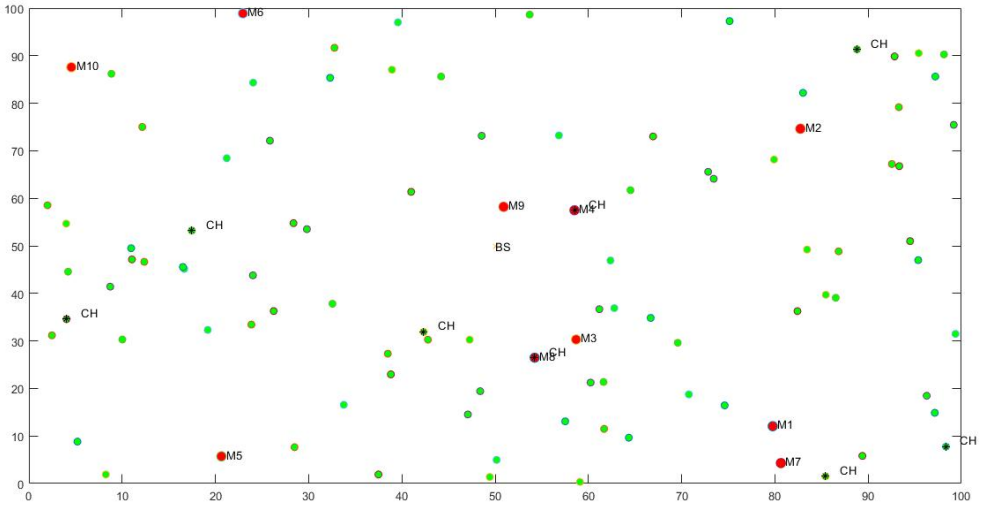
The sensor node for the black hole attack model in this scenario has a similar energy level to the non-malicious sensor node in the network model. The proposed LEACH routing simulated with Matlab and simulation result was evaluated and analyzed with the performance metrics mentioned in section 5.2.



(a) All sensor node random distribution in the network simulation area



(b) Malicious and normal node random distribution in the network simulation area



(c) Network simulation area after cluster formation

Figure 5.1: Random distribution of sensor node in simulation environment

The Proposed LEACH is the modified LEACH based on its energy efficiency and security during the CH selection and data transmissions on WSN routing protocol as discussed in chapter 4 at section 4.4.1.1. This protocol simulated with and without black hole attack and enhanced security mechanism to black hole attack detection and prevention in the proposed routing protocol. ES-LEACH, ES-LEACH under BHA, Secure ES-LEACH from BHA used to represent proposed LEACH for network model without black hole attack, network model under black hole attack, and security mechanisms enhanced for network model under black hole attack respectively for scenario1.

a) **Number of packet received at base station**

i. *LEACH vs LEAH Under Black Hole Attack and Secure LEACH*

The number of a packet sent to BS with LEACH and Secure LEACH routing protocol from black hole attack has a better result than LEACH under black hole attack as shown in figure (5.2). LEACH routing protocol is used as a base reference to evaluate the proposed routing protocol performance.

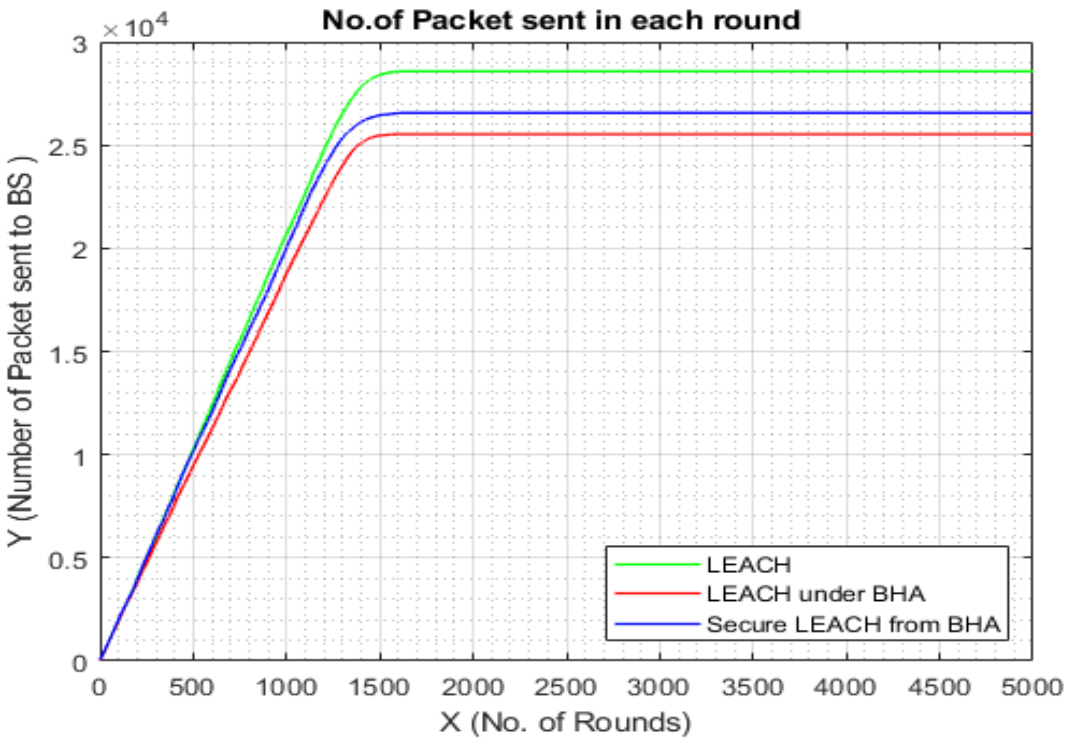


Figure 5.2: LEACH without and with black hole attack and Secure LEACH from black hole attack

ii. *Proposed LEACH vs LEACH*

The simulation result shows in figure (5.3), in the cases of a number of packets sent to BS, the proposed routing protocol performs more compared to LEACH with black and without black hole attack. In a cluster-based routing protocol, the number of CH selected in each round is very much, the energy consumption due to data aggregation and communication with BS is also high, it creates excessive loads in the network and the network lifetimes become short and the number of packets sent to BS is reduced parallelly with the network lifetime. So that, selecting the optimal number of CH in each round in WSN is one of the possible ways to reduce the energy consumption of WSN. Reducing the energy consumption in the network means extending the network lifetime and increasing the number of packets sent to BS of the network. As shown in figure (5.3), the proposed routing protocol implements an optimal number of CH selection mechanisms that improve the number of packets sent to BS by 237.65% compared with the LEACH routing protocol. And also, the number of packets sent to BS with the proposed routing protocol under black hole attack improved by 1.88% compared to the proposed routing protocol enhanced with black hole attack detection and prevention algorithm. This result illustrates that the proposed routing protocol performs its task effectively.

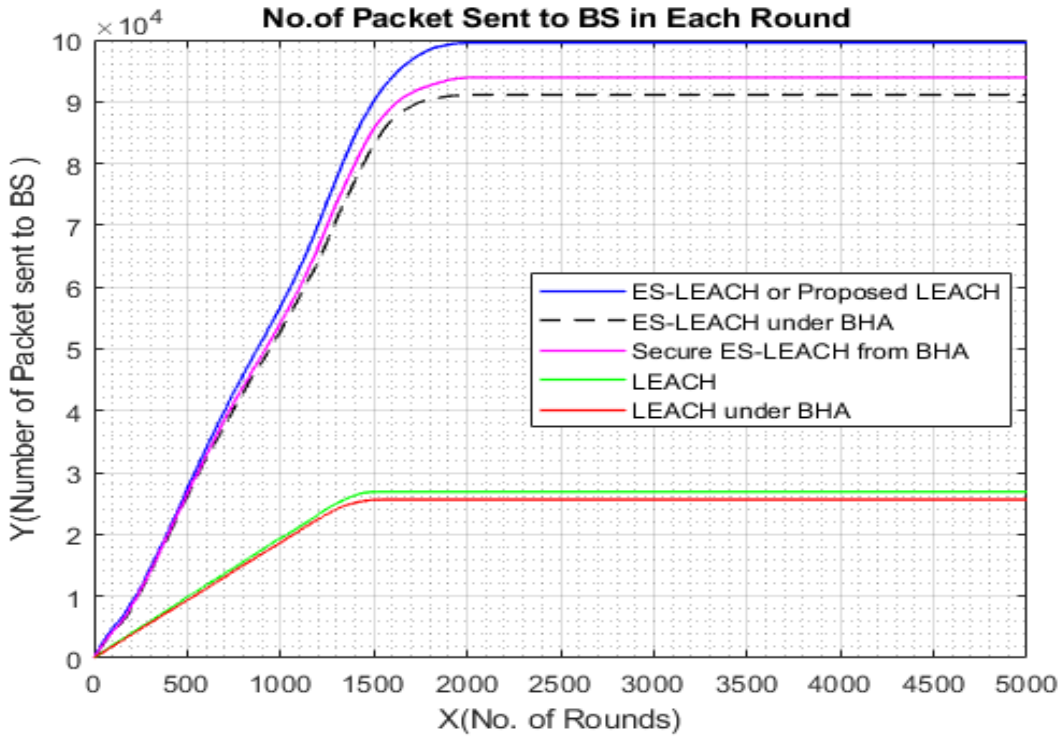


Figure 5.3: Comparison of proposed LEACH with all sensor nodes have equal initial energy level and LEACH with and without BHA packet sent to BS

b) **Network lifetime**

In this thesis, the network lifetime is evaluated in terms of the number of rounds in which the first node is dead, half node dead, and 90% node dead in the network. The simulation result in figure (5.5) shows that proposed LEACH without BHA dead around 1825 round but in original LEACH 90% sensor node dead around 1421 round, which indicates the proposed LEACH improves the network lifetime by 28.43%. This result indicates that the proposed routing protocol extends the network lifetime compared to LEACH. If sensor nodes exist in life in the network for more rounds, the network lifetime becomes longer and can send more packets to BS. In Figure(5.5), we will see the number of alive sensor nodes in the LEACH routing protocol and proposed LEACH routing protocol at different rounds.

i. *LEACH vs LEAH Under Black Hole Attack and Secure LEACH*

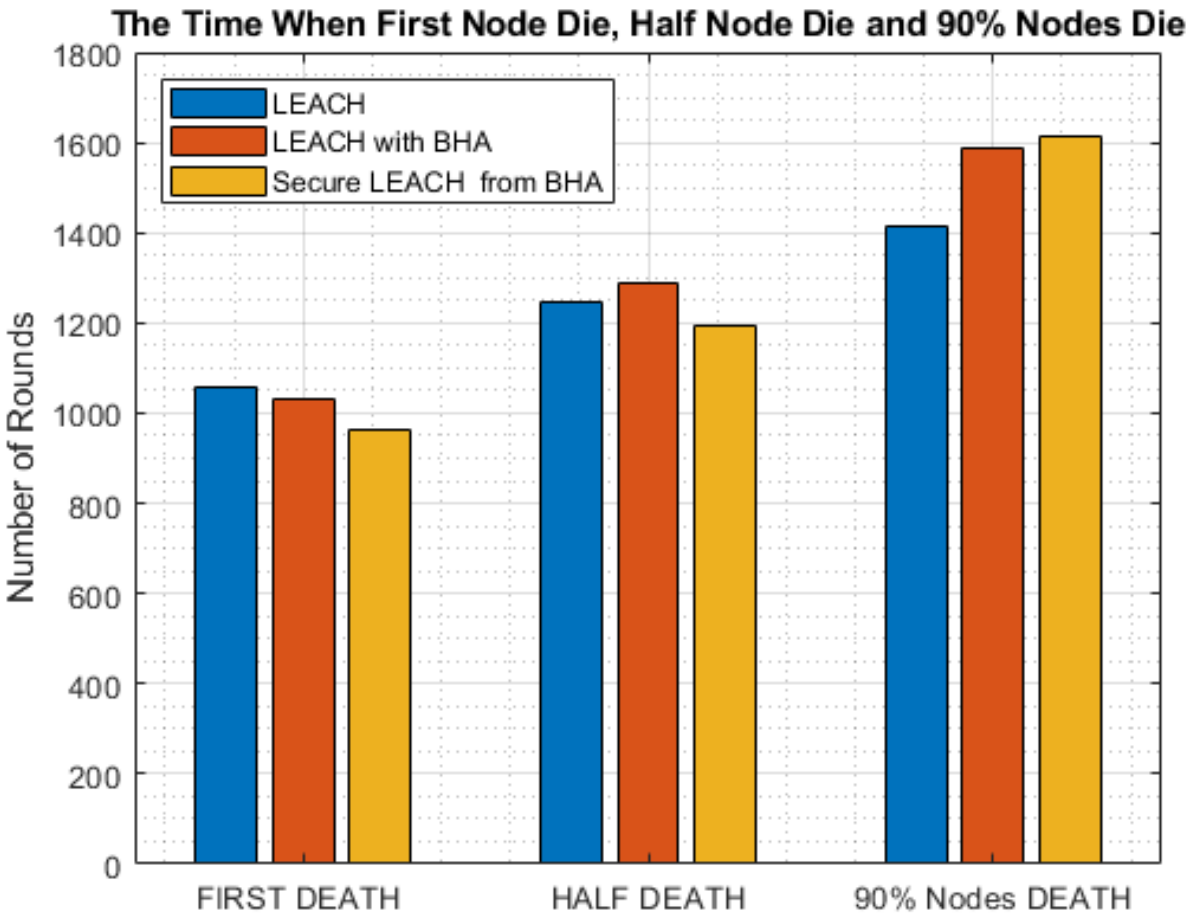


Figure 5.4: LEACH without and with black hole attack and Secure LEACH from black hole attack

ii. *Proposed LEACH Vs LEACH*

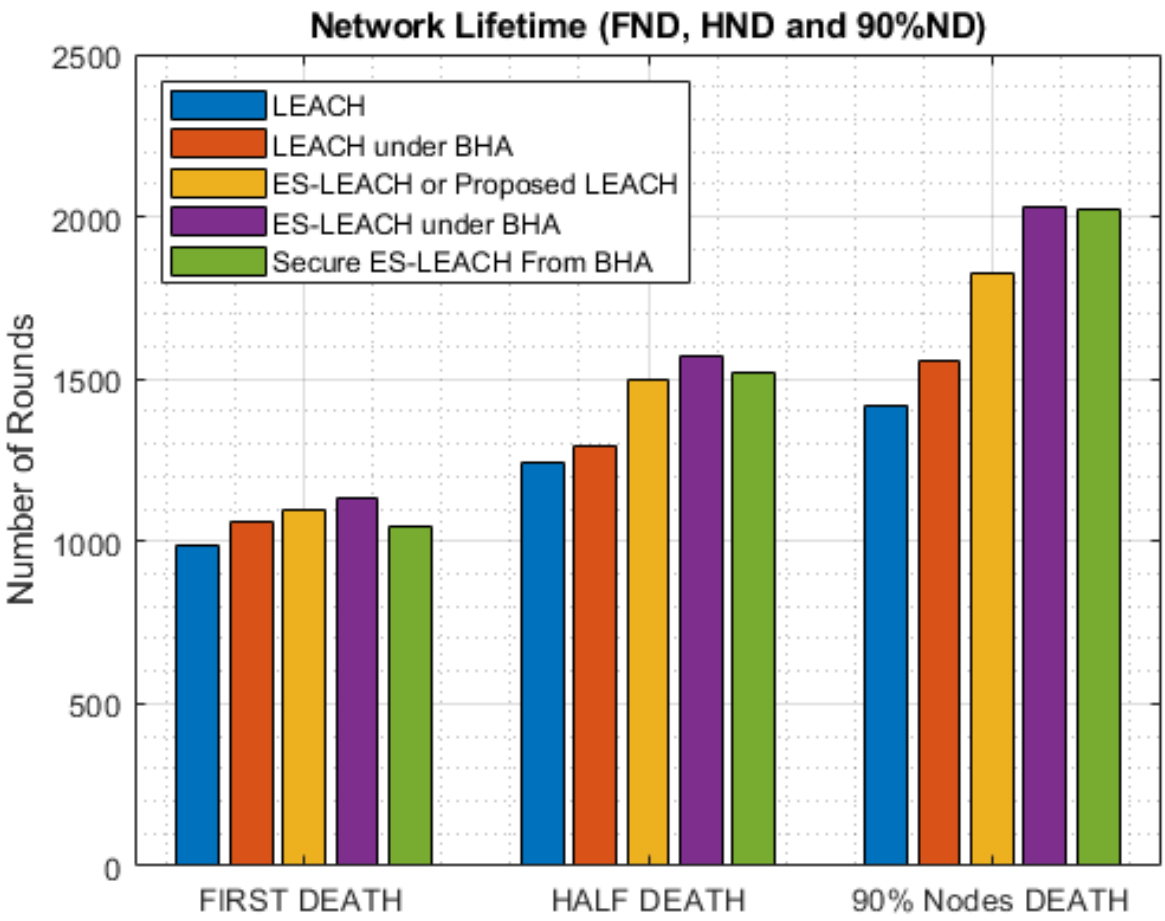


Figure 5.5: Network lifetime comparison of proposed LEACH and LEACH without and with black hole attack and Secure LEACH from black hole attack

c) **Remaining energy**

As shown in figure(5.7) round vs residual energy graph proposed LEACH(ES-LEACH) has more residual energy compared to LEACH routing protocol. Half of the network energy dissipated at rounds 805 and 624 for proposed LEACH(blue color) and LEACH(green color), which indicates the proposed LEACH improves energy efficiency by 29%. The residual energy of the network becomes 0 in LEACH at rounds 1396 and 1880 in the proposed LEACH, which is a 34.67% improvement. This result shows that the proposed LEACH is more energy-efficient than LEACH. In addition to this, the residual energy of proposed LEACH under black hole attack and after enhanced with security mechanisms have more residual energy compared to LEACH and proposed LEACH. The reason for having more residual energy in the network is the malicious sensor node or node under black hole attack

does not dissipate energy for data transmission to CH or BS. The presence of more residual energy in proposed LEACH indicates that the proposed LEACH extends the network lifetime more.

i. *LEACH vs LEAH Under Black Hole Attack and Secure LEACH*

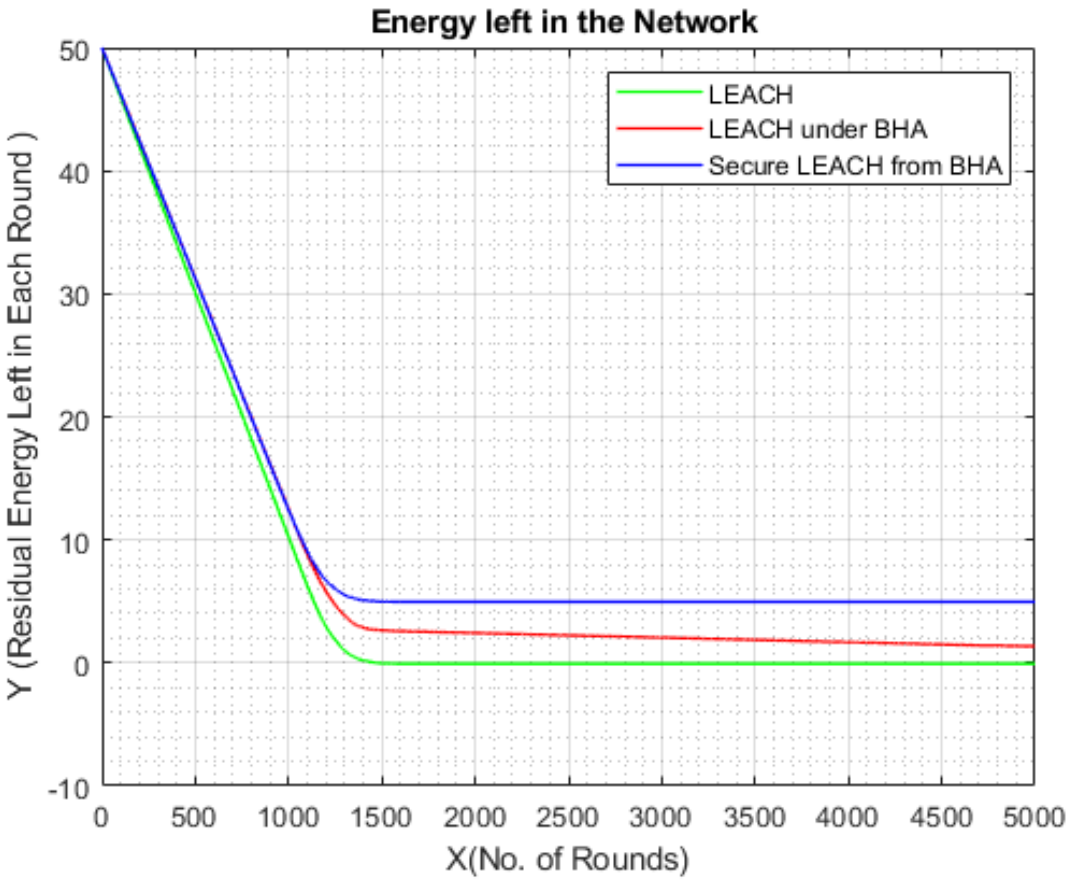


Figure 5.6: LEACH without and with black hole attack and Secure LEACH from black hole attack residual energy per round

ii. *Proposed LEACH vs LEACH*

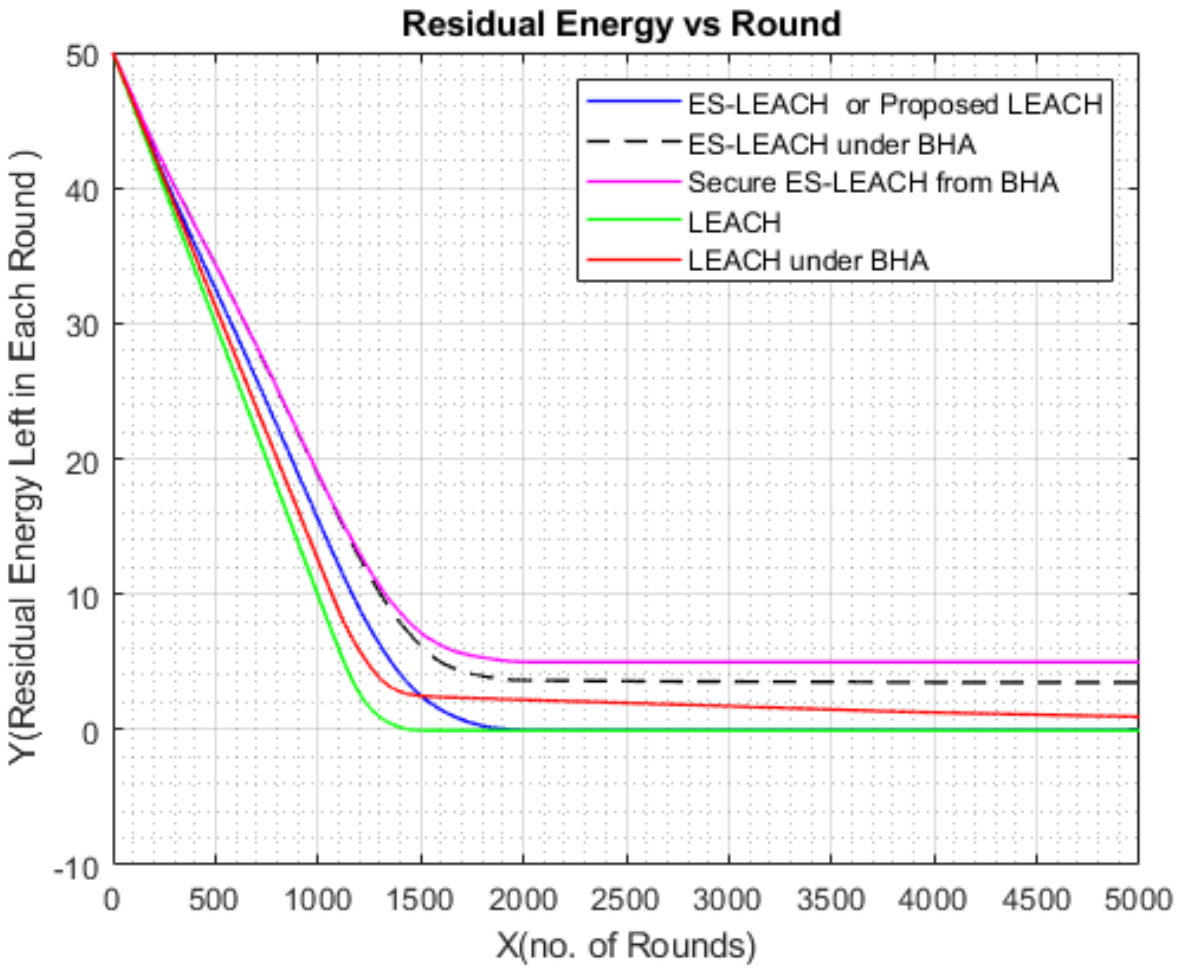


Figure 5.7: proposed LEACH and LEACH without and with black hole attack and Secure LEACH from black hole attack residual energy per round

d) **Throughput**

In figure (5.8), the throughput graph shows that the proposed LEACH protocol under black hole attack and enhanced with security mechanisms have better results in comparison with LEACH protocol. Improvement of throughput in proposed LEACH due to proposed LEACH use energy in the network efficiently and have more residual energy than LEACH. Network lifetime and the number of packets sent to CH and BS throughout the network lifetime are directly related to residual energy in the network. The network has more residual energy then, the network can send more packets in the network shown in figure (5.8).The network has more residual energy then, the network can send more packets in the network shown in

figure (5.8). Around round 3500, the proposed LEACH improves the throughputs of the network by 21.676% compared to the LEACH routing protocol. *Proposed LEACH vs LEACH*

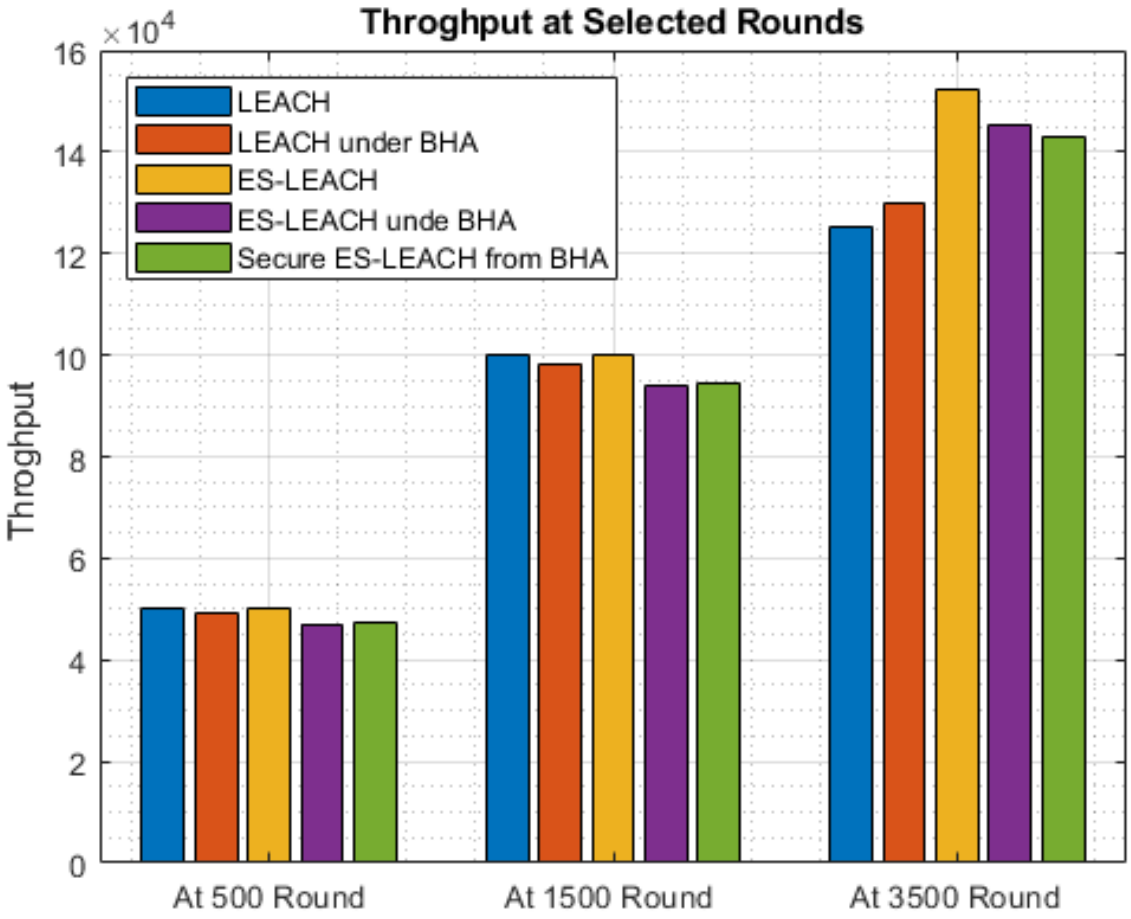


Figure 5.8: Proposed LEACH and LEACH without and with black hole attack and Secure LEACH from black hole attack throughput per round

5.3.3 Scenario 2: Simulation Result of Network Model under Energy Enhanced Malicious Node

In this scenario, the proposed LEACH routing model presented in chapter 4 at section 4.4.1.2. simulated with and without black hole attacks in the network. ES-LEACH-ESN, ES-LEACH-ESN under BHA, and Secure ES-LEACH-ESN from BHA were used to represent the graph of proposed LEACH for network model without black hole attack, network model under black hole attack, and security mechanisms enhanced for network model under black hole attack respectively for scenario 2. The attack model in this scenario contains a malicious node enhanced with more energy than a normal sensor node in the network. In this scenario performance of the proposed system is evaluated with the following performance metrics.

a) **Number of packet received at base station**

The simulation result in figure (5.9) shows the proposed LEACH routing protocol with black hole attack and enhanced with security mechanisms perform better than LEACH and DEEC routing protocol on the number of packets sent to BS. In the proposed LEACH routing protocol number of CH fluctuation or variation in each round is very less than LEACH and DEEC routing protocol. If the fluctuation of CH in the network is stable the network routing protocols transmit more data properly to BS as shown in the proposed LEACH in figure (5.9).

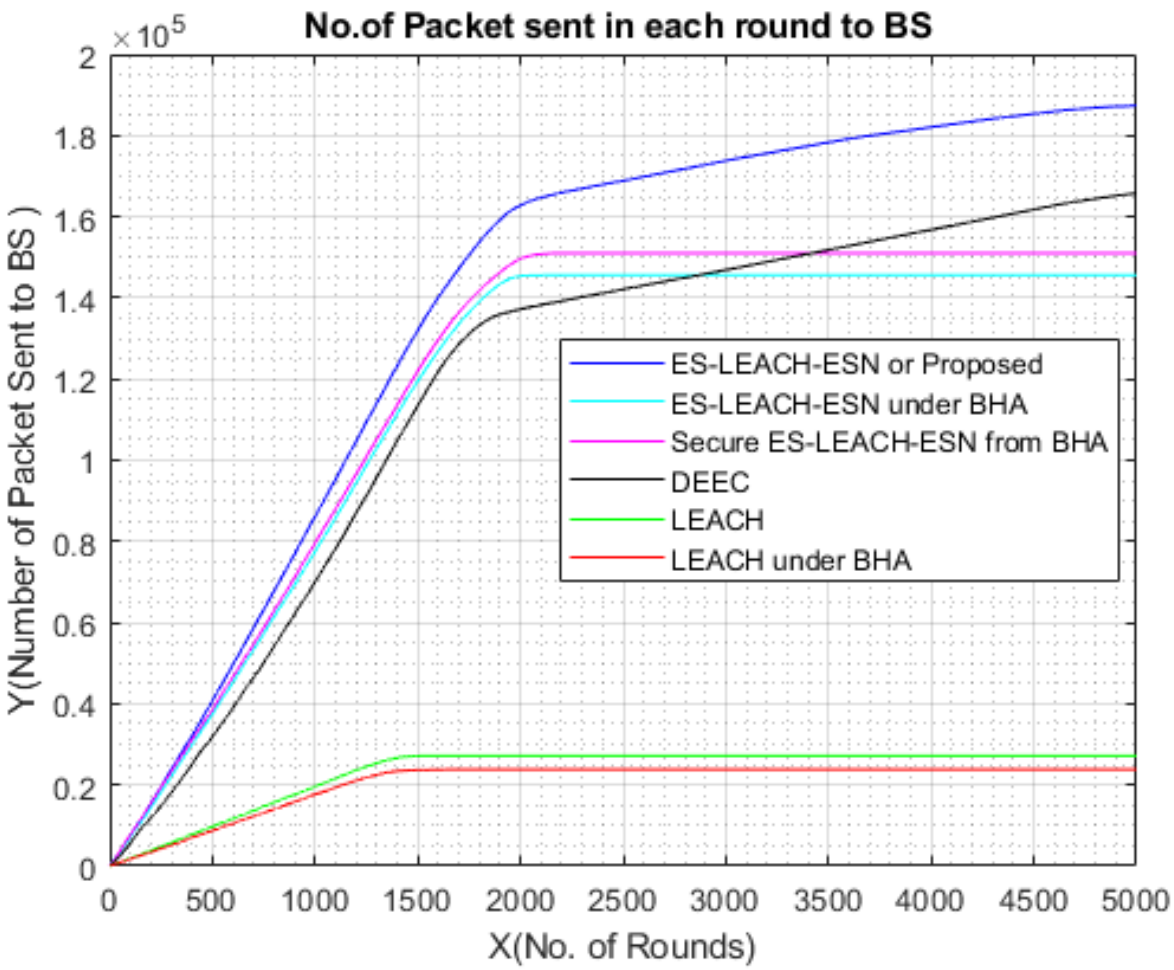


Figure 5.9: Proposed LEACH with energy enhanced sensor node and LEACH with and without BHA packet transmission to BS per round comparison with related protocols

b) **Network lifetime**

The network lifetime in WSN has been measured in terms of the sensor nodes that exist alive for each round. The simulation result in figure(5.10) shows that the proposed LEACH with energy enhanced sensor nodes has more lifespan than the LEACH routing protocol. As shown in figure (5.10), the number of rounds that sensor nodes died extends in the case of proposed LEACH compared to LEACH and DEEC.

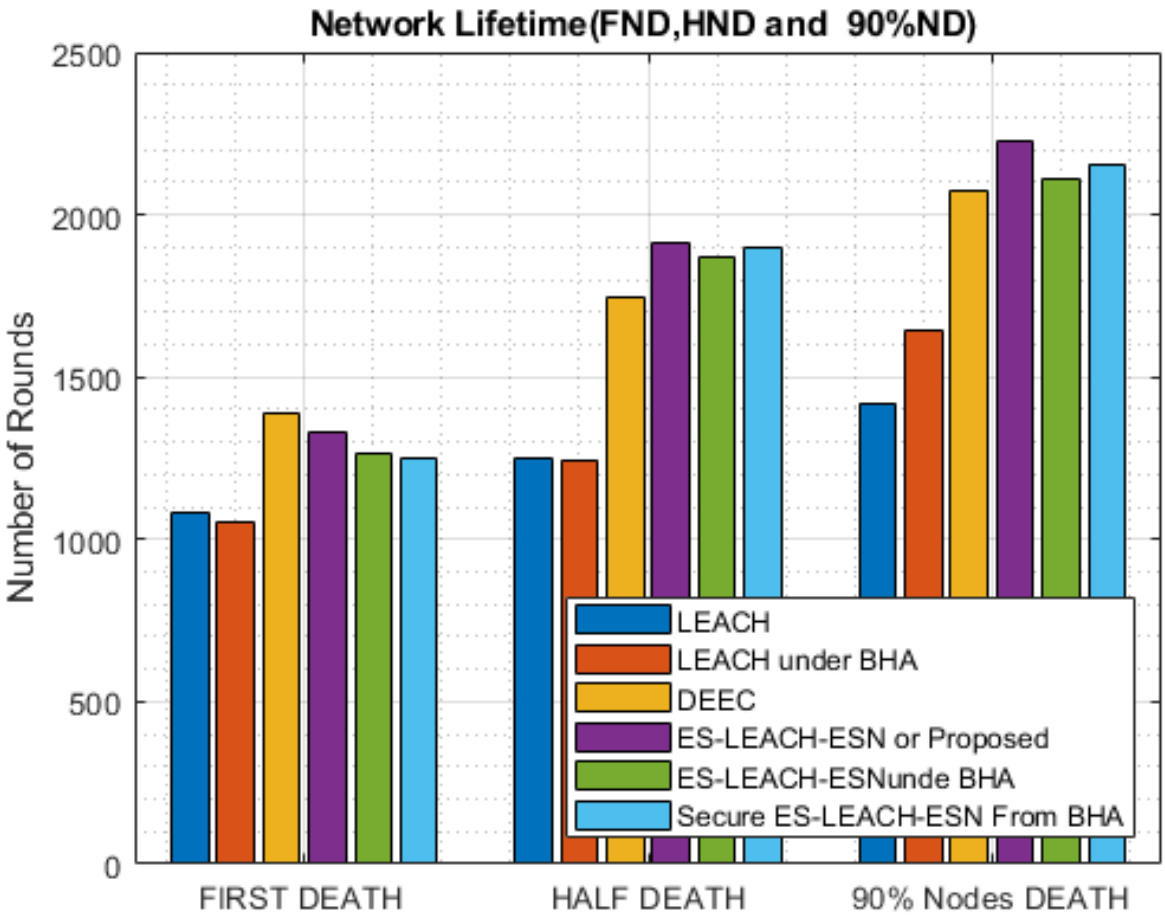


Figure 5.10: Proposed LEACH with energy enhanced sensor node and LEACH with and without BHA Network Lifetime

c) **Remaining energy**

In figure (5.11), the simulation result shows that the remaining energy of proposed LEACH with and without black hole attack has more residual energy level than LEACH and DEEC routing protocol in each round. This result shows that by improving energy utilization and security of the LEACH routing protocol, we can extend the network lifetime of WSN as a whole.

d) **Throughput**

Proposed LEACH has more residual energy and is secure from black hole attacks. Due to energy-efficient utilization and security solution within the proposed LEACH has been able to produce more throughput than LEACH and DEEC, as we can see in figure(5.12.

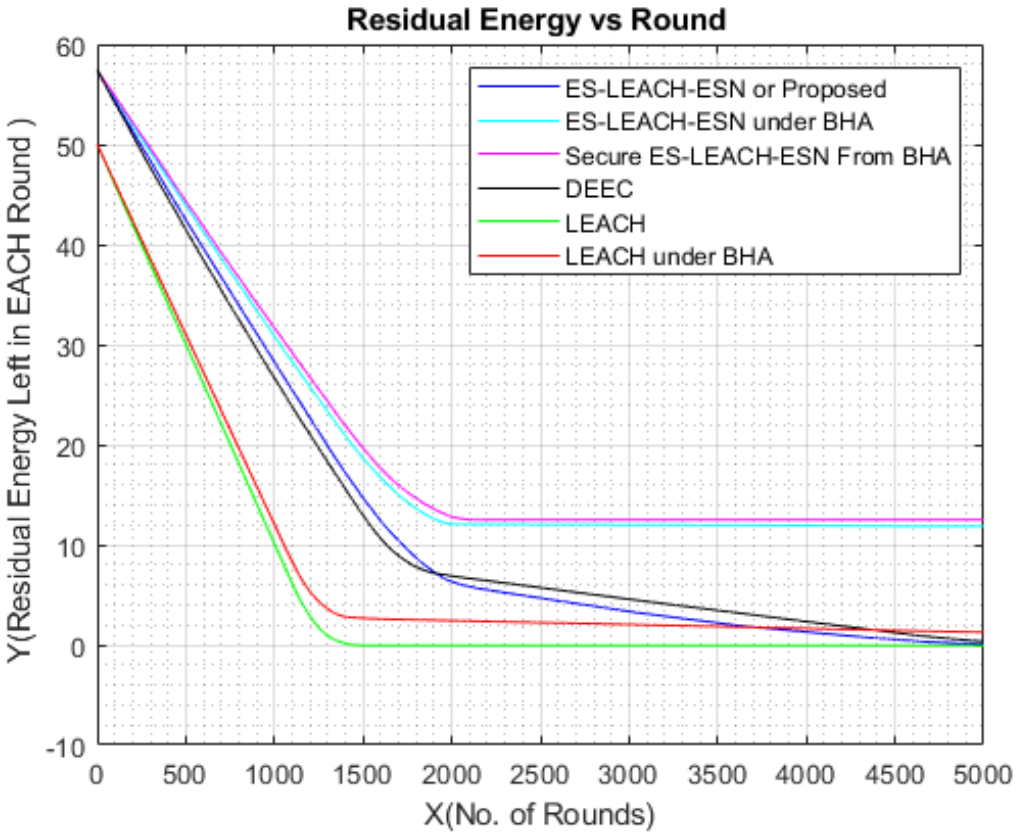


Figure 5.11: Proposed LEACH with energy enhanced sensor node and LEACH with and without BHA residual energy per each round

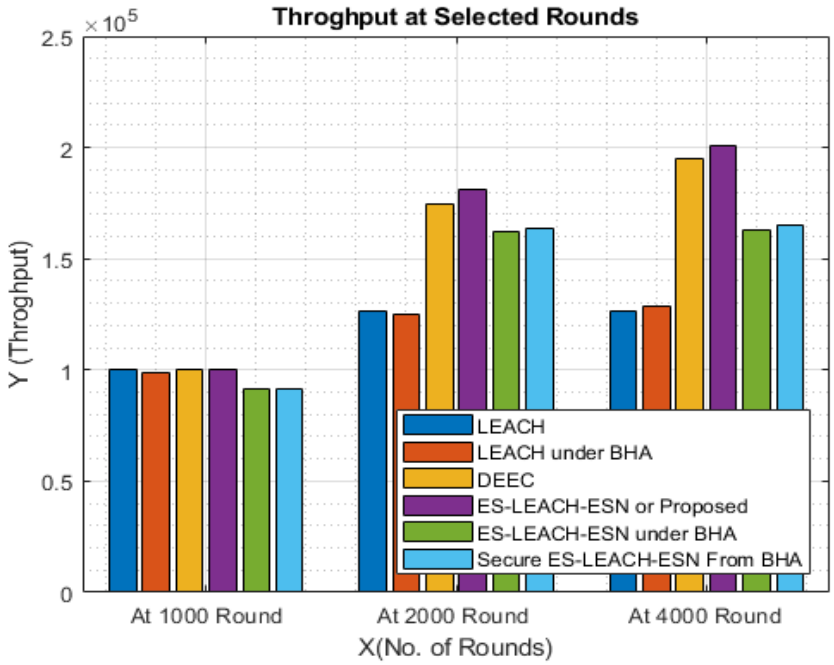


Figure 5.12: Proposed LEACH with energy enhanced sensor node and LEACH with and without BHA throughput per each round

Chapter 6

Conclusion and Future Recommendation

This paper presents an energy-efficient and secure LEACH routing protocol against black hole attacks for WSN. The energy inefficiency issue of the LEACH routing protocol handle by modifying the threshold function equation parameters for the CH selection algorithm. Those parameters are residual energy of sensor node in the network, average network energy, and distance between cluster head candidate node and base station (BS). On the other hand, the malicious node selected as CH in the network was detected and prevented using the sensor node behaviors in the network. Generally, the proposed routing protocol in this paper reduces the energy utilization and probability of malicious node selected as CH that performs black hole attack in LEACH for WSN. The proposed routing protocol with a homogeneous network model improves the LEACH routing by an average of 34.67%, 28.43% 237.65%, and 21.676% in terms of residual energy, network lifetime, packets sent to BS, and throughputs respectively. Proposed LEACH enhanced with black hole attack detection and prevention mechanism improves the proposed LEACH under black hole attack by 1.88% in terms of the number of packets sent to BS. The security mechanism implemented in this paper focused on improving the data availability.

Finally, the simulation result shown in both scenarios in this thesis reducing energy utilization and increasing residual energy, increase the number of packets sent to BS, throughput, network lifetime of WSN by improving cluster head selection algorithms in terms of energy

efficiency and security. In future work, extend the proposed protocol in the case of multi hope LEACH routing and improving the attack model to more than one type and its prevention mechanisms.

References

[1] Bhakti Parmar, Jayesh Munjani, Jemish Meisuria, and Ajay Singh. A survey of routing protocol leach for wsn. *International Journal of Scientific and Research Publications*, 4 (1), 2014.

[2] Rania Khadim, Abdelhakim Maaden, Ansam Ennaciri, and Mohammed Erritali. An energy-efficient clustering algorithm for wsn based on cluster head selection optimization to prolong network lifetime. *International Journal of Future Computer and Communication*, 7(3), 2018.

[3] Meenakshi Tripathi, Manoj Singh Gaur, and Vijay Laxmi. Comparing the impact of black hole and gray hole attack on leach in wsn. *Procedia Computer Science*, 19:1101–1107, 2013.

[4] Manish M Patel and Priyanka K Patel. Intrusion detection system based on trust value in wireless sensor networks. In *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, pages 618–620. IEEE, 2019.

[5] Huisheng Gao, Ruping Wu, Mingjing Cao, and Can Zhang. Detection and defense technology of blackhole attacks in wireless sensor network. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 601–610. Springer, 2014.

[6] Mohammad Wazid, Avita Katal, Roshan Singh Sachan, RH Goudar, and DP Singh. Detection and prevention mechanism for blackhole attack in wireless sensor network. In *2013 International Conference on Communication and Signal Processing*, pages 576–581. IEEE, 2013.

[7] Abhinav Kaurav and Kakelli Anil Kumar. Detection and prevention of black hole attack in wireless sensor network using ns-2.35 simulator. *IJSR CSEIT*, 2(3):717–722, 2017.

[8] Sunil Kumar Singh, Prabhat Kumar, and Jyoti Prakash Singh. A survey on successors of leach protocol. *Ieee Access*, 5:4298–4328, 2017.

[9] Zuo Chen, Min He, Wei Liang, and Kai Chen. Trust-aware and low energy consumption security topology protocol of wireless sensor network. *Journal of Sensors*, 2015, 2015.

[10] Amjad Mehmood, Jaime Lloret, and Sandra Sendra. A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring. *Wireless Communications and Mobile Computing*, 16(17):2869–2883, 2016.

[11] Amine Kardi and Rachid Zagrouba. Attacks classification and security mechanisms in wireless sensor networks. *Advances in Science, Technology and Engineering Systems Journal*, 4(6):229–243, 2019.

[12] Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian. Leach-based security routing protocol for wsns. In *Advances in Computer Science and Information Engineering*, pages 253–258. Springer, 2012.

[13] Vishali Bansal and Krishan Kumar Saluja. Anomaly based detection of black hole attack on leach protocol in wsn. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pages 1924–1928. IEEE, 2016.

[14] Nongmaithem Island Devi and Rajeev Kumar Patial. *Black Hole Attack Detection on Leach Protocol in WSN*. PhD thesis, Lovely Professional University, 2017.

[15] Naveen Kumar and Jasbir Kaur. Improved leach protocol for wireless sensor networks. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–5. IEEE, 2011.

[16] Ahmed Saidi and Khelifa benahmed Pr. Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks. *Ad Hoc Networks*, page 102215, 2020.

[17] Dionisis Kandris, Christos Nakas, Dimitrios Vomvas, and Grigorios Koulouras. Applications of wireless sensor networks: an up-to-date survey. *Applied System Innovation*, 3(1): 14, 2020.

[18] Mohamed Boukhani and Abderrahmane Hajraoui. Security in wireless sensor networks communication protocols: challenges and solutions. 2018.

[19] Ivana Tomić and Julie A McCann. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal*, 4(6):1910–1923, 2017.

[20] Vikash Kumar, Anshu Jain, PN Barwal, et al. Wireless sensor networks: security issues, challenges and solutions. *International Journal of Information and Computation Technology (IJICT)*, 4(8):859–868, 2014.

[21] Mahmood Ali and Ravula Sai Kumar. Real-time support and energy efficiency in wireless sensor networks, 2008.

[22] Rashim Rana Er Anoopa Arya. A survey on secure and energy efficient leach protocol. 2016.

[23] Hassan Oudani, Salah-Ddine Krit, Lahoucine El Maimouni, and Jalal Laassiri. Energy consumption in wireless sensor network: Simulation and compartative study of flat and hierarchical routing protocols. *IADIS International Journal on Computer Science & Information Systems*, 12(1), 2017.

[24] Prachi Dewal, Gagandeep Singh Narula, and Vishal Jain. Detection and prevention of black hole attacks in cluster based wireless sensor networks. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 3399–3403. IEEE, 2016.

[25] Mervat Mustafa Raouf. Clustering in wireless sensor networks (wsns). *Journal of Baghdad University College of economic sciences*, 57:01–09, 2019.

[26] Khalid MO Nahar, Ra'ed M Al-Khatib, Malek Barhoush, and Alfian Abdul Halin. Mpf-leach: modified probability function for cluster head election in leach protocol. *International Journal of Computer Applications in Technology*, 60(3):267–280, 2019.

[27] Arvind Kumar et al. *Energy efficient clustering algorithm for wireless sensor network*. PhD thesis, Lovely Professional University, 2017.

[28] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd annual Hawaii international conference on system sciences*, pages 10–pp. IEEE, 2000.

[29] Reshma I Tandel. Leach protocol in wireless sensor network: a survey. *International Journal of Computer Science and Information Technologies*, 7(4):1894–1896, 2016.

[30] Li Tian, Huaichang Du, and Yanwei Huang. The simulation and analysis of leach protocol for wireless sensor network based on ns2. In *2012 International Conference on System Science and Engineering (ICSSE)*, pages 530–533. IEEE, 2012.

[31] K Ramesh and Dr K Somasundaram. A comparative study of clusterhead selection algorithms in wireless sensor networks. *arXiv preprint arXiv:1205.1673*, 2012.

[32] Ms Neha Bhadu and Uma Kumari. Leach: Energy efficient routing protocol for wsns along with its enhancements. 2016.

[33] Siddiq Iqbal, SP Aravind Srinivas, G Sudharsan, and Sagar S Kashyap. Comparison of different attacks on leach protocol in wsn. *International Journal of Electrical, Electronics and Data Communication*, 8(8):16–19, 2014.

[34] Muneer Bani Yassein, Shadi Aljawarneh, and Rasha K Al-huthaifi. Enhancements of leach protocol: Security and open issues. In *2017 International Conference on Engineering and Technology (ICET)*, pages 1–8. IEEE, 2017.

[35] Shweta Varshney and Rakesh Kuma. Variants of leach routing protocol in wsn: A comparative analysis. In *2018 8th International conference on cloud computing, data science & engineering (confluence)*, pages 199–204. IEEE, 2018.

[36] M Bani Yassein, Yaser Khamayseh, and Wail Mardini. Improvement on leach protocol of wireless sensor network (vleach. In *Int. J. Digit. Content Technol. Appl. 2009*. Citeseer, 2009.

[37] Md Solaiman Ali, Tanay Dey, and Rahul Biswas. Aleach: Advanced leach routing protocol for wireless microsensor networks. In *2008 International Conference on Electrical and Computer Engineering*, pages 909–914. IEEE, 2008.

[38] Haibo Liang, Shuo Yang, Li Li, and Jianchong Gao. Research on routing optimization of wsns based on improved leach protocol. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):194, 2019.

[39] Semanti Das and Abhijit Das. An algorithm to detect malicious nodes in wireless sensor network using enhanced leach protocol. In *2015 International Conference on Advances in Computer Engineering and Applications*, pages 875–881. IEEE, 2015.

[40] Nihar Roy and Pravin Chandra. Energy efficient positioning of base station in clustered wsn. *Available at SSRN 3446675*, 2019.

[41] Salahddine Krit Hassan Oudani, Mustapha Kabrane, Kaoutar Bandaoud, Mohamed Elaskri, Khaoula Karimi, Hicham Elbousty, and Lahoucine Elmaimouni. Energy efficient in wireless sensor networks using cluster-based approach routing. *International Journal of Sensors and Sensor Networks*, 5(5-1):6–12, 2017.

[42] Padmalaya Nayak, V Bhavani, and B Lavanya. Impact of black hole and sink hole attacks on routing protocols for wsn. *International Journal of Computer Applications*, 116(4), 2015.

[43] Gurjinder Kaur, VK Jain, and Yogesh Chaba. Detection and prevention of blackhole attacks in wireless sensor networks. In *International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, pages 118–126. Springer, 2017.

[44] Samir Athmani, Djallel Eddine Boubiche, and Azeddine Bilami. Hierarchical energy efficient intrusion detection system for black hole attacks in wsns. In *2013 World Congress on Computer and Information Technology (WCCIT)*, pages 1–5. IEEE, 2013.

[45] Muneer Alshowkan, Khaled Elleithy, and Hussain AlHassan. Ls-leach: a new secure and energy efficient routing protocol for wireless sensor networks. In *2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications*, pages 215–220. IEEE, 2013.

[46] A Krishnakumar and V Anuratha. An energy-efficient cluster head selection of leach protocol for wireless sensor networks. In *2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)*, pages 57–61. IEEE, 2017.

[47] Tri Gia Nguyen, Chakchai So-In, and Nhu Gia Nguyen. Two energy-efficient cluster head selection techniques based on distance for wireless sensor networks. In *2014 International Computer Science and Engineering Conference (ICSEC)*, pages 33–38. IEEE, 2014.

[48] Rohini Sharma, Narendra Mishra, and Sumit Srivastava. A proposed energy efficient distance based cluster head (dbch) algorithm: An improvement over leach. *Procedia Computer Science*, 57(807-814):28, 2015.

[49] Wided Abidi and Tahar Ezzedine. New approach for selecting cluster head based on leach protocol for wireless sensor networks. In *International Conference on Evaluation of Novel Approaches to Software Engineering*, volume 2, pages 114–120. SCITEPRESS, 2017.

[50] Surender Kumar, Manish Prateek, Neelu Jyothi Ahuja, and Bharat Bhushan. De-leach: Distance and energy aware leach. *arXiv preprint arXiv:1408.2914*, 2014.

[51] WooSuk LEE, Kye-Dong Jung, and Jong-Yong Lee. Improvement of cluster head selection of leach protocol. *International Journal of Applied Engineering Research*, 12(20): 10002–10006, 2017.

[52] Trupti Mayee Behera, Sushanta Kumar Mohapatra, Umesh Chandra Samal, Mohammad S Khan, Mahmoud Daneshmand, and Amir H Gandomi. Residual energy-based cluster-head selection in wsns for iot application. *IEEE Internet of Things Journal*, 6(3):5132–5139, 2019.

[53] Khalid A Darabkh and Jumana N Zomot. An improved cluster head selection algorithm for wireless sensor networks. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 65–70. IEEE, 2018.

[54] Fang Zhu and Junfang Wei. An energy-efficient unequal clustering routing protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks*, 15(9): 1550147719879384, 2019.

[55] Ch Usha Kumari and M Ramya Krishna. High performance wireless communication channel using leach protocols. *Pak. J. Biotechnol*, 13:52–56.

[56] Wendi B Heinzelman, Anantha P Chandrakasan, and Hari Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on wireless communications*, 1(4):660–670, 2002.

[57] Rohit D Gawade and Sanjay L Nalbalwar. A centralized energy efficient distance based routing protocol for wireless sensor networks. *Journal of Sensors*, 2016, 2016.

[58] Guijun Chen, Xueying Zhang, Jun Yu, and Maofeng Wang. An improved leach algorithm based on heterogeneous energy of nodes in wireless sensor networks. In *2012 International Conference on Computing, Measurement, Control and Sensor Network*, pages 101–104. IEEE, 2012.

[59] Adeel Iqbal, Mariam Akbar, Nadeem Javaid, Safdar Hussain Bouk, Manzoor Ilahi, and RD Khan. Advanced leach: A static clustering-based heteroneous routing protocol for wsns. *arXiv preprint arXiv:1306.1146*, 2013.

[60] Li Qing, Qingxin Zhu, and Mingwen Wang. Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. *Computer communications*, 29(12):2230–2237, 2006. 1132.

[61] Abderrahim BENI HSSANE and Moulay Lahcen. Improved and balanced leach for heterogeneous wireless sensor networks. *IJCSE International Journal on Computer Science and Engineering*, 2(08):2633–2640, 2010.

[62] Afnan N Al-Romi. *An Enhanced Hierarchical Energy Efficient Intrusion Detection System for Malicious Packet Dropping Attacks in Wireless Sensor Networks*. PhD thesis, Prince Sultan University, 2015.

[63] Frank Comeau and Nauman Aslam. Analysis of leach energy parameters. *Procedia Computer Science*, 5:933–938, 2011.

Appendices

Appendix A

Matlab Simulation Source Code

In this section, we put the MATLAB source code that is written to accomplish different scenarios of this thesis work. By combining this source code we analyze the proposed routing protocol and make compression of each protocol in this thesis. Due to the size of the Matlab code, all codes used in this thesis are not included in this section. The remaining Matlab codes simulation environment setup and others structures are similar to the presented code in this section.

A.1 LEACH routing Protocol

A.1.1 LEACH routing Protocol with Black Hole Attack

```
 % LEACH  with  Black hole attack
function [STATISTICS2,FD2,HD2,AD2]=LEACH_under_BHA(IniEng,NetSize,...
NoOfNode,NoOfRound,cluster_head_percentage,LEACH_R_BHA)
% Simultion Environment setup
xm=NetSize;
ym=NetSize;
sink.x=0.5*xm;
sink.y=0.5*ym;
n=NoOfNode;
P=cluster_head_percentage;
Eo=IniEng;
sink.x=0.5*xm;
sink.y=0.5*ym;
rmax=NoOfRound; %maximum number of rounds
ETX=50*0.000000001; % Tranmitter energy
ERX=50*0.000000001; % Receiver energy
Efs=10*0.000000000001; %Free Space energy
```

```
Emp=0.0013*0.000000000001; %Multipath Loss
EDA=5*0.000000001; %Data Aggregation Energy/compression energy
a=1.5;%fraction of energy enhancment of advance nodes
do=sqrt(Efs/Emp);  %distance do is measured
EtLEACH_BHA=0;  % add for original LEACH routing with BHA
m=0.1;   %  malicious node percentage
normal=n*(1-m);  % sensor nodes normal nodes
advance=n*m;   %  malicous nodes
figure(1);
for i=1:1:advance
SLEACH_BHA(i).xd=rand(1,1)*xm;
XRLEACH_BHA(i)=SLEACH_BHA(i).xd;
SLEACH_BHA(i).yd=rand(1,1)*ym;
YRLEACH_BHA(i)=SLEACH_BHA(i).yd;
SLEACH_BHA(i).G=0;
plot(SLEACH_BHA(i).xd,SLEACH_BHA(i).yd,'+','MarkerSize',6,'MarkerFaceColor','
text(SLEACH_BHA(i).xd+1,SLEACH_BHA(i).yd-0.5,num2str(i));
hold on;
SLEACH_BHA(i).E=Eo;
SLEACH_BHA(i).ENERGY=1;
ELEACH_BHA(i)= SLEACH_BHA(i).E;
EtLEACH_BHA= EtLEACH_BHA+ELEACH_BHA(i);
SLEACH_BHA(i).type='N';
end
for i=advance+1:1:n
SLEACH_BHA(i).xd= rand(1,1)*xm;
XRLEACH_BHA(i)=SLEACH_BHA(i).xd;
SLEACH_BHA(i).yd= rand(1,1)*ym;
YRLEACH_BHA(i)= SLEACH_BHA(i).yd;
SLEACH_BHA(i).G=0;
plot(SLEACH_BHA(i).xd,SLEACH_BHA(i).yd,'o', 'MarkerSize',6,'MarkerFaceColor',
text(SLEACH_BHA(i).xd+1,SLEACH_BHA(i).yd-0.5,num2str(i));
hold on;
SLEACH_BHA(i).E=Eo;
SLEACH_BHA(i).ENERGY=0;
ELEACH_BHA(i)= SLEACH_BHA(i).E;
EtLEACH_BHA=EtLEACH_BHA+ELEACH_BHA(i);
SLEACH_BHA(i).type='N';
end
hold off;
SLEACH_BHA(n+1).xd=sink.x;
```

```
SLEACH_BHA(n+1).yd=sink.y;

%% this is used to calculate max and min distance from nodi to BS
% Finding the cost matrix of the network
for i=1:1:n+1
for j=1:1:n+1
cost(i,j)=sqrt((SLEACH_BHA(i).xd-(SLEACH_BHA(j).xd))^2 + ...
          (SLEACH_BHA(i).yd-(SLEACH_BHA(j).yd))^2);
end
end
src=n+1;
% Finding distance between the nodes and base station
for i=1:1:n
dist(i)=cost(src,i);
end
TotalDis =sum(dist); %Total Distanece between all sensor nodes and BS
dtoAveg = TotalDis/100; % Average Distance Between Sensor node and BS
% calculate the  absolute differwnce between Averge Distance to BS with node
for i= 1:1:n
distZ(i)= cost(i,src);
Abs_Dis (i)= abs(dtoAveg -cost(i,src));
Threshold_modefication(i) = Abs_Dis (i)/ dtoAveg;
end
% Counters for cluster heads (CH) and clusters in the network
countCHs_LEACH_BHA=0;
cluster_LEACH_BHA=1;
flag_first_dead_LEACH_BHA=0;
flag_half_dead_LEACH_BHA=0;
flag_all_dead_LEACH_BHA=0;
dead_LEACH_BHA=0;
first_dead_LEACH_BHA=0;
half_dead_LEACH_BHA=0;
all_dead_LEACH_BHA=0;
allive_LEACH_BHA=n;
%counter for bit transmitted to Bases Station and to Cluster Heads
packets_TO_BS_LEACH_BHA=0;
packets_TO_BS_per_round_LEACH_BHA=0; % packets counter to BS per round
packets_TO_CH_LEACH_BHA=0;
for r=0:1:rmax
packets_TO_BS_per_roundLEACH_BHA=0;
if(mod(r, round(1/P) )==0)
```

```
for i=1:1:n
SLEACH_BHA(i).G=0;
SLEACH_BHA(i).cl=0;
end
end
%Remaining Energy Calculation  in the network at each round
LEACH_R_BHA=0;
for i=1:100
LEACH_R_BHA=SLEACH_BHA(i).E+LEACH_R_BHA;
end
STATISTICS.LEACH_R_BHA(r+1)= LEACH_R_BHA;
EcLR_BHA = EtLEACH_BHA - STATISTICS.LEACH_R_BHA(r+1);
STATISTICS.EcLR_BHA(r+1)= EcLR_BHA;
LEACH_BHAavg = LEACH_R_BHA/100;
STATISTICS.LEACH_BHAavg(r+1)=  LEACH_BHAavg;
Ea4_BHA=EtLEACH_BHA*(1-r/rmax)/n;
dead_LEACH_BHA=0;
for i=1:1:n
if (SLEACH_BHA(i).E<=0)
dead_LEACH_BHA=dead_LEACH_BHA+1;
if (dead_LEACH_BHA==1)
if(flag_first_dead_LEACH_BHA==0)
first_dead_LEACH_BHA=r;
flag_first_dead_LEACH_BHA=1;
end
end
if(dead_LEACH_BHA==0.5*n)
if(flag_half_dead_LEACH_BHA==0)
half_dead_LEACH_BHA=r;
flag_half_dead_LEACH_BHA=1;
end
end
if(dead_LEACH_BHA==0.9*n)
if(flag_all_dead_LEACH_BHA==0)
all_dead_LEACH_BHA=r;
flag_all_dead_LEACH_BHA=1;
end
end
end
if SLEACH_BHA(i).E>0
SLEACH_BHA(i).type='N';
```

```
end
end
STATISTICS.DEAD_LEACH_BHA(r+1)=dead_LEACH_BHA;
STATISTICS.ALLIVE_LEACH_BHA(r+1)=allive_LEACH_BHA-dead_LEACH_BHA;
countCHs_LEACH_BHA=0;
cluster_LEACH_BHA=1;
for i=1:1:n
if Ea4_BHA>0
if(SLEACH_BHA(i).E>0)
temp_rand42=rand;
if ( (SLEACH_BHA(i).G)<=0)
if(temp_rand42<= (P/(1-P*mod(r,round(1/P)))))
countCHs_LEACH_BHA=countCHs_LEACH_BHA+1;
% Implement Black hole attack
if (SLEACH_BHA(i).ENERGY ~=1)
packets_TO_BS_LEACH_BHA=packets_TO_BS_LEACH_BHA+1;
%packet counter for each rouund to BS
packets_TO_BS_per_round_LEACH_BHA=packets_TO_BS_per_round_LEACH_BHA+1;
PACKETS_TO_BS_LEACH_BHA(r+1)=packets_TO_BS_LEACH_BHA;
end
SLEACH_BHA(i).type='C';
SLEACH_BHA(i).rn=r;
SLEACH_BHA(i).G=round(1/P)-1;
C1L_BHA(cluster_LEACH_BHA).xd=SLEACH_BHA(i).xd;
C1L_BHA(cluster_LEACH_BHA).yd=SLEACH_BHA(i).yd;
distance=sqrt( (SLEACH_BHA(i).xd-(SLEACH_BHA(n+1).xd) )^2 +...
(SLEACH_BHA(i).yd-(SLEACH_BHA(n+1).yd) )^2 );
C1L_BHA(cluster_LEACH_BHA).distance=distance;
C1L_BHA(cluster_LEACH_BHA).id=i;
X1L_BHA(cluster_LEACH_BHA)=SLEACH_BHA(i).xd;
Y1L_BHA(cluster_LEACH_BHA)=SLEACH_BHA(i).yd;
cluster_LEACH_BHA=cluster_LEACH_BHA+1;
distance;
%% Energy disipation between CH and BS
if ((distance>do) && (SLEACH_BHA(i).ENERGY ~=1))
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( (ETX+EDA)*(4000) + ...
Emp*4000*( distance*distance*distance*distance ));
end
if ((distance<=do) && (SLEACH_BHA(i).ENERGY ~=1))
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( (ETX+EDA)*(4000) + ...
Efs*4000*( distance * distance ));
```

```
end
end
end
end
end
end
STATISTICS.COUNTCHS_LEACH_BHA(r+1)=countCHs_LEACH_BHA;
for i=1:1:n
if ( SLEACH_BHA(i).type=='N' && SLEACH_BHA(i).E>0 )
if(cluster_LEACH_BHA-1>=1)
min_dis=sqrt( (SLEACH_BHA(i).xd-SLEACH_BHA(n+1).xd)^2 +...
              (SLEACH_BHA(i).yd-SLEACH_BHA(n+1).yd)^2 );
min_dis_cluster=0;
for c=1:1:cluster_LEACH_BHA-1
temp=min(min_dis,sqrt( (SLEACH_BHA(i).xd-C1L_BHA(c).xd)^2 +...
                  (SLEACH_BHA(i).yd-C1L_BHA(c).yd)^2 ) );
if ( temp<min_dis )
min_dis=temp;
min_dis_cluster=c;
end
end
if(min_dis_cluster~=0)
min_dis;
if (SLEACH_BHA(i).ENERGY ~=1)
if (min_dis>do)
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( ETX*(4000)+...
Emp*4000*( min_dis * min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( ETX*(4000)+ ...
Efs*4000*( min_dis * min_dis));
end
end
SLEACH_BHA(C1L_BHA(min_dis_cluster).id).E = ...
SLEACH_BHA(C1L_BHA(min_dis_cluster).id).E- ( (ERX + EDA)*4000 );
packets_TO_CH_LEACH_BHA=packets_TO_CH_LEACH_BHA+1;
else
min_dis;
if (SLEACH_BHA(i).ENERGY ~=1)
if (min_dis>do)
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( ETX*(4000) + ...
```

```
Emp*4000*( min_dis * min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( ETX*(4000) +...
Efs*4000*( min_dis * min_dis));
end
packets_TO_BS_LEACH_BHA=packets_TO_BS_LEACH_BHA+1;
%added for packet ch to BS per round
packets_TO_BS_per_round_LEACH_BHA=packets_TO_BS_per_round_LEACH_BHA+1;
PACKETS_TO_BS_LEACH_BHA(r+1)=packets_TO_BS_LEACH_BHA;
end
end
SLEACH_BHA(i).min_dis=min_dis;
SLEACH_BHA(i).min_dis_cluster=min_dis_cluster;
else
min_dis=sqrt( (SLEACH_BHA(i).xd-SLEACH_BHA(n+1).xd)^2 + ...
(SLEACH_BHA(i).yd-SLEACH_BHA(n+1).yd)^2 );
if (SLEACH_BHA(i).ENERGY ~=1)
if (min_dis>do)
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( ETX*(4000) +...
Emp*4000*( min_dis * min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLEACH_BHA(i).E=SLEACH_BHA(i).E- ( ETX*(4000) +...
Efs*4000*( min_dis * min_dis));
end
packets_TO_BS_LEACH_BHA=packets_TO_BS_LEACH_BHA+1;
% packet counter for CH to BS
packets_TO_BS_per_round_LEACH_BHA=packets_TO_BS_per_round_LEACH_BHA+1;
end
end
end
end
STATISTICS.PACKETS_TO_CH_LEACH_BHA(r+1)=packets_TO_CH_LEACH_BHA;
STATISTICS.PACKETS_TO_BS_LEACH_BHA(r+1)=packets_TO_BS_LEACH_BHA;
% packet counter from CH to BS per round
STATISTICS.PACKETS_TO_BS_PER_ROUND_LEACH_BHA(r+1)=...
                                packets_TO_BS_per_round_LEACH_BHA;
STATISTICS.THROUGHPUT_LEACH_BHA(r+1)=STATISTICS.PACKETS_TO_BS_LEACH_BHA(r+1).
                                    +STATISTICS.PACKETS_TO_CH_LEACH_BHA(r+1);
end
```

```
STATISTICS2=STATISTICS;
FD2=first_dead_LEACH_BHA;
HD2=half_dead_LEACH_BHA;
AD2= all_dead_LEACH_BHA;

STATISTICS.DEAD_LEACH_BHA(r+1)
STATISTICS.ALLIVE_LEACH_BHA(r+1)
STATISTICS.PACKETS_TO_CH_LEACH_BHA(r+1)
STATISTICS.PACKETS_TO_BS_LEACH_BHA(r+1)
STATISTICS.COUNTCHS_LEACH_BHA(r+1)
```

A.2 Proposed LEACH Routing Protocol

A.2.1 Scenario 1 without Black Hole Attack

```
%% Thsesis Experment
% LEACH With Modified Threshold Fnction
function [STATISTICS3,FD3,HD3,AD3]=LEACHD(IniEng,NetSize,...
NoOfNode,NoOfRound,cluster_head_percentage,LEACHD_R)
xm=NetSize;
ym=NetSize;
sink.x=0.5*xm;
sink.y=0.5*ym;
n=NoOfNode;
P=cluster_head_percentage;
Eo=IniEng;
sink.x=0.5*xm;
sink.y=0.5*ym;
ETX=50*0.000000001; % Tranmitter energy
ERX=50*0.000000001; % Receiver energy
Efs=10*0.000000000001; %Free Space energy/
Emp=0.0013*0.000000000001; %Multipath Loss
EDA=5*0.000000001;    %Data Aggregation Energy/
a=1.5; %fraction of energy enhancment of advance r malicious node
rmax=NoOfRound; %maximum number of rounds
do=sqrt(Efs/Emp);  %distance do is measured
EtLD=0;
m=0.1;
normal=n*(1-m);  % sensor nodes normal nodes
advance=n*m;    %  Advanced nodes
figure(1);
```

```
% Snsor node and BS configuration
for i=1:1:advance
SLD(i).xd=rand(1,1)*xm ;
XR(i)=SLD(i).xd ;
XRLD(i)=XR(i);
SLD(i).yd=rand(1,1)*ym;
YR(i)=SLD(i).yd;
YRLD(i)=YR(i);
SLD(i).G=0;
plot(SLD(i).xd,SLD(i).yd,'+','MarkerSize',8,'MarkerFaceColor','g')
hold on;
SLD(i).E=Eo;
SLD(i).ENERGY=1;
ELD(i)= SLD(i).E;
EtLD= EtLD+ELD(i);
SLD(i).type='N';
end
for i=advance+1:1:n
SLD(i).xd= rand(1,1)*xm;
XR(i)=SLD(i).xd;
XRLD(i)=SLD(i).xd;
SLD(i).yd= rand(1,1)*ym;
YR(i)=SLD(i).yd;
YRLD(i)= YR(i);
SLD(i).G=0;
plot(SLD(i).xd,SLD(i).yd,'o', 'MarkerSize', 8, 'MarkerFaceColor', 'g')
hold on;
SLD(i).E=Eo;
SLD(i).ENERGY=0;
ELD(i)= SLD(i).E;
EtLD=EtLD+ELD(i);
SLD(i).type='N';
end
hold off;
SLD(n+1).xd=sink.x;
SLD(n+1).yd=sink.y;
plot(SLD(n+1).xd,SLD(n+1).yd,'x');
%% This is used to calculate max and min distance from nodi to BS
% Finding the cost matrix of the network
for i=1:1:n+1
for j=1:1:n+1
```

```
cost(i,j)=sqrt((SLD(i).xd-(SLD(j).xd))^2 +...
(SLD(i).yd-(SLD(j).yd))^2);
end
end
src=n+1;
% Finding distance between the nodes and base station
for i=1:1:n
dist(i)=cost(src,i);
end
TotalDis =sum(dist); % Total Distanece between all sensor nodes and BS
dtoAveg = TotalDis/100; % Average Distance Between Sensor node and BS
% calculate the  absolute differwnce between Averge Distance to BS
witnode i
for i= 1:1:n
distZ(i)= cost(i,src);
Abs_Dis (i)= abs(dtoAveg -cost(i,src));
Threshold_modefication(i) = Abs_Dis (i)/ dtoAveg;
end
% Counters for cluster heads (CH) and clusters in the network
countCHs_LEACHD=0;
cluster_LED =1;
flag_first_dead_LEACHD =0;
flag_half_dead_LEACHD =0;
flag_all_dead_LEACHD =0;
first_dead_LEACHD =0;
half_dead_LEACHD =0;
all_dead_LEACHD =0;
allive_LEACHD =n;
%counter for bit transmitted to Bases Station and to Cluster Heads
packets_TO_BS_LEACHD =0;
packets_TO_BS_per_round_LEACHD =0;
packets_TO_CH_LEACHD =0;
for r=0:1:rmax
% packets counter to BS per round
packets_TO_BS_per_round_LEACHD =0;
if(mod(r, round(1/P) )==0)
for i=1:1:n
SLD(i).G=0;
SLD(i).cl=0;
end
end
```

```
%Remaining Energy Calculation  in the network at each round
LEACHD_R=0;
for i=1:100
LEACHD_R=SLD(i).E+LEACHD_R;
end
STATISTICS.LEACHD_R(r+1)= LEACHD_R;
EcLDR = EtLD - STATISTICS.LEACHD_R(r+1);
STATISTICS.EcLDR(r+1)=EcLDR;
Ea5=EtLD *(1-r/rmax)/n;
%Number of Dead Node Calculation
dead_LEACHD =0;
for i=1:1:n
if (SLD(i).E<=0)
dead_LEACHD=dead_LEACHD+1;
if (dead_LEACHD ==1)
if(flag_first_dead_LEACHD ==0)
first_dead_LEACHD =r;
flag_first_dead_LEACHD =1;
end
end
if(dead_LEACHD==0.5*n)
if(flag_half_dead_LEACHD ==0)
half_dead_LEACHD =r;
flag_half_dead_LEACHD =1;
end
end
if(dead_LEACHD ==0.9* n)
if(flag_all_dead_LEACHD ==0)
all_dead_LEACHD =r;
flag_all_dead_LEACHD =1;
end
end
end
if SLD(i).E>0
SLD(i).rop=r;
SLD(i).type='N';
end
end
plot(SLD(n+1).xd,SLD(n+1).yd,'x');
text(SLD(n+1).xd,SLD(n+1).yd,'BS');
STATISTICS.DEAD_LEACHD(r+1)= dead_LEACHD;
```

```
STATISTICS.ALLIVE_LEACHD(r+1)=allive_LEACHD - dead_LEACHD;
% cluster head Selection
countCHs_LEACHD =0;
cluster_LED =1;
for i=1:1:n
if Ea5>0
if (SLD(i).E<= Eo)
p2(i)=P*SLD(i).E/Ea5;
end
if(SLD(i).E>0)
temp_rand5=rand;
if ( (SLD(i).G)<=0)
if(temp_rand5<= ((p2(i)/(1-(p2(i)*(r*mod(1,p2(i)))))) * ...
        Threshold_modefication(i))
countCHs_LEACHD=countCHs_LEACHD +1;
packets_TO_BS_LEACHD=packets_TO_BS_LEACHD+1;
% added for packet counter for each rouund to BS
packets_TO_BS_per_round_LEACHD=packets_TO_BS_per_round_LEACHD+1;
PACKETS_TO_BS_LEACHD(r+1)=packets_TO_BS_LEACHD;
SLD(i).type='C';
SLD(i).G=round(1/p2(i))-1;
CLED (cluster_LED).xd=SLD(i).xd;
CLED (cluster_LED).yd=SLD(i).yd;
plot(SLD(i).xd,SLD(i).yd,'k*');
text(SLD(i).xd,SLD(i).yd,'CH');
distance=sqrt( (SLD(i).xd-(SLD(n+1).xd) )^2 + (SLD(i).yd-(SLD(n+1).yd) )^2 );
CLED (cluster_LED).distance=distance;
CLED (cluster_LED).id=i;
XLED(cluster_LED)=SLD(i).xd;
YLED(cluster_LED)=SLD(i).yd;
cluster_LED=cluster_LED+1;
distance;
% Energy consumed by CH during data transmission to BS
if (distance>do)
SLD(i).E=SLD(i).E- ( (ETX+EDA)*(4000) + ...
                    Emp*4000*( distance*distance*distance*distance ));
end
if (distance<=do)
SLD(i).E=SLD(i).E- ( (ETX+EDA)*(4000)  + Efs*4000*( distance * distance ));
end
end
```

```
end
end
end
end
STATISTICS.COUNTCHS_LEACHD(r+1)=countCHs_LEACHD;
for i=1:1:n
if ( SLD(i).type=='N' && SLD(i).E>0 )
if(cluster_LED-1>=1)
min_dis=sqrt( (SLD(i).xd-SLD(n+1).xd)^2 + (SLD(i).yd-SLD(n+1).yd)^2 );
min_dis_cluster=0;
for c=1:1:cluster_LED-1
% DistanceToCH -> Sensor node To CH
temp=min(min_dis,sqrt((SLD(i).xd-CLED (c).xd)^2+(SLD(i).yd-CLED (c).yd)^2));
if ( temp<min_dis )
min_dis=temp;
min_dis_cluster=c;
end
end
if(min_dis_cluster~=0)
% Energy consumed by SN during data transmission to CH
min_dis;
if (min_dis>do)
SLD(i).E=SLD(i).E- ( ETX*(4000) + Emp*4000*( min_dis * min_dis * min_dis * mi
end
if (min_dis<=do)
SLD(i).E=SLD(i).E- ( ETX*(4000) + Efs*4000*( min_dis * min_dis));
end
SLD(CLED (min_dis_cluster).id).E = SLD(CLED (min_dis_cluster).id).E- ...
                                    ( (ERX + EDA)*4000 );
packets_TO_CH_LEACHD=packets_TO_CH_LEACHD+1;
else
min_dis;
if (min_dis>do)
SLD(i).E=SLD(i).E- ( ETX*(4000) + Emp*4000*( min_dis * ...
                                        min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLD(i).E=SLD(i).E- ( ETX*(4000) + Efs*4000*( min_dis * min_dis));
end
packets_TO_BS_LEACHD=packets_TO_BS_LEACHD+1;
%added for packet ch to BS per round
```

```
packets_TO_BS_per_round_LEACHD=packets_TO_BS_per_round_LEACHD+1;
PACKETS_TO_BS_LEACHD(r+1)=packets_TO_BS_LEACHD;
end
SLD(i).min_dis=min_dis;
SLD(i).min_dis_cluster=min_dis_cluster;
else
min_dis=sqrt( (SLD(i).xd-SLD(n+1).xd)^2 + (SLD(i).yd-SLD(n+1).yd)^2 );
if (min_dis>do)
SLD(i).E=SLD(i).E- ( ETX*(4000) + Emp*4000*( min_dis *...
                                        min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLD(i).E=SLD(i).E- ( ETX*(4000) + Efs*4000*( min_dis * min_dis));
end
packets_TO_BS_LEACHD=packets_TO_BS_LEACHD+1;
%packet counter for CH to BS
packets_TO_BS_per_round_LEACHD=packets_TO_BS_per_round_LEACHD+1;
end
end
end
STATISTICS.PACKETS_TO_CH_LEACHD(r+1)=packets_TO_CH_LEACHD;
STATISTICS.PACKETS_TO_BS_LEACHD(r+1)=packets_TO_BS_LEACHD;
% packet counter from CH to BS per round
STATISTICS.PACKETS_TO_BS_PER_ROUND_LEACHD(r+1)=packets_TO_BS_per_round_LEACHD;
STATISTICS.THROUGHPUT_LEACHD(r+1)=STATISTICS.PACKETS_TO_BS_LEACHD(r+1)+...
                                  STATISTICS.PACKETS_TO_CH_LEACHD(r+1);
end
STATISTICS3=STATISTICS;
FD3=first_dead_LEACHD;
HD3= half_dead_LEACHD;
AD3= all_dead_LEACHD;

STATISTICS.DEAD_LEACHD(r+1)
STATISTICS.ALLIVE_LEACHD(r+1)
STATISTICS.PACKETS_TO_CH_LEACHD(r+1)
STATISTICS.PACKETS_TO_BS_LEACHD(r+1)
STATISTICS.COUNTCHS_LEACHD(r+1)
```

A.2.2 Scenario 1 Proposed system enhanced with security mechanisms for black hole attack

```
%%  Proposed LEACH enhanced security mechanisms for Black Hole attack
function [STATISTICS5,FD5,HD5,AD5]=Secure_LEACHD_FromBHA(IniEng,NetSize,...
        NoOfNode,NoOfRound,cluster_head_percentage,LEACHD_BA_RSec)
xm=NetSize;
ym=NetSize;
sink.x=0.5*xm;
sink.y=0.5*ym;
n=NoOfNode;
P=cluster_head_percentage;
Eo=IniEng;
sink.x=0.5*xm;
sink.y=0.5*ym;
ETX=50*0.000000001; % Tranmitter energy
ERX=50*0.000000001; % Receiver energy
Efs=10*0.000000000001; %Free Space energy
Emp=0.0013*0.000000000001; %Multipath Loss
EDA=5*0.000000001; %Data Aggregation Energy
a=1.5; %fraction of energy enhancment of advance nodes
rmax=NoOfRound; %maximum number of rounds
do=sqrt(Efs/Emp);  %distance do is measured
EtLD_BASec=0;
m=0.1;
normal=n*(1-m);  %sensor nodes normal nodes
advance=n*m;   %  malicous nodes
figure(1);
for i=1:1:advance
SLD_BASec(i).xd=rand(1,1)*xm;
XRLD_BASec(i)=SLD_BASec(i).xd;
SLD_BASec(i).yd=rand(1,1)*ym;
YRLD_BASec(i)=SLD_BASec(i).yd;
SLD_BASec(i).G=0;
plot(SLD_BASec(i).xd,SLD_BASec(i).yd,'+','MarkerSize', 6,'MarkerFaceColor', 'g
text(SLD_BASec(i).xd+1,SLD_BASec(i).yd-0.5,num2str(i));
hold on;
SLD_BASec(i).E=Eo;
SLD_BASec(i).ENERGY=1;
ELD_BASec(i)= SLD_BASec(i).E;
EtLD_BASec= EtLD_BASec+ELD_BASec(i);
SLD_BASec(i).type='N';
end
for i=advance+1:1:n
```

```
SLD_BASec(i).xd= rand(1,1)*xm;
XRLD_BASec(i)=SLD_BASec(i).xd;
SLD_BASec(i).yd =rand(1,1)*ym;
YRLD_BASec(i)= SLD_BASec(i).yd;
SLD_BASec(i).G=0;
plot(SLD_BASec(i).xd,SLD_BASec(i).yd,'o','MarkerSize',6,'MarkerFaceColor','g')
text(SLD_BASec(i).xd+1,SLD_BASec(i).yd-0.5,num2str(i));
hold on;
SLD_BASec(i).E=Eo;
SLD_BASec(i).ENERGY=0;
ELD_BASec(i)= SLD_BASec(i).E;
EtLD_BASec=EtLD_BASec+ELD_BASec(i);
SLD_BASec(i).type='N';
end
hold off;
SLD_BASec(n+1).xd=sink.x;
SLD_BASec(n+1).yd=sink.y;

%% this is used to calculate max and min distance from nodi to BS
% Finding the cost matrix of the network
for i=1:1:n+1
for j=1:1:n+1
cost(i,j)=sqrt((SLD_BASec(i).xd-(SLD_BASec(j).xd))^2 + ...
(SLD_BASec(i).yd-(SLD_BASec(j).yd))^2);
end
end
src=n+1;
% Finding distance between the nodes and base station
for i=1:1:n
dist(i)=cost(src,i);
end
TotalDis =sum(dist); % Total Distanece between all sensor nodes and BS
dtoAveg = TotalDis/100; %Average Distance Between Sensor node and BS
% calculate the  absolute differwnce between Averge Distance to BS
with node i
for i= 1:1:n
distZ(i)= cost(i,src);
Abs_Dis (i)= abs(dtoAveg -cost(i,src));
Threshold_modefication(i) = Abs_Dis (i)/ dtoAveg;
end
% Counters for cluster heads (CH) and clusters in the network
```

```
countCHSLD_BASec=0;
clusterLD_BASec=1;
flag_first_deadLEACHD_BASec=0;
flag_half_deadLEACHD_BASec=0;
flag_all_deadLEACHD_BASec=0;
deadLEACHD_BASec=0;
first_deadLEACHD_BASec=0;
half_deadLEACHD_BASec=0;
all_deadLEACHD_BASec=0;
allivELED_BASec=n;
%counter for bit transmitted to Bases Station and to Cluster Heads
packets_TO_BSLD_BASec=0;
packets_TO_BS_per_roundLEACHD_BASec=0;
packets_TO_CHLEACHD_BASec=0;
for r=0:1:rmax
packets_TO_BS_per_roundLEACHD_BASec=0;
if(mod(r, round(1/P) )==0)
for i=1:1:n
SLD_BASec(i).G=0;
SLD_BASec(i).cl=0;
end
end
%Remaining Energy Calculation  in the network at each round with Black hole a
LEACHD_BA_RSec=0;
for i=1:100
LEACHD_BA_RSec=SLD_BASec(i).E + LEACHD_BA_RSec;
end
STATISTICS.LEACHD_BA_RSec(r+1)= LEACHD_BA_RSec;
EcLD_BARSec=EtLD_BASec - LEACHD_BA_RSec;
STATISTICS.EcLD_BARSec(r+1)=EcLD_BARSec;
LEACHD_BAavgSec=LEACHD_BA_RSec/n;
STATISTICS.LEACHD_BAavgSec(r+1)= LEACHD_BAavgSec;
Ea_BASec=EtLD_BASec *(1-r/rmax)/n;
deadLEACHD_BASec=0;
for i=1:1:n
if (SLD_BASec(i).E<=0)
deadLEACHD_BASec=deadLEACHD_BASec+1;
if (deadLEACHD_BASec==1)
if(flag_first_deadLEACHD_BASec==0)
first_deadLEACHD_BASec=r;
flag_first_deadLEACHD_BASec=1;
```

```
end
end
if(deadLEACHD_BASec==0.5*n)
if(flag_half_deadLEACHD_BASec==0)
half_deadLEACHD_BASec=r;
flag_half_deadLEACHD_BASec=1;
end
end
if(deadLEACHD_BASec==0.9*n)
if(flag_all_deadLEACHD_BASec==0)
all_deadLEACHD_BASec=r;
flag_all_deadLEACHD_BASec=1;
end
end
end
if SLD_BASec(i).E>0
SLD_BASec(i).rop=r;
SLD_BASec(i).type='N';
end
end
STATISTICS.DEADLEACHD_BASec(r+1)=deadLEACHD_BASec;
STATISTICS.ALLIVELED_BASec(r+1)=allivELED_BASec-deadLEACHD_BASec;
countCHSLD_BASec=0;
clusterLD_BASec=1;
for i=1:1:n
if Ea_BASec>0
if (SLD_BASec(i).E<= Eo)
p2Bs(i)=P*SLD_BASec(i).E /Ea_BASec;
end
if(SLD_BASec(i).E>0)
temp_rand8=rand;
if ( (SLD_BASec(i).G)<=0) && ( SLD_BASec(i).E >= ...
STATISTICS.LEACHD_BAavgSec(r+1)/n) && (SLD_BASec(i).ENERGY ~=1)
if(temp_rand8<= ((p2Bs(i)/(1-(p2Bs(i)*(r*mod(1,p2Bs(i))))))) * ...
Threshold_modefication(i))
countCHSLD_BASec=countCHSLD_BASec+1;
% Black hole attack simulation
if (SLD_BASec(i).ENERGY ~=1)
packets_TO_BSLD_BASec=packets_TO_BSLD_BASec+1;
% added for packet counter for each rouund to BS
packets_TO_BS_per_roundLEACHD_BASec=packets_TO_BS_per_roundLEACHD_BASec+1;
```

```
PACKETS_TO_BSLD_BASec(r+1)=packets_TO_BSLD_BASec;
end
SLD_BASec(i).type='C';
SLD_BASec(i).G = round(1/p2Bs(i))-1;
CLD_BASec(clusterLD_BASec).xd=SLD_BASec(i).xd;
CLD_BASec(clusterLD_BASec).yd=SLD_BASec(i).yd;
distance=sqrt((SLD_BASec(i).xd-(SLD_BASec(n+1).xd) )^2 + ...
(SLD_BASec(i).yd-(SLD_BASec(n+1).yd) )^2 );
CLD_BASec(clusterLD_BASec).distance=distance;
CLD_BASec(clusterLD_BASec).id=i;
XLD_BASec(clusterLD_BASec)=SLD_BASec(i).xd;
YLD_BASec(clusterLD_BASec)=SLD_BASec(i).yd;
clusterLD_BASec=clusterLD_BASec+1;
distance;
% energy dissipation for aggregation + transferring of data to BS by CH
if ((distance>do) && (SLD_BASec(i).ENERGY ~=1))
SLD_BASec(i).E=SLD_BASec(i).E- ( (ETX+EDA)*(4000) + ...
Emp*4000*( distance*distance*distance*distance ));
end
if ((distance<=do)&& (SLD_BASec(i).ENERGY ~=1))
SLD_BASec(i).E=SLD_BASec(i).E- ( (ETX+EDA)*(4000)+...
Efs*4000*( distance * distance ));
end
end
end
end
end
end
STATISTICS.COUNTCHSLD_BASec(r+1)=countCHSLD_BASec;
for i=1:1:n
if ( SLD_BASec(i).type=='N' && SLD_BASec(i).E>0 )
if(clusterLD_BASec-1>=1)
% Distance between BS and Sensor Node
min_dis=sqrt( (SLD_BASec(i).xd-SLD_BASec(n+1).xd)^2 + ...
(SLD_BASec(i).yd-SLD_BASec(n+1).yd)^2 );
min_dis_cluster=0;
for c=1:1:clusterLD_BASec-1
temp=min(min_dis,sqrt( (SLD_BASec(i).xd-CLD_BASec(c).xd)^2 ...
+ (SLD_BASec(i).yd-CLD_BASec(c).yd)^2 ) );
if ( temp<min_dis )
min_dis=temp;
```

```
min_dis_cluster=c;
end
end
if(min_dis_cluster~=0)
min_dis;
if (SLD_BASec(i).ENERGY ~=1)
if (min_dis>do)
SLD_BASec(i).E=SLD_BASec(i).E- ( ETX*(4000) + ...
Emp*4000*( min_dis * min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLD_BASec(i).E=SLD_BASec(i).E- ( ETX*(4000)+...
Efs*4000*( min_dis * min_dis));
end
end
SLD_BASec(CLD_BASec(min_dis_cluster).id).E = ...
SLD_BASec(CLD_BASec(min_dis_cluster).id).E- ( (ERX + EDA)*4000 );
packets_TO_CHLEACHD_BASec=packets_TO_CHLEACHD_BASec+1;
else
min_dis;
%%calculate the disipated energy  for non-malicious node
if (SLD_BASec(i).ENERGY ~=1)
if (min_dis>do)
SLD_BASec(i).E=SLD_BASec(i).E- ( ETX*(4000)+...
Emp*4000*( min_dis * min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLD_BASec(i).E=SLD_BASec(i).E- ( ETX*(4000)+...
Efs*4000*( min_dis * min_dis));
end
packets_TO_BSLD_BASec=packets_TO_BSLD_BASec+1;
%added for packet ch to BS per round
packets_TO_BS_per_roundLEACHD_BASec=packets_TO_BS_per_roundLEACHD_BASec+1;
PACKETS_TO_BSLD_BASec(r+1)=packets_TO_BSLD_BASec;
end
end
SLD_BASec(i).min_dis=min_dis;
SLD_BASec(i).min_dis_cluster=min_dis_cluster;
else
min_dis=sqrt( (SLD_BASec(i).xd-SLD_BASec(n+1).xd)^2 +...
(SLD_BASec(i).yd-SLD_BASec(n+1).yd)^2 );
```

```
if (SLD_BASec(i).ENERGY ~=1)
if (min_dis>do)
SLD_BASec(i).E=SLD_BASec(i).E- ( ETX*(4000) +...
Emp*4000*( min_dis * min_dis * min_dis * min_dis));
end
if (min_dis<=do)
SLD_BASec(i).E=SLD_BASec(i).E- ( ETX*(4000) + ...
Efs*4000*( min_dis * min_dis));
end
packets_TO_BSLD_BASec=packets_TO_BSLD_BASec+1;
% packet counter for CH to BS
packets_TO_BS_per_roundLEACHD_BASec=packets_TO_BS_per_roundLEACHD_BASec+1;
end
end
end
end
STATISTICS.PACKETS_TO_CHLEACHD_BASec(r+1)=packets_TO_CHLEACHD_BASec;
STATISTICS.PACKETS_TO_BSLD_BASec(r+1)=packets_TO_BSLD_BASec;
% packet counter from CH to BS per round
STATISTICS.PACKETS_TO_BS_PER_ROUNDLEACHD_BASec(r+1)=...
                        packets_TO_BS_per_roundLEACHD_BASec;
STATISTICS.THROUGHPUT_LEACHD_BASec(r+1)=STATISTICS.PACKETS_TO_BSLD_BASec(r+1)+
STATISTICS.PACKETS_TO_CHLEACHD_BASec(r+1);

TotalNetworkEnergy=0;
for i=1:n
if SLD_BASec(i).E>0
TotalNetworkEnergy=TotalNetworkEnergy + SLD_BASec(i).E;
end
end
STATISTICS.TotalEnergy(r+1)=TotalNetworkEnergy;
STATISTICS.AvgEnergy(r+1)=TotalNetworkEnergy/n;
end
STATISTICS5=STATISTICS;
FD5=first_deadLEACHD_BASec;
HD5=half_deadLEACHD_BASec;
AD5= all_deadLEACHD_BASec;

STATISTICS.DEADLEACHD_BASec(r+1)
STATISTICS.ALLIVELED_BASec(r+1)
STATISTICS.PACKETS_TO_CHLEACHD_BASec(r+1)
```

```
STATISTICS.PACKETS_TO_BSLD_BASec(r+1)
STATISTICS.COUNTCHSLD_BASec(r+1)
```

A.3 Main Function

The main function code presented in this section is not the full thesis Matlab code, which contains only three full functions listed above and the other two functions used in this thesis.

```
%% Thsesis Experment
clear all
close all
IniEng=0.5;%0.5; % Initial Energy of Every Node
NetSize=100; % Network Size
NoOfNode=100; % Number of Node
NoOfRound=5000; % Number of Round
cluster_head_percentage=0.1;
[STATISTICS1,FD1,HD1,AD1]=LEACH(IniEng,NetSize,NoOfNode,NoOfRound,...
                                cluster_head_percentage);
[STATISTICS2,FD2,HD2,AD2]=LEACH_under_BHA(IniEng,NetSize,NoOfNode,NoOfRound,..
                                    cluster_head_percentage);
[STATISTICS3,FD3,HD3,AD3]=LEACHD(IniEng,NetSize,NoOfNode,NoOfRound,...
                                 cluster_head_percentage);
[STATISTICS4,FD4,HD4,AD4]=LEACHD_BHA(IniEng,NetSize,NoOfNode,NoOfRound,...
                                     cluster_head_percentage);
[STATISTICS5,FD5,HD5,AD5]=Secure_LEACHD_FromBHA(IniEng,NetSize,NoOfNode,...
                                        NoOfRound,cluster_head_percentage);
figure(2)
r=0:NoOfRound;
%% Residual energy Graph Ploting
plot( r,STATISTICS3.LEACHD_R,'b',...
r, STATISTICS4.LEACHD_BA_R,'--k',...
r, STATISTICS5.LEACHD_BA_RSec,'-m',...
r,STATISTICS1.LEACH_R,'g',...
r,STATISTICS2.LEACH_R_BHA,'r', 'linewidth',1);
legend('ES-LEACH  or Proposed LEACH', 'ES-LEACH under BHA',...
'Secure ES-LEACH from BHA', 'LEACH ','LEACH under BHA');
xlabel('X(no. of Rounds)');
ylabel('Y(Residual Energy Left in Each Round )');
title('Residual Energy vs Round ');
grid on ;
grid minor;
```

```
%% Packet Sent to BS
figure(3)
plot(r,STATISTICS3.PACKETS_TO_BS_LEACHD,'b',...
r,STATISTICS4.PACKETS_TO_BSLD_BA,'--k', ...
r,STATISTICS5.PACKETS_TO_BSLD_BASec,'-m',...
r,STATISTICS1.PACKETS_TO_BS_LEACH,'g',...
r,STATISTICS2.PACKETS_TO_BS_LEACH_BHA,'r', 'linewidth',1);
legend('ES-LEACH or Proposed LEACH', 'ES-LEACH under BHA',...
'Secure ES-LEACH from BHA','LEACH','LEACH under BHA','Location','Best');
xlabel('X(No. of Rounds)');
ylabel('Y(Number of Packet sent to BS )');
title('No.of Packet Sent to BS in Each Round ');
grid on ;
grid minor;

%% Network Lifetime with Bar Graph
figure(4)
bargraph=[FD1, FD2,FD3,FD4, FD5;....
HD1,HD2,HD3,HD4,HD5;...
AD1,AD2,AD3,AD4,AD5];
bar(bargraph,'group');
legend('LEACH','LEACH under BHA','ES-LEACH or Proposed LEACH',...
'ES-LEACH under BHA', 'Secure ES-LEACH From BHA','Location','NorthWest');
title('Network Lifetime (FND, HND and 90%ND)');
xticklabels({'FIRST DEATH ', 'HALF DEATH', '90% Nodes DEATH'})
ylabel('Number of Rounds');
grid on ;
grid minor;
%% THROUGHPUT GRAPH PLOTING
figure(5)
plot(r,STATISTICS3.THROUGHPUT_LEACHD(r+1),'b',...
r, STATISTICS4.THROUGHPUT_LEACHD_BA(r+1),'--k',...
r,STATISTICS5.THROUGHPUT_LEACHD_BASec(r+1),'-m',...
r, STATISTICS1.THROUGHPUT_LEACH(r+1),'g',....
r,STATISTICS2.THROUGHPUT_LEACH_BHA(r+1),'r', 'linewidth',1);
legend('ES-LEACH or Proposed LEACH', 'ES-LEACH under BHA',...
'Secure ES-LEACH from BHA','LEACH','LEACH under BHA','Location','Southeast');
xlabel('X(No. of rounds)');
ylabel('Y(Number of Packet Sent Per Round ');
title('THROUGHPUT')
```

```
grid on ;
grid minor;

%% Throghput with  bar graph
figure(6)
bargraph2= [STATISTICS1.THROUGHPUT_LEACH(500), STATISTICS2.THROUGHPUT_LEACH_BH
STATISTICS3.THROUGHPUT_LEACHD(500),STATISTICS4.THROUGHPUT_LEACHD_BA(500),...
STATISTICS5.THROUGHPUT_LEACHD_BASec(500);...
STATISTICS1.THROUGHPUT_LEACH(1000), STATISTICS2.THROUGHPUT_LEACH_BHA(1000),...
STATISTICS3.THROUGHPUT_LEACHD(1000),STATISTICS4.THROUGHPUT_LEACHD_BA(1000),...
STATISTICS5.THROUGHPUT_LEACHD_BASec(1000);...
STATISTICS1.THROUGHPUT_LEACH(3500), STATISTICS2.THROUGHPUT_LEACH_BHA(3500),...
STATISTICS3.THROUGHPUT_LEACHD(3500),STATISTICS4.THROUGHPUT_LEACHD_BA(3500),...
STATISTICS5.THROUGHPUT_LEACHD_BASec(3500)];
bar(bargraph2,'group');
legend('LEACH','LEACH under BHA','ES-LEACH ','ES-LEACH unde BHA' ,....
'Secure ES-LEACH from BHA ', 'Location','NorthWest');
title('Throghput at Selected Rounds');
xticklabels({ 'At 500 Round',' At 1500 Round  ', ' At 3500 Round '})
ylabel('Throghput ');
grid on ;
grid minor;
```