



BA-LEACHC: Biphase Authentication Based LEACH-C Protocol for Wireless Sensor Networks

By

MODISAOTSILE MAROPE

Reg. No: 16100031

Department of Computer Science and Information Systems (CS & IS),

Faculty of Sciences,

Botswana International University of Science and Technology

Email: modisaotsile.marope@studentmail.biust.ac.bw, Phone Number: (+267) 72 983 825

A Dissertation/Thesis Submitted to the College of ICT in Partial Fulfilment of the Requirements
for the Award of the Degree of Master of Science in Computer Science and Software Engineering
of BIUST

Supervisor(s): Prof, Kuthadi Venu Madhav

Department of CS & IS,

Faculty of Sciences, BIUST

kuthadiv@biust.ac.bw, (+267) 493 1104

Signature: _____

Date: 01 February 2021

January, 2021

i. DECLARATION AND COPYRIGHT

I, Modisaotsile Marope (16100031), declare that this thesis is my own original research work and that it has not been presented and will not be presented to any other university for a similar or any other degree award.

Signature

The image shows a stylized, handwritten signature in black ink. The signature appears to be the initials 'M R P' written in a cursive, connected style.

This thesis is copyright material protected under the Berne Convention, the Copyright Act of 1999 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for researcher private study, critical scholarly review or discourse with an acknowledgement, without the written permission of the office of the Provost, on behalf of both the author and the Botswana International University of Science and Technology (BIUST).

ii. CERTIFICATION

The undersigned certifies that he has read and hereby recommends for acceptance by the Faculty of Sciences a thesis titled: **BA-LEACHC: Biphase Authentication Based LEACH-C Approach for Wireless Sensor Networks**, in partial fulfilment of degree of Master of Science in Computer Science and Software Engineering of the Botswana International University of Science and Technology (BIUST).

Prof Venu Madhav Kuthadi
(Supervisor)

Signature: _____

Date: 01 February 2021

iii. ACKNOWLEDGEMENTS

Special thanks to my supervisor Prof Venu Madhav Kuthadi for guiding and advising me throughout my research work. He mentored me both in research area and career. Moreover, I would like to thank fellow Computer Science postgraduates' students for the support and knowledge sharing, especially simulating Wireless Sensor Networks (WSNs) in MATLAB. Special recognition also goes to Dr. Banyatsang Mphago for the valuable inspiration to complete my research work in time.

Moreover special thanks to Dr. Hlomani Hlomani for helping me identify a research problem to work on, which is in line with Computer Science field in WSNs. Without his guidance and assistance, I could not have managed to start and complete my Master's Degree. And lastly, Sincere thanks to my intimates for their material help throughout my studies at BIUST.

iv. TABLE OF CONTENTS

i. DECLARATION AND COPYRIGHT	2
ii. CERTIFICATION	3
iii. ACKNOWLEDGEMENTS	4
iv. TABLE OF CONTENTS	5
v. LIST OF FIGURES	8
vi. LIST OF TABLES	9
vii. LIST OF ABBREVIATIONS	10
viii. ABSTRACT	11
CHAPTER 1	12
1. Introduction	12
1.1 Wireless Sensor Network	12
1.1.1 Basic Components in WSNs	13
1.2 Protocol Stack for WSNs	15
1.2.1 DoS (Denial of Service) attack across layers	15
1.3 WSN security requirements	18
1.3.1 Confidentiality in data	18
1.3.2 Integrity in data	18
1.3.3 Authentication in data	18
1.3.4 Data availability	18
1.3.5 Freshness in data	19
1.4 Background to the problem and related studies	19
1.5 Problem statement	21
1.6 Objectives	22
1.7 Research questions	22
1.8 Expected outcome	22
1.9 Thesis contributions	23
1.10 Motivation	23

1.11 Thesis outline	23
CHAPTER 2	25
2. Literature review	25
2.1 LEACH protocol	25
2.1.1 LEACH operation	26
2.2 LEACH-C approach	28
2.2.1 Possible security challenges in LEACH-C	29
2.3 Genetic algorithmns (GAs).....	30
2.3.1 Genetic algorithm process	30
2.3.2 Genetic algorithm operators	31
2.3.3 Application of GAs in WSN design	32
2.4 WSN secure schemes.....	33
2.5 Secure variants of LEACH.....	37
2.6 Summary	41
CHAPTER 3	42
3. Methodology.....	42
3.1 Adopted stages	42
3.2 Implementation methodology	43
3.3 Network scenario and parameters.....	46
3.4 BA-LEACHC: Proposed work	47
3.4.1 Modify proposed approach	50
CHAPTER 4	54
4. Simulation Results.....	54
4.1 Experiments and graphs	54
4.2 Evaluation and comparison of BA-LEACHC and LEACH variants.....	60
CHAPTER 5	62
5. Conclusion and Future work.....	62
5.1 Introduction	62
5.2 Summary of the study	62

5.3 Conclusion	63
5.4 Future work.....	63
REFERENCES.....	65
PLAGIARISM REPORT	68
PROOFREADING CERTIFICATE	69

v. LIST OF FIGURES

Figure 1. 1: Node block diagram	13
Figure 1. 2: sink/ BS (Base Stations)	14
Figure 1. 3: Sensor node radio model	15
Figure 1. 4: WSN protocol stack	15
Figure 2. 1: Hierarchical structure	26
Figure 2. 2: LEACH approach setup	27
Figure 2. 3: LEACH protocol steady-state phase	28
Figure 2. 4: Fitness based selection	31
Figure 2. 5: BAS procedure diagram	34
Figure 3.1: MATLAB (R2015) user interface	43
Figure 3.2: Flow chart of the proposed approach	45
Figure 3.3: BA-LEACHC summary diagram	48
Figure 4. 1: Network deployments	54
Figure 4. 2: Suspicious node	55
Figure 4. 3: Range of the sensor nodes	55
Figure 4. 4: Cluster head failure call for security scheme	56
Figure 4. 5: Dynamic path	56
Figure 4. 6: Finalize route	56
Figure 4. 7: Finalize path as a destination node	57
Figure 4. 8: Throughput (Per cent)	57
Figure 4. 9: End to end delay (second)	58
Figure 4. 10: Energy consumption (joules)	59
Figure 4. 11: Packet delivery rate (Per cent)	59
Figure 4. 12: Comparison in EC	60
Figure 4. 13: Comparison in ST	61

vi. LIST OF TABLES

Table 1.1: Security analysis.....	20
-----------------------------------	----

vii. LIST OF ABBREVIATIONS

BA-LEACHC: -Biphase Authentication based Low Energy Adaptive Clustering Hierarchy Centralized

BS: -Base Station

CDMA: - Code Division Multiple Access

CH: -Cluster Head

CM: -Cluster Members

CurTn: - Current total number of live nodes

DoS: -Denial of Service Attack.

LEACH-C: -Low Energy Adaptive Clustering Hierarchy Centralized

LEACH-CH: - Energy Efficient and Adaptive Clustering for WSNs using Low Energy Adaptive Cluster Hierarchy

LEACH-F: - Fixed Number of Cluster Low Energy Adaptive Cluster Hierarchy

LEACH-L: -Energy Balanced Low Energy Adaptive Cluster Hierarchy

LEACH-V: -Vice cluster Low Energy Adaptive Cluster Hierarchy

MATLAB: - Matrix Laboratory

MLEACH: -Mobile Low Energy Adaptive Clustering Hierarchy

MS-LEACH: -Multi-hop and Single-hop routing Low Energy Adaptive Clustering Hierarchy.

PAWN: -Payload-based Mutual Authentication

PEGASIS: -Power-Efficient Gathering in Sensor Information Systems

PrevTn: - Previous total number of live nodes

REQ: - Requests

SecLEACH: -Security Low Energy Adaptive Clustering Hierarchy.

S-LEACH: -Solar-aware Low Energy Adaptive Clustering Hierarchy.

SS-LEACH: -Specification based Secure Low Energy Adaptive Clustering Hierarchy

TDMA: -Time Division Multiple Access

TF-LEACHC: -Trust Factor based Centralized Low Energy Adaptive Clustering Hierarchy.

WSNs: -Wireless Sensor Networks

viii. ABSTRACT

The intention in Wireless Sensor Networks (WSNs) is to group sensed raw facts from geographical area under monitoring. Yet, sensor nodes sometimes report tempered (falsified) information resulting from malicious nodes. Hence, various studies recommend pre-identification of malicious node as essential for reliable and healthy networks. Different techniques have been proposed to deal with bogus sensor nodes in WSNs, ranging from authentication to trust based approaches. In this research, a recent lightweight scheme called Biphase Authentication Scheme (BAS) is utilised with genetic algorithm (GA) to integrate with (LEACH-C) Low Energy Adaptive Clustering Hierarchy Centralized clustering approach for identification as well as disjoin bogus nodes in WSN. BAS offers small-scale authentication based on unique identity number, master key, key generation based algorithm plus pairwise key. The LEACH-C genetic algorithm utilized with BAS successfully cross examine paths for all nodes connected to failed cluster head therefore, enabling for easy identification of sensor node linked to unsafe path and finally allowing for authentication process to isolate malicious node. The objective fitness approximation of GA in our work might appropriate basing on, extremely high calculation time of single solution, missing of the accurate model for fitness calculation and uncertainty of fitness function or distortion. The proposed approach (BA-LEACHC) is more effective and resistant against denial of service attacks (DoS) due to successful bogus node identification and removal. Moreover, the envisioned protocol is able to provide security with minimal power consumption of 10.6 joules lower than its comparatives.

CHAPTER 1

1. Introduction

1.1 Wireless Sensor Network

Wireless sensor networks are built-up from several or multiple base stations as well as variety of limited resourced nodes classified into base stations (BS) and member nodes (MN) (Monnet et al., 2016). In military, health, tracking and other applications, WSNs are typically deployed in neglected and hostile settings. For such situations, the wireless based networks are susceptible to physical tampering and also different remote attacks for instance Denial of Service (DoS), Sybil, Blackhole, and so on. As a result, security and defence of nodes against destructive behaviours is incredibly essential. However, it is always best to integrate security measures in routing protocols instead of designing a standalone secure mechanism for nodes on basis that nodes are resource constrained due to storage limitations, unbound energy, restricted computation processes and limited communication capabilities. Moreover, one of the contributing factors that prevents execution of robust security in protocols include high usage of energy which reduces network life time considerably. As a result, designing an efficient as well as energy reliable security protocols in WSNs is challenging.

The WSN energy efficient protocols are categorized into hierarchical, location and flat based routing. Clustering in hierarchical form mainly reduces routing outlays and also energy consumption of network nodes. Clustering enables for easy upkeep of topology as well as extending wireless sensor network scalability. The grouping of nodes (clustering) becomes possible through algorithms responsible for clustering. The algorithm will pick some nodes as cluster heads (CH) guided by metrics such as flexibility and amount of power in the node. Among the selected CH, each has to approve neighbour nodes as associate node and manage the functionality. Various nodes grouping approaches have actually recommended by numerous WSN literature. For instance (Boyinbode et al., 2010), (Haque & Yoshida, 2012) examines various clustering algorithms and highlight important attributes and properties. The LEACH approach is one example with hierarchical structure and offers minimal energy consumption in a clustering format. This protocol is also a foundation protocol for many existing protocols.

1.1.1 Basic Components in WSNs

1.1.1.1 Sensor node (SN)

A sensor node is a small device built-up from a couple of sensing unit and a mote system as displayed in figure 1.1. A node works by sensing/ gathering information from the surrounding then relays it to mote. A node can either be cluster head or member node. Usually SNs utilization is for monitoring environmental aspects like temperature, dampness, noise and also individual health criterion like heart beat and etcetera. The Micro-Electro-Mechanical System based sensing unit has discovered excellent use of SNs. Node mote components includes central processing unit, memory, battery plus A/D converter which links to radio and also sensing unit transceiver. The design of each node is enabled to support the execution of multi-hop routing algorithm and relay communicating data packages to the sink. In network execution a node can either be cluster head or cluster member depending on the functionality of the routing algorithm (Michal, 2013). Figure 1.1 depicts node block diagram:

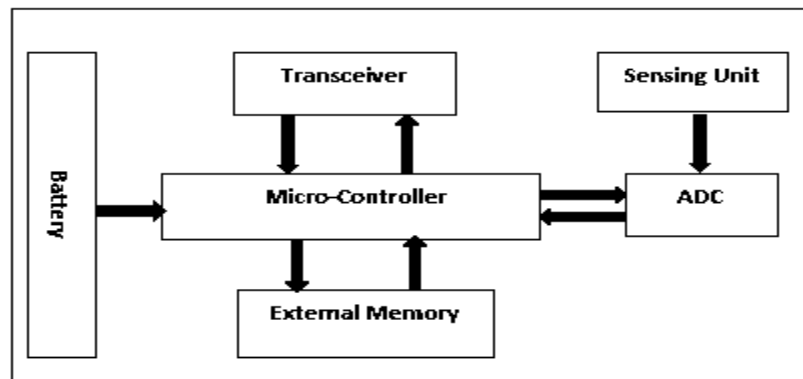


Figure 1. 1: Node block diagram

Cluster head (CH): It is responsible for monitoring and managing the functionality of member nodes or cluster nodes. A cluster may comprise of one CH. A CH collects raw facts from ordinary nodes, process and transfer to the sink (BS) and sometimes to another CH depending on the topology of the network.

Member node (MN): Is an ordinary node that failed CH selection process, its duty is to collect environment data or information then takes it directly to cluster head. Most of the time MNs turns to be nodes with less amount of energy during the time of deployment.

1.1.1.2 Sink node/ BS (base station)

The fundamental use of sink node is to insure and maintain WSN reliability. The components that constructs BS includes processor, radio board, antenna, as well as universal serial bus interface board. Before network setup, sink is programmed using low-power mesh networking to enable communication in a wireless operation. The presence of BS is significant as all network nodes forward their collections to BS for dispensation and decision making. Placement of sink mostly depend on the ability of node to preserve energy and the amount of space to be covered by the network. Normally, depending on the nature of network and routing algorithm, a base stations can either be movable or fixed for collection of sensed data (Michal, 2013). Figure 1.2 present BS/ sink.



Figure 1. 2: sink/ BS (Base Stations)

1.1.1.3 Radio model

Several publications presumed the same radio model under discussion. The physical parts of the model include; the transmitter which is responsible for providing energy to route electrons in the radio transmitter as well as power amplifier. The other hardware include receiver which disperse the received radio electrons as signified. As depicted in Figure 1.3 the gap between receiver and transmitter facilitates use of total free space and design of multipath fading channel. In a case whereby the distance is less compared to the limit, then it means utilization of total free area, if not, then utilize multipath model.

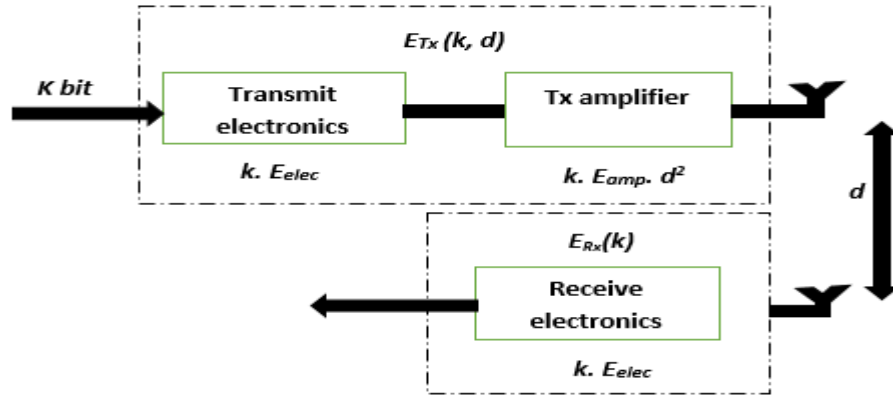


Figure 1. 3: Sensor node radio model

1.2 Protocol Stack for WSNs

There is a model called OSI (Open System Interconnection). Almost all communication protocols are based upon the 7 layers of the very same model. Furthermore, communication style by WSN can be categorized into various layers. WSN does not adhere very closely to the split style of the OSI model as various other networks. As shown in Figure 1.4, WSN protocol stack break into 5 significant layers such as Physical, Datalink, Network, Transport, as well as Application layer. This model is valued at categorizing numerous protocol attacks, as well as corresponding defences (Network & Manaa, n.d.), (Mishra et al., 2015). The following Figure 1.4 depicts WSN OSI model:

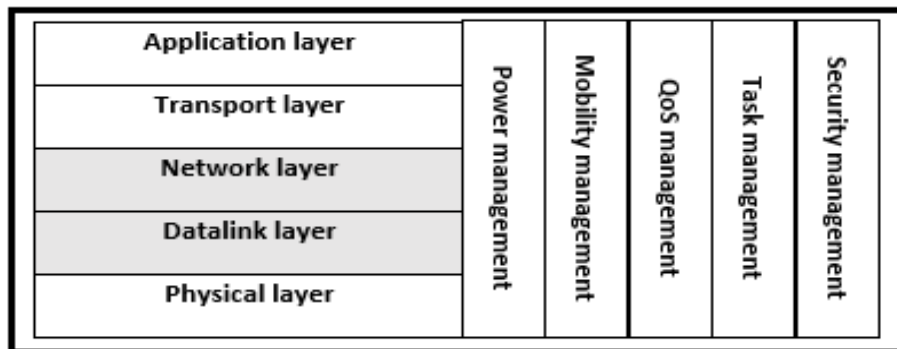


Figure 1. 4: WSN protocol stack

1.2.1 DoS (Denial of Service) attack across layers

The DoS attacks in WSNs influence practical damages which threatens human health and safety across areas of life. DoS attacks generally describes an intruder's intentional efforts to subvert or

damage WSN. Nonetheless, this attack can include any action that disturbs full functionalities of the network (Gavrić & Simić, 2018).

1.2.1.1 Application layer

This layer manages network traffic and provides different software applications for data translation in a readable format. It also sends queries to collect required information in the network. The attacks for this layer include sensory overload that result when adversary stimulate sensor node to overload the network. As for this attack huge data bundles are pushed to sink causing network traffic hence consuming more energy. A possible counter measure to this attack involves bandwidth limiting and effective data aggregation. Another attack in this layer is path-based which flood end to end communication by injecting replayed data packets. A possible solution to path-based attack is applying a good authentication approach.

1.2.1.2 Transportation layer

It assists in maintaining the data flow. The possible attacks involved with this layer include flooding as well as de-synchronization. The intruder might continuously establish fresh connection request up-until connection resources get finished or get to an optimum limitation. Most of the important networks demand will certainly be ignored. Sometimes an intruder can repetitively send packets of data to a node making the receiver to ask for re-transmission of failed structures. In a proper tracking the intruder can weaken and also disturb the host by interfering with its capabilities of effectively exchanging information hence causing exhaustion of power while trying recovery of faked errors.

1.2.1.3 Network layer

It is responsible for information routing, particularly picking paths to send out information. Some of the common network layer attacks includes:

Spoofed routing information: -In WSNs it targets the routing information. An attacker might modify information involved with routing packets with intension to interfere with network traffic. These

disturbances include production of routing loopholes, attracting or pushing back data packets in some nodes, creating long or short routes and so on.

Selective forwarding: In a normal WSN setup all engaged nodes are supposed to be collecting and sending data packets properly. An intruder might jeopardize a node in a manner that is unique when forwarding packets, as it would drop some.

Sinkhole: The intruder compromised node looks more appealing to surrounding nodes as it would imitate information involved with routing packets. With the caused confusion ordinary node selects endangered node as an alternative to route data.

Sybil: It's a WSN attack whereby one node provides more than one network identity.

1.2.1.4 Data link layer

Its attacks consist of actively produced collisions, resource exhaustion, as well as injustice in distribution. In a situation whereby 2 nodes attempt sending same regularity one after the other collision occurs. An intruder may capitalize on re-occurrence of collisions to exhaust network resources. In some instances the layer may continuously effort re-transmitting damaged packets of data. If the discovery of re-transmissions is late, node energy level will certainly reduce. The discussed attacks result in unfairness among node. For instance, an attacker may cause disturbance to real-time applications of some nodes through distracting structure of communications.

1.2.1.5 Physical layer

It is responsible for offering durable modulation and transmission. Just like in any other radio based medium, jamming always threatens physical layer. The major physical layer attacks are as follows;

Jamming: - It obstructs radio frequencies utilized for nodes interaction. Any WSN jamming resource is capable of putting the entire network at stake.

Tampering: -Here, WSNs typically run in outside environments and as a result it may cause permanent damages to sensor nodes. Malicious node can force captured node to release or give secret keys hence modifying program codes afterwards.

1.3 WSN security requirements

Wireless sensor network shares certain commonness to regular wired network system yet likewise displays numerous features which seem uniquely special. WSN safety measures ought to shield tempered network information and isolate misbehaving nodes. Security requirements are classified into primary and secondary. Secondary requirements include: self-organization, secure localization and time synchronization. Primary requirements are most important when it comes to reinforcing protocol security (Khan & Khan, 2019), (Dener, 2014). Primary requirements are discussed as follows:

1.3.1 Confidentiality in data

Safety techniques must guarantee zero access to data packets and should not be recognized by any individual other than the intended recipient. (i) A node should not permit access to its sensed data to neighbours unless they are licensed to do so, (ii) public details such as node identities, as well as public secrets keys of nodes need to likewise be secured to avoid traffic related attacks.

1.3.2 Integrity in data

Data integrity is responsible for protecting the aggregated data against reply attacks. This requirement ensures that the broadcasted messages reach the destination point without any modification.

1.3.3 Authentication in data

The aspect guarantees true self in adversary nodes. A bogus node is not only responsible to data and information packets modification, additionally may alter a number of packets through inserting self-made packages. The reason why is requirement for receiver to authenticate obtained packages as to whether they originated from genuine nodes. When two nodes exchange information verification may be attained via MAC (message authentication code) from common secret keys. Several authentication schemes have actually been suggested by scientist's majority emphases secure routing.

1.3.4 Data availability

It maintains and protects WSN services against any form of denial of service. Any attack aiming to destroy nodes responsible for aggregating data can result in poor network service provision. While some systems take advantage of additional interaction between nodes, some systems suggest the utilization of a CACA (central access control system) to confirm message arrival to every message to its recipient.

1.3.5 Freshness in data

It ensures that processed data is current and also confirms the absence of old message replays. It is particularly essential for sensor nodes sharing secret keys for exchange of messages. An intruder can use old secret key as shadow new key to launch reply attack. To check the freshness of data time specific counter is added to a packet of data.

1.4 Background to the problem and related studies

Successful implementation of security measures during the designing stage of cluster-based routing protocol is extremely critical for preventing attacks and vulnerabilities of network. Few studies focused on securing existing protocols when learning about multiple harms from DoS attack and rising costs as result of secure less networks. (Guyeux et al., 2017), (Sorout & Singh, 2016) reported the significance of securing cluster-based routing protocols for WSNs and indicates that intense security is achievable at low cost in development stage of each protocol. Most of the cluster-based routing protocols focus on reducing energy consumption of node and improving network coverage and performance, hence less priority given to security.

(Saadawy & Shaaban, n.d.) Presented several proposed cluster-based routing protocols for WSNs in which only few focus on addressing security problems. Authors in (Rahayu et al., 2015) (Rohbanian et al., 2013) discussed security application on the following existing protocols: Watchdog-LEACH, SecLEACH, GS-LEACH, S-LEACH, LS-LEACH, RLEACH, PAWN, TF-LEACHC, and MS-LEACH. (Kaushal & Kaur, 2015) stated that any protocol created without considering security requirements is liable to attacks and vulnerabilities such as DoS. (Jasuja, 2017) reported that currently they are many unsecure cluster-based routing protocols and was supported by *Singh et al* on the same statement. (S. K. Singh et al., 2017) also proved the statement to be correct by

discussing more than thirty secure-less LEACH versions. Numerous routing approaches were developed to decrease energy usage across network. (Bagula, 2012) verifies the point of saving energy across various routing algorithms to be true, by indicating that sensor nodes use irreplaceable batteries with energy that has to be used wisely. The study work by (Jasuja, 2017) also discusses the following unsecure routing protocols; CCM (Chain-Cluster-based Mixed routing), ACT (Arranging-Cluster Sizes and Transmission Ranges), HEED (Hybrid Energy-Efficient Distributed Clustering) and MWBCA (Multi-Weight-Based Clustering Algorithm).

(Jan et al., 2017) reviewed security of LEACH-C versus SecLEACH and PAWN and discovered that LEACH-C supplies zero data confidentiality, no authentication, and no data freshness while SecLEACH and PAWN favourably reacted to the stipulated requirements. Other unaddressed security requirements by this review paper include safe and secure localization, data schedule and information integrity. None of the security requirements is achieved by LEACH-C. The outcomes of this review paper suggested that LEACH-C has no trustworthy security mechanism. Table 1.1 shows the relative analysis of the evaluation paper.

Table 1.1: Security analysis

Security Services	LEACH-C (Low Energy Adaptive Clustering Hierarchy Centralized)	SecLEACH (Security Low Energy Adaptive Clustering Hierarchy)	PAWN (Payload-based Mutual Authentication)
Data authentication	None	Message Authentication Code	two-step
Data confidentiality	None	Message Authentication Code	Payload
Data freshness	None	Nonces	Nonces

Numerous clustering routing algorithms are developed to decrease energy usage and improve network coverage area and efficiency, and for this reason, a lesser priority is given to security. There are many proposed cluster-based routing protocols for WSNs however only a few address

network security problems. Other unaddressed security requirements by this review paper include protected localization, data schedule, and data stability. None of the security requirements is accomplished by LEACH-C. The outcomes of this evaluation paper indicated that LEACH-C has no dependable security system.

1.5 Problem statement

The review paper (Jan et al., 2017) demonstrated the inability of LEACH-C to provide member node (MN) to cluster head (CH) authentication, and that result in the protocol susceptible to various attacks. LEACH-C cluster heads broadcast time interval allocated to messages per participant node during data packet transmission process. Therefore, this broadcasted messages stand a chance of modification by the trespassers. Additionally the sensed data by participant nodes are sent with zero security consideration to cluster heads.

This research work tends to address the problem of malicious node network flooding in WSNs that operates with LEACH-C routing protocol by identifying and authenticating malicious or suspicious nodes. Destructive nodes in every network setup can possibly replicate messages and permit DoS (Denial of Service attacks) and subsequently disabling the entire network.

Trust-Factor based LEACH-C (TF-LEACHC) is proposed by (Chandrasekaran, 2014) as first variant protocol that attempts securing LEACH-C, based upon the typical values of its trust aspects (Communication, Data, Functionality, Location, Energy, Trust upgrade, and also Risk). Due to the fact that there is a possibility to deflect the entire network nodes based on wrong trust factor values not resulting from harmful attacks, TF-LEACHC gives unreliable safety to LEACH-C. And also, based on the special attributes of trust in WSNs such as criteria analysis for trust system, reduced intricacy of formulae and balance period of trust credibility (Yu et al., 2012), distinct difficulties exist in establishing a trust structure in WSNs by choosing the ideal approach.

1.6 Objectives

The key objective of this study is to design an improved LEACH-C protocol for WSNs that secures network by providing external and internal authentication to nodes identified as malicious as well as new nodes requesting for connection.

Specific: The specific objectives for this work are listed below as;

- ✓ To determine and also isolate destructive nodes using genetic algorithm.
- ✓ To integrate Biphase Authentication Scheme with LEACH-C approach.
- ✓ To deliver packets of data from source to destination node in trusted manner.
- ✓ To boost the lifetime of a WSNs.
- ✓ To reduce source to destination data packet delivery delay.
- ✓ To minimize power usage at the node level.

1.7 Research questions

As a method of offering remedies to security difficulties faced by network utilizing LEACH-C protocol to route data packets, the research study attempts to respond to the following questions:

Q1. How can Biphase Authentication Scheme secure mechanisms be merged into LEACH-C?

Q2. How to identify safe path for reliable data packet transmission using genetic algorithm?

Q3. How can one reliably secure LEACH-C without heavily impacting its primary goal of lowering energy usage and enhancing network lifetime?

Q4. Is it possible to reduce network traffic by identifying and authenticating suspicious nodes?

1.8 Expected outcome

This research work is expected to influence the academics and research works that consider developing safe and secure protocols in wireless networks. Consideration of secure routing in WSNs promotes quality network services across various reputable applications. The following will be accomplished on the basis of integrating LEACH-C and Biphase Authentication Scheme:

1. Secure version of LEACH-C that:
 - a. Protects WSNs against DoS attacks.
 - b. Minimize unnecessary network traffic.

2. Safe LEACH-C approach that maintains the main objectives for original LEACH-C which include:
 - a. Decreasing node energy intake.
 - b. Improving average network lifetime.
3. A survey paper that influences scientists to take notice of the need for securing cluster-based routing algorithms as popular algorithms.

1.9 Thesis contributions

In this thesis, a cluster-based approach as well as a lightweight scheme, namely LEACH-C (Low Energy Adaptive Cluster Hierarchy Centralized) and also BAS (Biphase Authentication Scheme)' have actually been combined to provide power effective as well as trusted data delivery in WSNs. The validated LEACH-C procedure has actually been tailored to detect nodes that illegally joined the network. Security is a vital aspect in every network hence this contribution of this research. Through this piece of work, the network life time will increase considering that the protocol will disjoin fraudulent nodes. Low duplication of messages will be experienced due to sidelining malicious nodes.

1.10 Motivation

The motivation in WSNs centre on the fact that it is a continuing research field in today's computation science as well as telecom. The implementation of security in wireless clustering network approaches is currently defined with minimum network delays and low energy usage during data transmission and aggregation. The stipulated motivational points influenced selection of Low Energy Adaptive Clustering Hierarchy Centralized as focal approach for this work. Also, hierarchical-routing using LEACH-C is subjected to less, but then again very important limitations such as security problems.

1.11 Thesis outline

This research is structured into five chapters. Whereby Chapter 1 initializes aims of research. Chapter 2 explores relevant literature from various source of information that enabled for a comprehensive research. Chapter 3 describes complete methodology used to implement BA-LEACHC protocol starting from node deployment to comparative analysis. Chapter 4 describes full procedure followed in the proposed study. Also, Chapter 5 offers result discussion based on

MATLAB simulation, and lastly thesis summary and scope for future researches and investigations in the same field.

CHAPTER 2

2. Literature review

The necessary in-depth literature survey to get initial knowledge and study scope for securing LEACH-C through utilizing Biphase Authentication Scheme with genetic algorithm is discussed in this chapter. This chapter offers review of literature for mother protocol (LEACH) and its variant (LEACH-C). This review provides clarification in similarities and variations of the two protocols since LEACH-C is modified from LEACH to reduce node energy exhaust. Moreover, possible threats are identified for this hierarchical-cluster-based protocols. The chapter also discusses Genetic Algorithm (GA) and its applications in WSNs. Furthermore, the section looks on recent WSN security schemes that can easily integrate with LEACH-C for possible adoption of authentication process. Lastly, it touches on the discussion of recent existing secure LEACH-based routing protocols and section summary respectively.

2.1 LEACH protocol

(W. B. Heinzelman et al., 2002), (W. R. Heinzelman et al., 2005) presented hierarchical structured protocol for wireless networks, named LEACH (Low Energy Adaptive Clustering Hierarchy). This approach divides network participant sensor nodes in to clusters and each cluster has single CH. CH puts together and also compress details obtained from corresponding nodes then forward to sink. If a node was picked as the CH, the node will experience high power consumption as compared to member nodes; this may results from CH prerequisite to send data packets to data centre which might be long distance apart. This protocol utilizes random rotation in sensor nodes selected as CHs to equally dispense energy across network. All LEACH and its variants follow a hierarchical structure as shown in Figure 2.1.

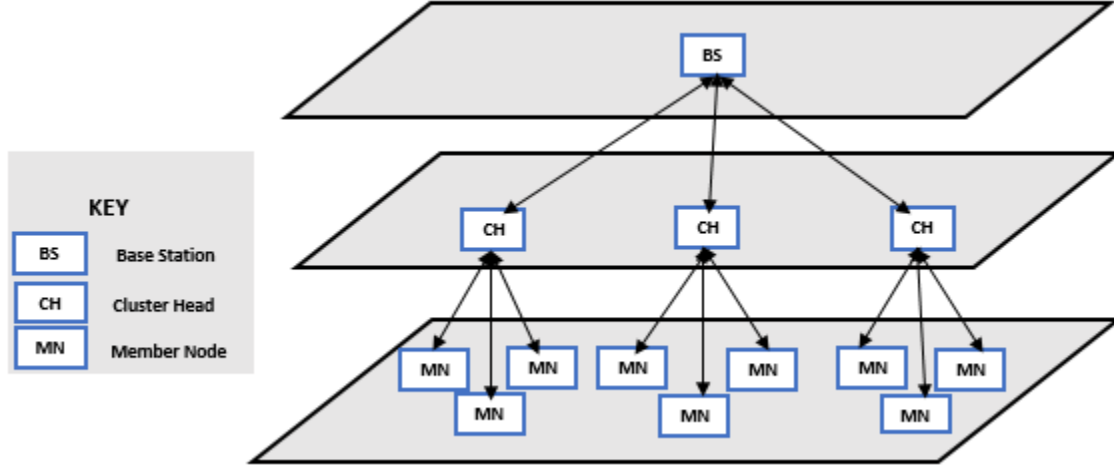


Figure 2. 1: Hierarchical structure

2.1.1 LEACH operation

This approach executes in two phases which are Setup phase and Steady phase

i) **Setup phase:** Throughout this, a selected quantity of nodes, y , pick themselves as CHs. The self-selection is done in accordance to the threshold value, $TT(n)$. This value is dependent on set percentage for qualifying node to become CH, $-y$, in the present round r , as well as the collection of nodes that failed to meet requirements of becoming CH in the last $1/y$ rounds, which is represented by GG . The formula is given below:

$$TT(n) = 1 - y \left[r \bmod \left(\frac{1}{y} \right) \right] \text{ if } n \in GG \quad (2.1)$$

$$TT(n) = 0 \text{ otherwise}$$

All nodes intending to become CH selects a value, that lays between zero and one, if the selected value is smaller than $TT(n)$, then that means successful CH selection for current round. Each chosen CH distribute advertisement message across the network recruiting ordinary nodes to become part of the cluster. Ordinary nodes take part as cluster members depending on announcement message signal strength. CHs receive a recognition message from non-CHs nodes as a notification that message will be collected from the same. After obtaining recognition message from corresponding member nodes CHs creates a Time Division Multiple Access schedule to specifically allocate time length to each node, stating when to send collected packets of data. LEACH setup is depicted in Figure 2.2.

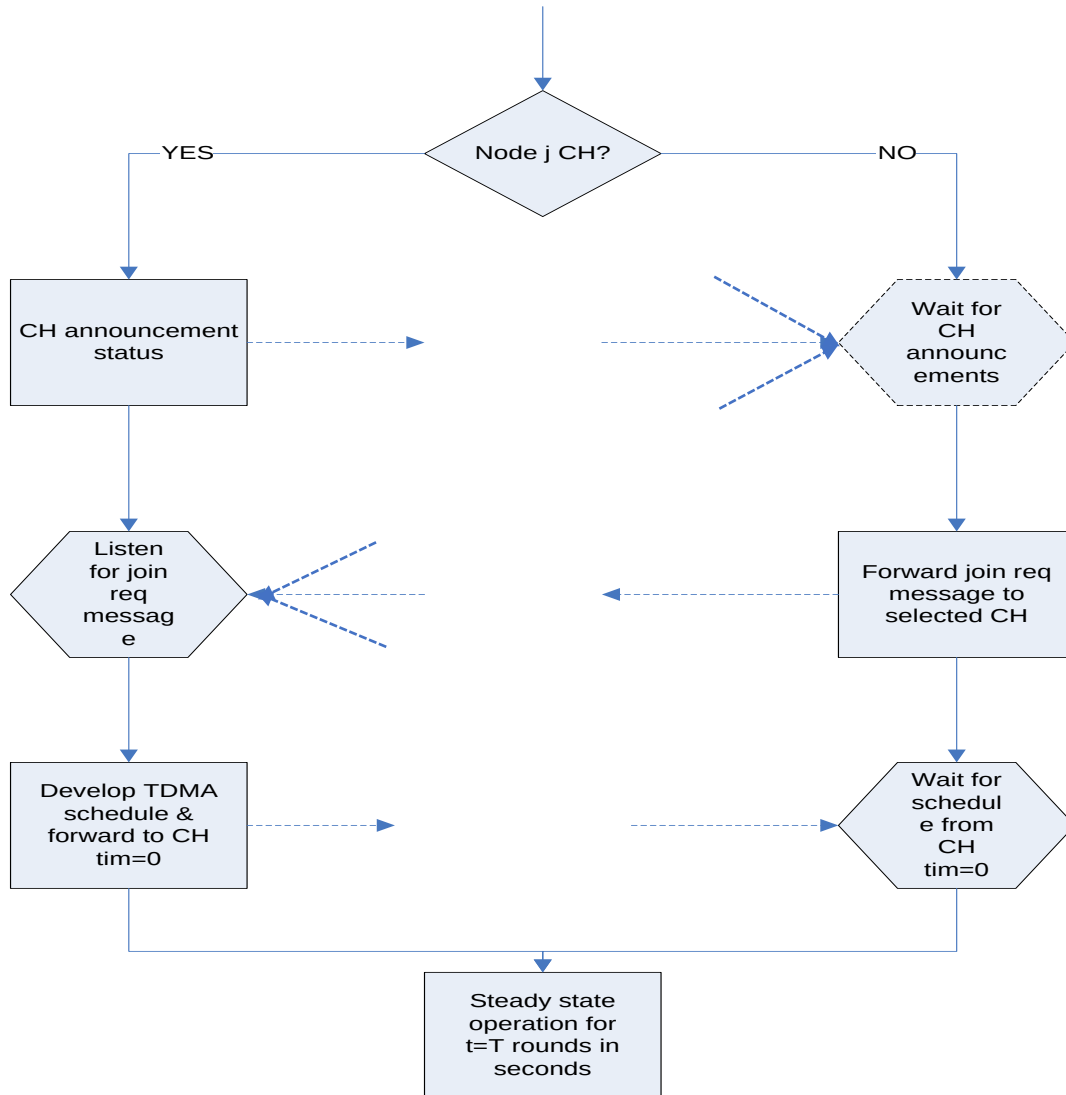


Figure 2. 2: LEACH approach setup

ii) Steady state

Throughout this phase, member nodes (MN) begin sensing data as well as sending it to corresponding CHs basing upon created TDMA schedule. CHs receive sensed data from participant nodes, then that data is summed up and forwarded to data centre or BS. After execution of this phase the protocol returns to setup stage where some member nodes stand a chance to become CHs. To avoid sensor nodes interfering with neighbouring clusters, each cluster communicates through the utilization of unique CDMA codes/slots. The LEACH steady-state phase is depicted by Figure 2.3.

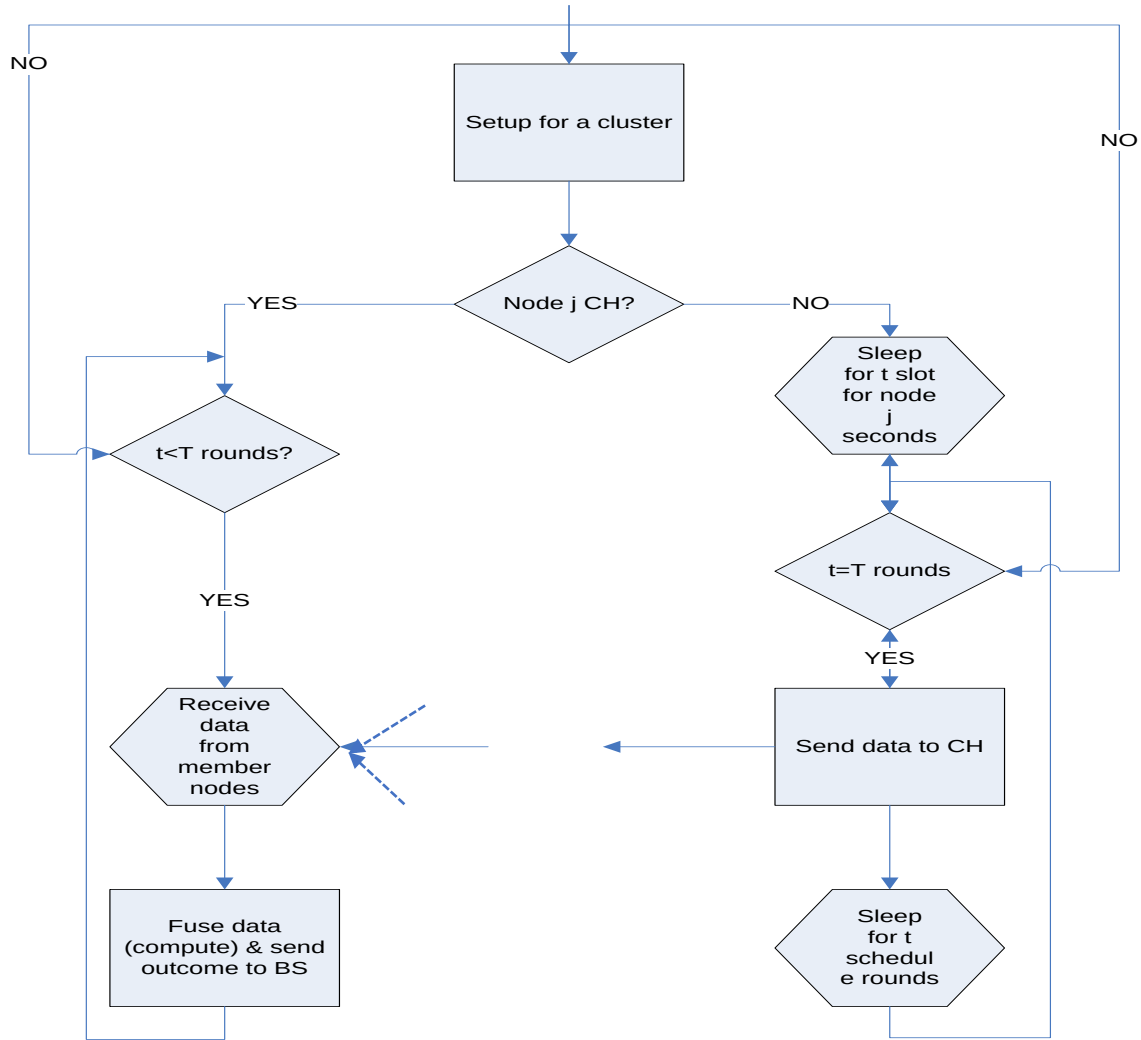


Figure 2. 3: LEACH protocol steady-state phase

2.2 LEACH-C approach

It applies a centralized approach whereby important decisions like selecting CHs, building clusters and distributing crucial network information is carried by sink. This approach creates good clusters by selecting CHs across or throughout area of node deployment. Phase 2 of this approach is fully executed by sink hence resulting in low usage of energy when forming clusters. LEACH as well as LEACH-C follows the setup process. In every round during LEACH-C execution setup phase requires each node to send their position and residual energy to sink. GPS (Global Positioning System) is used in acquiring node position and remaining energy. Building better clusters in LEACH-C depend on equal distribution of energy across sensor nodes. Sink computes average energy for each

nodes, and any node with energy value smaller than set average value is restricted joining cluster head selection process. Sink produces optimal clusters H , from nodes with energy value more than set average energy value utilizing simulated annealing approach for the process. Average node energy is computed by equation 2.2.

$$E_{avg} = \frac{\sum_{j=1}^M P_j}{M} \quad (2.2)$$

Where P_j is recurring power of j th node and also M signifying sensor node range. In situations having geographical area $A \times A$ with M nodes evenly distributed across network, equation 2.3 will be used to compute H .

$$H = \sqrt{\frac{M}{2\pi} \frac{\epsilon_{fs}}{\epsilon_{mp}} \frac{R}{dis^2tobs}} \quad (2.3)$$

Where dis^2tobs symbolise distance in between sink and CH. ϵ_{fs} represent broadcast parameters while ϵ_{mp} denotes circuit receiver. The simulated annealing algorithm shortens area coverage between sink and CH hence leading to low energy consumption in a cluster. The broadcasting of advertisement message involving CHs selection and cluster formation resumes soon after ending current process. Sink distributes CHs identity to all network participant nodes, and in case CH identity matches member node identity, then it stands a promotion chance as CH. CHs transmit the TDMA schedule to all member nodes belonging to their clusters. Data transmission begins across network clusters basing on the broadcasted TDMA schedule. In central LEACH, the full procedure is taken care of by the BS, so it is quite energy effective which is in contrast to LEACH. For location details, every node needs support from GPS which is a pricey gadget and also takes in additional power (W. B. Heinzelman et al., 2002; Zhao et al., 2012).

2.2.1 Possible security challenges in LEACH-C

As discussed in the introductory chapter, that clustering approaches are concerned with intelligent node grouping which promote communication using low energy. LEACH-C as base protocol for this

study experience inside and outside attacks during phase one execution process. Usually, with zero security application mechanisms, LEACH-C may go through the following attacks;

- ✓ Bogus node might self-present as cluster head through communicating announcement message across network.
- ✓ An intruder can connect to a cluster during setup execution and deny genuine nodes from sign up.
- ✓ An intruder might accomplish information concerning the member nodes and also cluster head from clustering process.
- ✓ An intruder might try to disturb the clustering process through launching denial of service attacks.

2.3 Genetic algorithmns (GAs)

The Genetic algorithms capabilities include solving complex problems as indicated by previous studies, ranging from numerical to business optimization problems. This type of algorithms follow 'survival of the fittest' principle whereby a fitness value is assigned per solution problem. GAs are different ranging from optimizing to decision-based algorithms, based on their fast evaluation and convergence abilities. The utilization of GAs in newly established network protocol and other computer systems is on the rise, and that requires optimization of parameters. This algorithm is a stochastic technique introduced in 1958 by *Charles Darwin*. The modelling of GAs is based on the ideology of evolution through natural selection and employability of individual population. The purpose of fitness function is to simply evaluate individuals, and the reproduction of offsprings will vary according to fitness value. A genetic algorithm also holds to a population of n solutions (chromosomes) corresponding to specific fitness value.

2.3.1 Genetic algorithm process

The selected parents mate based on their fitness and produce offsprings through a reproductive plan. Subsequently, for offsprings to inherit parents features, high reproduction chances are given to high fit solutions. Since the size of the population is kept static extra space is set aside to cater for offsprings resulting from parents multiplying. The death of individuals from population means

automatic replacement by the new chromosomes. This may result in creation of a new generation if parents from an older population cannot reproduce. As generations succeed each other, best solutions prosper and minimum fit solutions perish. New generation solutions are an improvement of previous generation solutions as they contain improved genes on average rate. Finally, when a population is producing offsprings same like in previous generation, the algorithm is said to have met the target solutions for solving the quantified problem. Figure 2.4 shows fitness based selection (Tabassum, 2014).

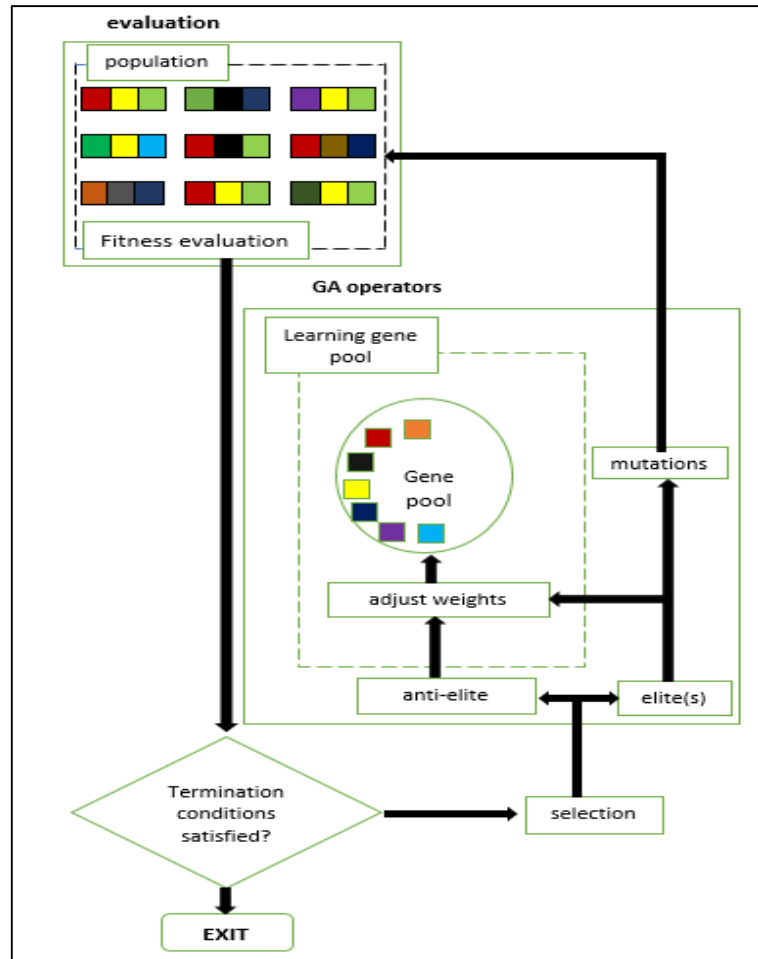


Figure 2. 4: Fitness based selection

2.3.2 Genetic algorithm operators

According to (Abirami & Priakanth, 2014), (Rahmanian et al., 2011) this algorithm evolves via three operators, immediately after generating initial population randomly. The operators are briefly discussed as follows in a sequential order:

Selection: It enables better individuals to pass genes to the imminent generation. The fitness value pertaining to an individual determines the goodness, while the objective function determines fitness.

Crossover: This operator enables for mating among individuals. The selection operator selects two individuals from the population for mating. Random selection of crossover point along bit strings takes place, and the exchange of value per string occurs up to the stipulated point. As parents mate new offsprings are created and passed on to the imminent generation of population. Good portions of individuals in previous population are recombined for creating better individuals for next generation.

Mutation: The initialization of random modification is through this operator. Mutation is responsible for maintaining population diversity to avoid early convergence. Some new individuals may experience flipped bits as a result of low likelihood. The absence of crossover operator result in a parallel and a noise-tolerant algorithm.

Genetic Algorithm Pseudo Code:

Phase1:- Random generation of introductory population $W(0)$;

Phase2:- Calculate and store fitness $f(w)$ per individual w in the present population $W(y)$;

Phase3:- Define selection likelihood $p(w)$ per individual m in $W(y)$ such a way that $p(w)$ is related to $f(w)$;

Phase4:- Generating $W(y+1)$ via the likelihood of selecting individuals from $W(y)$ so as to produce offspring through following selection, crossover and mutation.

Phase5:- Phase 2 is repeated until obtaining a substantial solution.

2.3.3 Application of GAs in WSN design

Several research works in wireless sensor networks adopted the use of genetic algorithms for optimization purposes. The use of GAs in designing WSNs was successfully implemented in many studies and laid foundation for other related works with the same approaches. Below are the few selected GA based algorithms:

(Deshmukh et al., 2016) recommended a clustering approach with WSNs using GA. The key goal for Deshmukh approach is to minimize energy consumption and ensure network load balancing. The GA in this protocol selects optimal path for better routing and minimal power usage. (S. P. Singh & Sharma, 2018) has presented GAEEC (Genetic Algorithm Based Energy Efficient Clustering) for WSNs. Genetic approach for GAEEC operates on two phases with dissimilar parameters and operators for optimized clustering. This approach provides improvement for cluster head selection as it picks the best CH in each cluster based on current residual energy. GAEEC out performs LEACH when compared looking at throughput as well as usage of energy. (Baranidharan & Santhi, 2015) proposed GAECH (a Genetic Algorithm based Energy efficient Clustering Hierarchy) for WSNs. GAECH fitness function exits to deal with Half Node Die, First Node Die as well as Last Node Die. Fitness function in this approach enable for creation of well-balanced clusters through considering essential cluster parameters.

When applying genetic algorithm into a problem, three basic steps are considered; first representation of the problem (this means converting candidate solution to genotype which can be easily manipulated and evolved by a genetic algorithm). Secondly, fitness function formulation pertaining to each individual (imaginable solution to the stipulated network problem), and lastly selection of genetic operators and proper mechanism for implementation.

2.4 WSN secure schemes

This section of literature review discusses three recent wireless sensor network security schemes. The adoption of hierarchical structure and their ability to isolate malicious nodes by these three security schemes motivated our selection. The authentication techniques proposed by the schemes seemed to be able to fit well since we intend to address security problems in a cluster-based protocol that follows hierarchical structure (LEACH-C). This work provides basic concepts of applying authentication techniques in wireless networks.

(Riaz et al., 2017) presented a new approach named BAS which provides initial small scale authentication to new nodes connection requests. IEEE 802.15.4 defines 2 major WSN gadgets

namely: Full and Reduced function gadgets. In this scheme, FFD (full function devices) symbolise authenticating SNs (Sensor Nodes) while RFD represent network ordinary node and NN signifying new node. Figure 2.5 shows BAS procedural diagram indicating initial to final authentication stages.

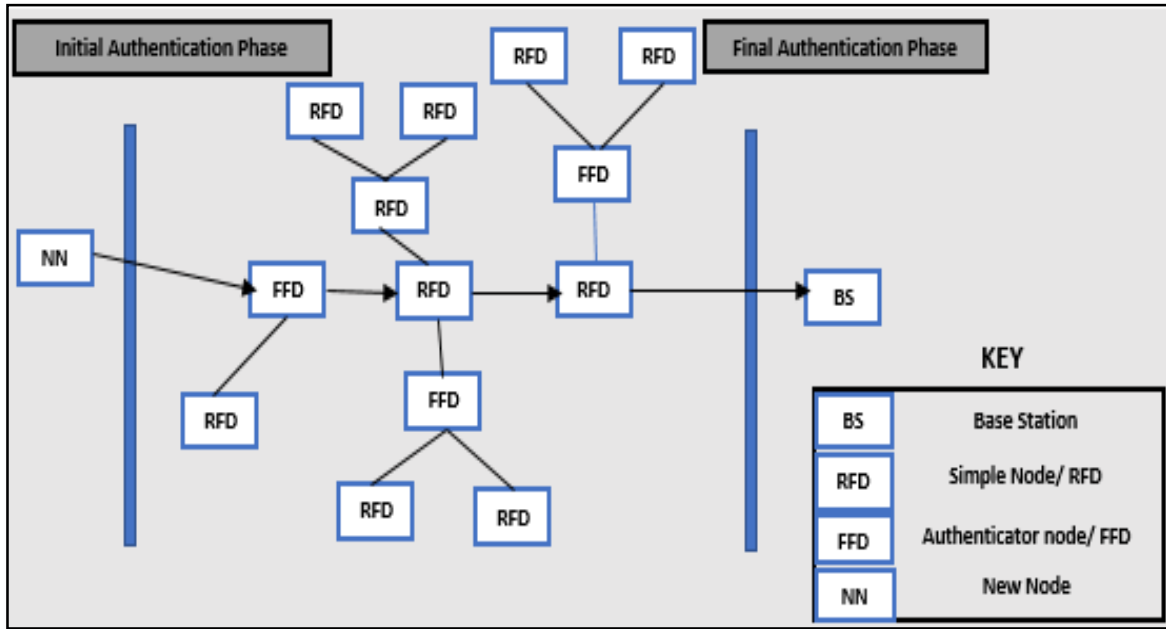


Figure 2. 5: BAS procedure diagram

Initial phase: - This phase works through utilizing a node with authentication capabilities. New node with interests of joining network sends request through FFD which acts as a gateway. FFD also has capabilities of blocking request messages from suspicious node or NN depending their conversation. Successful conversation between NN and FFD means request messages forwarding to BS for further interrogation in final phase.

Final phase: - It is mainly executed in the BS, whereby BS compares identity and key pairs received from FFD node in its database. If identity and key pairs match novel node will be granted access to the network.

In Biphase Authentication Scheme, the first step is the identification between the two hops and then identifier node contains the required phase, whether hop *B* is the original node and connection between the system networks. The steps are as follows:

$$\text{Step 1} \quad P_1 = B \rightarrow BM: [JD_B] \quad (i)$$

Basically, in step 1 sensor node transfers its id ($[JD_B]$) to authenticate sensor node.

Where equ. (i) P_1 is a receiver (message), B is an initial node and a BM authentication node.

Step 2: Identifier hop node gets the data message P_1 from the B and evaluates the following methods:

a) It computes the encoded key (k_p) Utilizing the unsystematic selection T and generating key approach in equation (i).

b) Sending the similar to initial node B

$$P_2 = BM \rightarrow B: [T] \quad (ii)$$

Step 3: The hop node B is identified as an operator and has the main or a master key (k_{Master}), Utilizing random data T and generating key approach.

Step 4: The node B connects k_p to identify node BM .

$$P_3 = B \rightarrow BM: [k_p] \quad (iii)$$

Step 5: Identifier node gets P_3 from B and presents the desired functions,

Selecting the k_p Where the actual data satisfy desired value and data to hop B based on identification method.

$$P_4 = BM \rightarrow B: [In\ process] \quad (iv)$$

b) When the hop B get the data P_4 from identifier node that forward the identifier hop to the controller.

Step 6: When the node B gets the data P_4 from identifier node that forwards the paired key K_{MC} to identifier hop.

$$P_5 = B \rightarrow BM: [K_{MC}] \quad (v)$$

Step 7: Authenticator node transfers node B request to Data Center (DC).

$$P_6 = BM \rightarrow DC: [JD_B, K_{MC}] \quad (vi)$$

Last authenticate performs with the help of DC and consists the following step.

Step 8: DC gets a reply from authenticate node, it decodes message, verifies K_{MC} and JD_B delivered by authenticate node and compared with saved values in data set.

If verification done, then novel sensor node is proved and accept message is transfer to authenticate SN (Sensor Node).

$$P_7 = DC \rightarrow \text{BM: [Approved]} \quad (\text{vii})$$

If verification is not done and then

$$M_8 = DC \rightarrow \text{BM: [not approved]} \quad (\text{viii})$$

Step 9: Authenticate sensor node only transfers message to node B .

$$M_9 = \text{BM} \rightarrow B: [\text{Accepted}] \quad (\text{ix})$$

If the message is rejected, the authenticate sensor node will not transfer it to B node.

(Zawaideh & Salamah, 2019) presented WT-MND (weight trust-based malicious node detection) which is an approach for detecting bogus sensor nodes in WSN applying efficient weight trust. The nodes in this approach account for false-positive and false-negative cases. The effectiveness of WT-MND relies on the ability of trust-based process to recover half dying nodes from malfunctioning. Depending on node behaviour WT-MND computes multiple trust-update factors for each node. The scheme also, has higher DR (Detection Ratio) and lower MDR (Mis-Detection Ratio) which increases its scalability and effectiveness. Detecting and isolating malicious nodes in WT-MND is achieved through four major components. Below is an explanation of the components.

Indirect trust (IT) calculation: - In this component, a selected CM (cluster member) forwards direct trust values of other CMs to corresponding CH in each round. CHs in every cluster computes AT (average trust), indirect trust and weight of all network CMs.

Isolating malicious node: - In this component, indirect trust value calculated for cluster members is compared to preset MAT (minimum acceptable trust) value by CH. If indirect trust value is less than MAT node is considered malicious and removed from the network. If not, node is admitted as normal node. The minimum acceptable trust value is among 0 and 1.

Trust-update factor computation: - In the first 4-time division multiple access (TDMA) frames of every round CM forward sensed data to corresponding cluster heads. Cluster heads perform data aggregation on sensed data and monitor the behavior of each cluster member. The behavior monitoring is archived by keeping record of occurred errors during data transmission by CMs. Cluster heads will then, compute trust-update factor (TU) for corresponding member nodes based on recorded errors. TU computed through equation 2.4.

$$TU(i) = 1 - \frac{err(i)}{2*N} (i = 1 \text{ to } j) \quad (2.4)$$

Where N represent count of TDMA frames per round: At the end, in every round CHs forms TUV (trust update vector) as $[TU(1), TU(2), \dots TU(j)]$. The falsified information of MNs reduces their $TU(i)$ values.

Direct trust (DT) updating: - Cluster heads broadcast trust update factors, so that each node updates its TV. The TV (trust vector) is updated by multiplying old direct trust values with matching TU (trust update factor) as displayed by equation 2.5:

$$TV_{(l)update}[j] = TU(j) * TV_{(l)old}[j], (l = 1 \text{ to } N)(j = 1 \text{ to } N) \quad (2.5)$$

(Tseng et al., 2007) suggested IDUAS (Improved Dynamic User Authentication Scheme) that provides authentication in order to win the defect of user authentication scheme. It does this by providing fight contrary to forged and reply attack. It's an enhanced version that authenticates users before joining network. In this scheme, users are able to change passwords easily and it's possible to join network via various member nodes. No additional computation is needed in the scheme. This approach executes in 4 phases; authentication, password changing, registration and lastly login. IDUAS and User Authentication Scheme phases follows same execution except changing password phase. During changing password phase, if a user wants to make changes to the password, will send identity, previous hashed and current passwords to entry node. Immediately after receiving password change request message, authenticator node confirms user identity and sent hashed password for correctness. In a case where the hashed password is incorrect or ID not found in the database, then send access denial message. Authenticator send changed password message to the user for correct hashed password. It provides better security compared to user authentication scheme. Unfortunately, it is prone to various threats such as compromised node.

2.5 Secure variants of LEACH

(Rohbanian et al., 2013) recommended Watchdog-LEACH that incorporates unique safety mechanisms to LEACH protocol to ensure network safety. Watchdog-LEACH uses spontaneous watchdog approach which is implemented before steady phase. Moreover, it uses decentralized

intrusion detection technique in setup for detecting possible network interruption. Watchdog LEACH phases are as follows:

Setup Phase: - This phase executes in the same manner like in LEACH protocol, yet watchdog LEACH enables watchdog nodes to detect any possible intrusion.

Watchdog node Selection phase: - This phase is responsible for appointing watchdog nodes and it utilizes a spontaneous watchdog approach. Each sensor node has a tracking module that is triggered upon successful nomination as watchdog. If node picked as a CH in previous phase, thereafter it's not allowed to contest for watchdog selection. Equation 2.6, 2.7 and 2.8 depicts watchdog selection formula:

$$f(c, d, m) = \frac{PRB_d^{d-c,c} \cdot (m-1)^{d-c}}{VR_{m,d}} \quad (2.6)$$

$$PRB_d^{d-c,c} = \frac{d!}{(d-c)! \cdot c!} \quad (2.7)$$

$$VR_{m,d} = m^d \quad (2.8)$$

Where, $PRB_d^{d-c,c}$ is the formula of permutation with repetitive aspects: $VR_{m,d}$ is the formula of r-permutations with repetitive aspects, d is the variety of nodes that could activate their tracking module to be watchdog (i.e., the number of nodes that are going to toss a dice), and m is the variety of nodes that are going to influence on the chance of turning on the watchdog nodes, usually equal to d (i.e., the number of sides of every dice).

Steady state and intrusion detection phase: - this phase in Watchdog-LEACH resembles Steady phase in LEACH protocol with some variations. Watchdog nodes do not sense setting signals rather they strictly serve the purpose of being watchdog and keep track of cluster interactions for both non-CH nodes and CH.

Breach detection: Watchdog nodes are independent from CHs so they additionally keep track of CHs behaviour. Throughout Steady phase, watchdog nodes pay attention to interruptions and also when malice is found, an alert is forwarded to BS. After each round, a notification message is sent

to each genuine node about suspicious nodes. This will result in rejection of messages from such nodes by genuine nodes.

(Alshowkan et al., 2013) introduced LS-LEACH (Lightweight secure-LEACH) which presumes that five percent from overall network nodes is dedicated to CH selection. Soon after each round and initial node deployment, CH selection begins. The new CHs selection is based upon higher amount of remaining power. The pre-selected CH notifies the BS about the credibility of the elected CH. The message from the CH to the BS is secured by message authentication code algorithm which shares the secret key between the BS and the CH. Afterwards, the BS transmits the list of the authenticated CHs to all nodes utilizing uTESLA. After broadcasting the list authenticated CHs, nodes start forwarding joint request to the nearest CHs. The appointment of CH ought to be based upon the range between the node and the cluster to decrease the energy needed when exchanging messages.

Election: -The CH election for upcoming round transpires in advance during current round. Nodes are chosen as CHs when having more power remaining than in other nodes ($S_i > energy_S_i$). Moreover, CHs need to have a strong signal with BS ($S_i > signal_S_i$).

Connection: -After successful selection of new CHs and alert to BS, the BS announce to each node about newly elected CHs. CH connect exact number member nodes prescribed per cluster ($S_i _ 30 S_i$). Furthermore, nodes ask for sign up with clusters on close range to minimize energy consumption during sending and receiving ($New_CH > signalNew_CH$).

Transmission: -Nodes follow three phases during operation: sensing, sleeping and also listening/transmitting. Transmission occurs when the sensor nodes are sensing the atmosphere. Moreover, it occurs when nodes are expecting to have interactions with the CH or BS. Sleeping takes place when the nodes are on sensing or listening modes. It is required for the nodes to be in sleep mode to prevent overhearing which consumes more energy. Nodes are also required to be having logs for the connections attempts that were linked to during initial stage. When the attempts get to a predefined threshold, an alert is sent to the CH and the BS. The BS has to follow the right procedure when the node is under attack.

(Kumar & Umamakeswari, 2016) presented SS-LEACH (Specification based secure LEACH protocol as one other safe variant of LEACH. It selects cluster heads based upon the remaining power and distance in between nodes. It follows three phases.

Phase one (Key pre-distribution formation): -This phase includes initialization of key pool and randomly selecting m keys in order to form key-ring per node prior to network placement. Threats like selective forwarding and others are managed through utilizing key appropriately.

Phase two (node self-location): -This phase gives chance to all network nodes to calculate coordinates aided by map growing algorithm. The base station coordinates are set to $k(0,0)$ as well as two referenced nodes c and also w selected to create a triangular. Sensor node c will be set to $c(e, 0)$, after that the coordinates of the node $w(x_w, y_w)$ can be acquired through equations 2.9 and 2.10.

$$x_w = \frac{e^2 + f^2 - g^2}{2e} \quad (2.9)$$

$$y_w = \pm \frac{\sqrt{(-e+f-g)(e-f-g)(e+f+g)}}{2e} \quad (2.10)$$

Node k , w and c broadcast corresponding information to various other nodes. In a case whereby other nodes share pairwise keys with k , w and c , the information will be parsed and stored across neighbouring nodes. BS stores coordinates pertaining to all nodes in the monitored area and that improves the security of the network.

Phase three (Periodicity): - is duplicated every round and entails 3 components: selection cluster heads, establishment of dynamic stochastic multi-paths cluster heads chains as well as steady information distribution. In this protocol, the initial cluster head is chosen by BS. BS transmits corresponding routing information and coordinates across the network and only nodes with relevant paired key will use as well as calculating space to reach base station basing on own coordinates. Node i sends back transmitting details with Q_i as well as H_i, k to BS. Or else, the node is refused to sign up with the network. $TT(n)$ represent node c chance to become first CH.

$$TT(n) = \frac{p}{1 - p * \left[rmod\left(\frac{h^1}{p}\right) \right]} * \left[a^Q c / Q_0 + (1 - a) H_{ci,k} / H_{max} \right] \text{ if } i \in G \quad (2.11)$$

0 otherwise

Where Q_0 representing node preliminary power. Q_c representing residual power in c node. The lengthiest broadcast distance in all nodes signified by H_{max} . H_c , k is the range between node c as well as BS. BS makes a comparison of all $TT(n)$ corresponding to its one-hop neighbouring nodes as well as selecting a node to be initial CH. The selected initial CH establishes its own $TT(n)=0$. Similarly, CH two selection process executed through initial CH. During the creation of vibrant stochastic multi-paths CHs chains, every CH communicates its purpose across network and also selects one from its members to represent as standby cluster head. Ordinary nodes elect specific cluster for connecting through grounded by signal strength and pairwise keys. After that each CH including on-standby CHs create dynamic stochastic multi-paths CHs chains. Finally, in steady information distribution phase, CHs hang on to receive data packets from participant nodes while in the meantime forwarding received data to sink.

2.6 Summary

In this chapter, BAS is described as one modern best authentication scheme that consumes less energy and requires less memory to operate. Therefore, it can fit well on/ with LEACH-C to tackle internal and external attacks for the safety of the network. The genetic algorithm have capabilities to help cross examine node path for safety of data during transmission process. Discussed secure variants of LEACH proves authentication as preferred and capable method to deal with malicious nodes.

CHAPTER 3

3. Methodology

3.1 Adopted stages

In order to explain, predict and comprehend phenomena of this research the following three stages were followed:

i. Preliminary stage: - A comprehensive survey of literature was accomplished by visiting relevant journal articles, conference papers, e-books, internet sites and other relevant sources of information. Therefore, the acquired information helped the research with basic and conceptual information about cluster-based routing protocols and basic concepts on WSN authentication.

ii. Implementation stage: - This stage involved simulating and programming on MATLAB (R2015b), and to obtain accuracy confidence interval is taken into consideration. The nodes are deployed randomly hence taking into consideration a hierarchical structure. Wireless channel is measured since the deployed nodes are connecting wirelessly basing on range of transmission, distance and so on. Results from simulations indicates BA-LEACHC achieves much well when looking at network life time metrics, throughput and also preliminary power of network nodes.

MATLAB environment was introduced with the purpose of giving access to Linpack and Eispack without the learning FORTRAN. These are the linear and Eigen packages of system. In the technical world, everyday some kinds of advancements are introduced for this purpose, the technical computing is required in each field and it is fulfilled by using high level languages such as MATLAB. MATLAB is a new kind of language that consists of some inbuilt tools and it also supportive for the OOP concepts; such as C++, and others. MATLAB session is a small task which helped in learning basic concepts about MATLAB. It includes both starting and ending process. The simple steps are:

1. Log in.
2. Invoke MATLAB
3. Simple and Easy Calculations
4. Quit

The Figure 3.1 shows user interface of MATLAB (R2015b) screen-shotted during complete implementation and coding stages, which include problem implementation, solution implementation, result analysis and comparison of BA-LEACHC and other relevant variants.

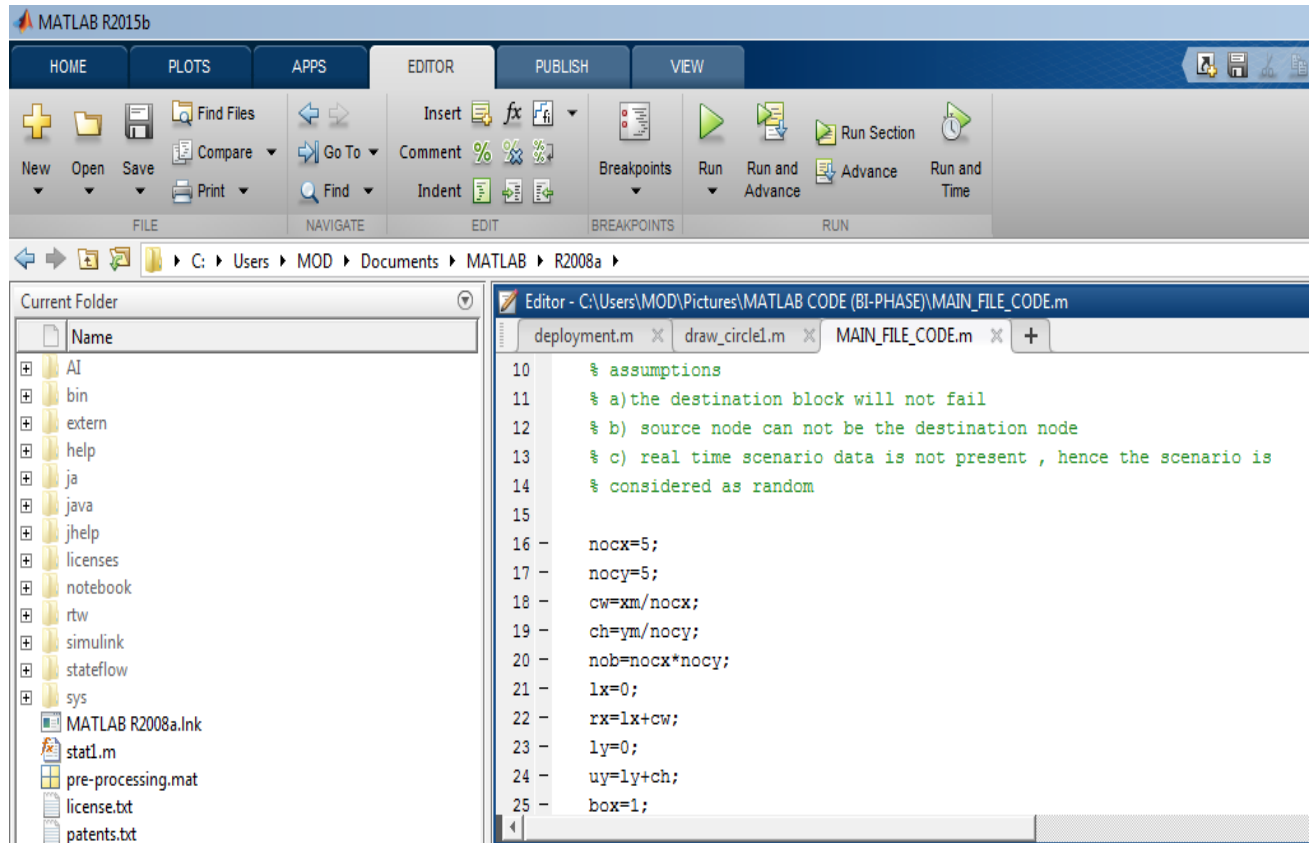


Figure 3.1: MATLAB (R2015) user interface

iii. **Testing stage:** - This stage entails analysing and comparing different network parameters.

3.2 Implementation methodology

The methodology for implementing the improved protocol which incorporates secure mechanisms of the Biphase Authentication Scheme is quite simple. In this contrast, we would be defining with authentication techniques in case of any failure occurrence while the transmitting data through a wireless sensor network. With BAS, we would be calling the objective function first for the other optimal path which would list down all those possible paths which may be included to transmit the data with the most possible least energy and the maximum number of data packets

transferred. There is a function named fitness function in which optimal techniques would figure out the best optimal solution for the transmission of the data through the LEACH-C protocol.

The ethical LEACH-C protocol would be configured as it is.

1. Firstly, node deployment takes place by entering the number of nodes values, length of network and width of the node in which implementation has been done.
2. Calculate location of x-axis and y-axis and time stamp of each node.
3. Time stamp of the nodes has been chosen as LEACH-C routing protocol.
4. Data transmission by nodes across WSN then attack comes and maximum energy consumed and overloading increases.
5. Starting of routing protocol:-

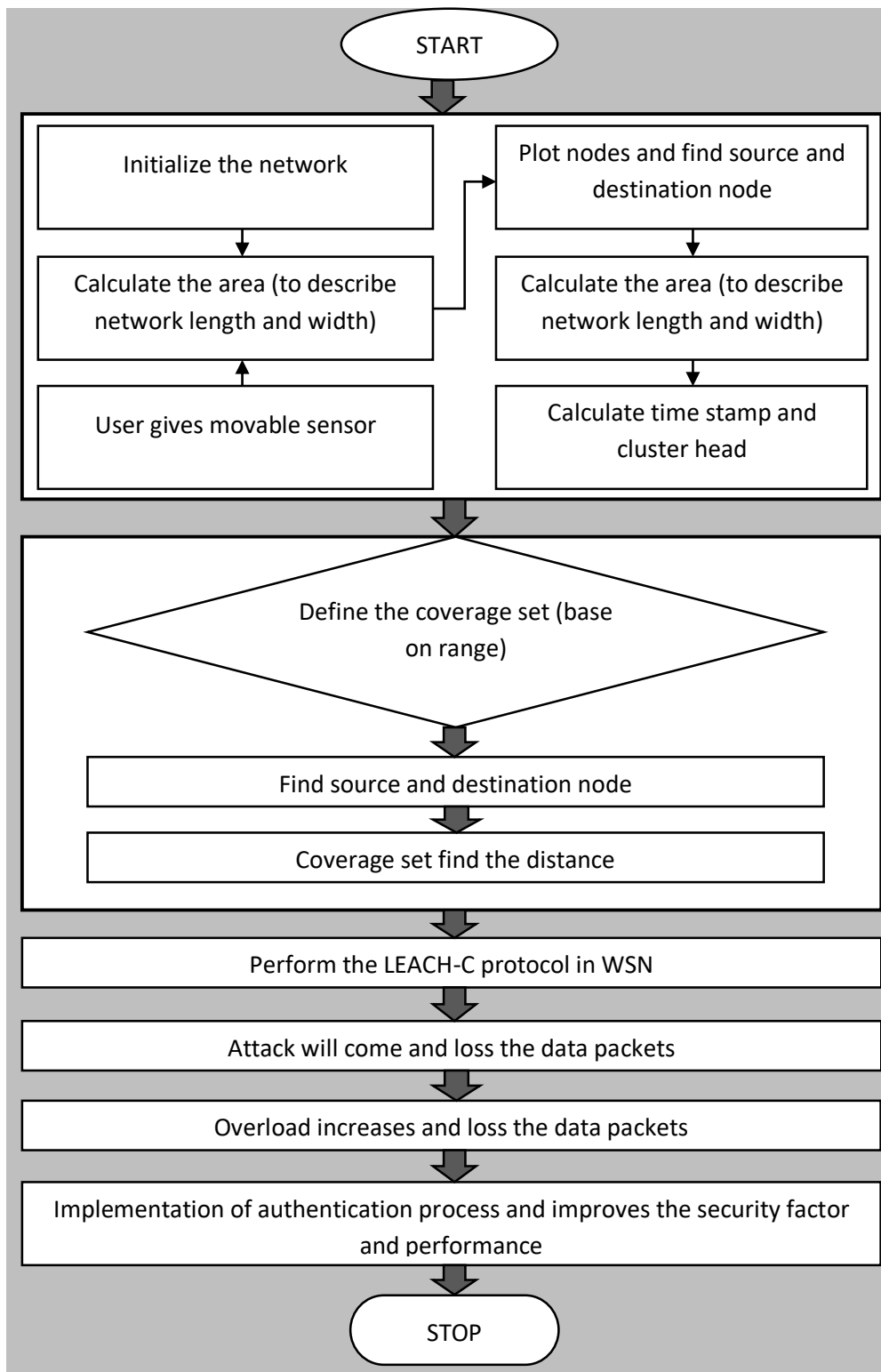


Figure 3.2: Flow chart of the proposed approach

Calculate time- stamp of node in first block to select cluster head.

Measure X and Y distance of network.

Find the coverage set between the nodes.

Checking of availability of destination.

6. Sending of data packets from source to destination.
7. Selection of any node from coverage set for setting of current nodes.
8. Checking of nodes till the 9th node.
9. Termination condition will apply if a node is not found between nodes nine.
10. Plot final route between sources and destination.
11. Then communicate the data from node to node across network after that attacker has come, delay increases, overload increases and high energy consumed in the network.
12. Implement a novel approach (LEACH-C) clustering algorithm to transmit the data packets one to another node.
13. Proposed approach to rectify and overcome the problems like reducing the energy factor, delay, packet loss and enhancing the secure factor.
14. Plotting of remaining nodes in the network.
15. Calculate performance metrics with proposed algorithm and comparison with the existing one.

3.3 Network scenario and parameters

In this work, researchers measured heterogeneous WSN, which is an approach whereby nodes under deployment do not contain the same energy. Suppose $m1$ function of nodes under deployment devise Alfa times extra energy compared to standard nodes, and whereby nn devise nodes quantity. Nodes with extra energy are referred to as advanced nodes. Hence,

Quantity of Standard Nodes = $(1-m1) * nn$.

Energy of Advanced_node = $e0 * (1+aa)$.

Energy of Standard nodes = $e0$.

Quantity of Adv_nodes = $m1 * nn$.

Therefore the summed network energy become equivalent to $((1-m1) * nn) * e0 + (m1*nn) * (e0 * (1+aa))$

The initial network simulation configuration stands as: -

- ✓ Network Area size: - 100*100 m.
- ✓ Number_of_Sen_nodes = 300
- ✓ Eneregy _per_node =1joules.
- ✓ Selection chances of node promotion to CH = 0.15.
- ✓ Size of message = 3000 bits.
- ✓ Five per cent of nodes devise twice over energy.

3.4 BA-LEACHC: Proposed work

For initial simulation of all the 300 nodes, each starts with 1Joule of energy which reduces as the node gets engaged in the network. The node engagement refers to transmitting, receiving and aggregating of data by a sensor node. We track the current_total_number of live nodes (CurTn) on every round starting on the second round. Moreover, a record is also kept for the previous_total_number of live nodes (PrevTn); that is immediate quantity of live nodes before current recorded total number of nodes. This enables for often checks on suspicious nodes or increase of nodes in the network. If $CurTn > PrevTn$, the authentic scheme modelled on cluster heads gets activated as the cluster head fails to transmit data, hence calling for optimization technique (objective fitness function). The objective fitness function determines safe path for data transmission. The cluster head connecting suspicious node reveals through network overloading and less delivery of packets of data from sender node to receiver node. In a situation whereby CurTn is less than equals to PrevTn network ignores, the assumption is that the number of nodes decrease due to node energy depletion (death of nodes). Else if CurTn is equals to PrevTn means steady quantity in deployed nodes and that results in healthier network. The Figure 3.3 shows a summary of our proposed work.

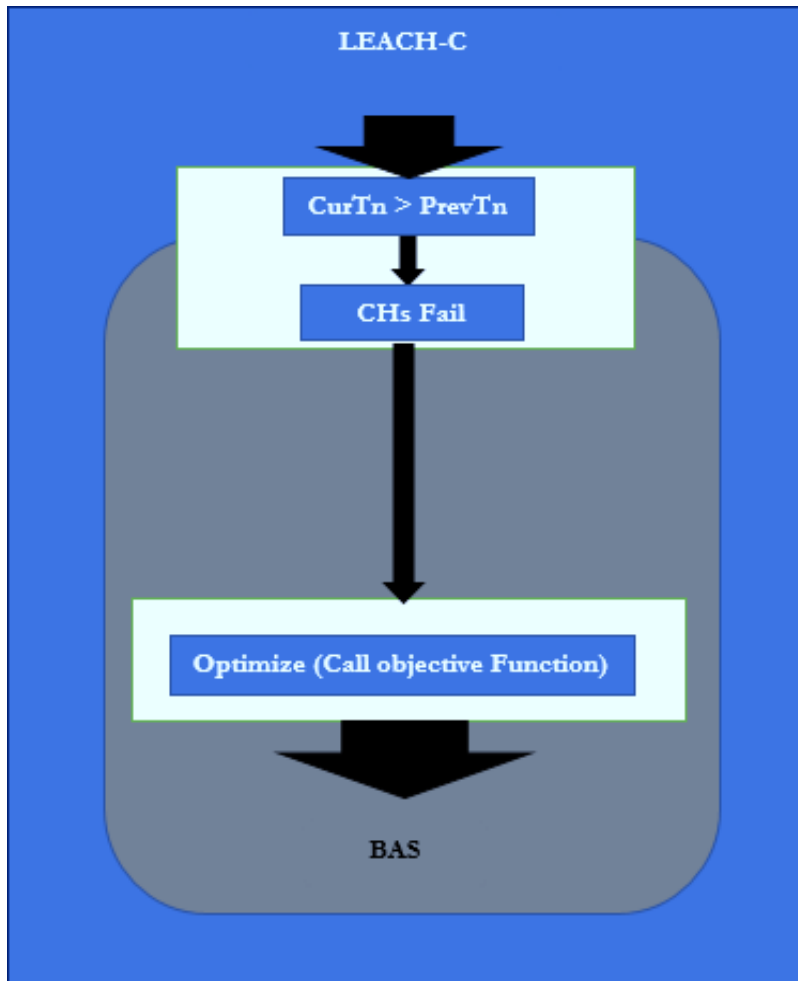


Figure 3.3: BA-LEACHC summary diagram

The space among the controller and cluster head is the central hop node that helps in decreasing the data for every cluster head in BA-LEACHC protocol. The lifetime of the protocol is enhanced by increasing the security of the protocol. During the communication procedure every node is located at static state, where the main cluster and every node rely on the basis of the strength of the node. In some cases where the nodes are not static, the controller selects the formation of the cluster head along the nearest nodes. Subsequently, the density of hop may reduce so differentiation of the hop may be adjusted to desired rules. In this algorithm for the BA- LEACHC steps implemented are: -

Initial stage:

Step 1: Initialization of the network structure during deployment of the nodes.

i) $GG \rightarrow S: iDh$, instance

Where GG is a group of network nodes, S cluster head and iDh is a node id or index.

ii) Broadcasting of the secure data and selection of S where $r \in SH \cap SAA(j)$

Where r several key_id in key ring, Sh several key_id in key ring and $SAA(j)$ nodes of key ring

$AA(j) \rightarrow GG: iDh$

Where $AA(j)$ is a member node.

Step 2: Communication with cryptographic technology through encrypted key.

i) $AA(j) \rightarrow GG: iDh, DAA(j)$

ii) $GG \rightarrow \text{Data Center (DC)}: iDh, DAA(j)$

Step 3: Creation of the network with increased security having maximum level of the infrastructure for each stage. The higher power approach in which hop is selected as the main cluster in relation to the remaining energy. The security keys are assigned to every node value.

There was an observation of the number of the frames and then power distribution as per desired node value where non-static value of node performs pattern identification. The communication between the hop nodes are given by the desired value of identified number, forwarding the packets in WSN.

Setup stage: Candidate Nodes (CN) $\rightarrow rr$.

1. If $rr < TT$ (nn) then, CH (Cluster Head) = CN else
2. Go to step1.
3. CH $\rightarrow GG: - ii$ (CH), join_ad.
4. $AA(ij) \rightarrow CH(jj) :- ii(CH(ji)), join_requ$.
5. $CH(ji) \rightarrow AA(ij) :- ii(CH(ji)), < tt(ij), ii(A(ij)) >$

Where ii is defined as an id.

Steady-state stage:

1. $AA(ij) \rightarrow CH(ji) :- ii(AA(ij)), ii(CH(ji)), information$
2. CH $\rightarrow BS: -ii(CH), ii(BS), agg_info$.

Numerous signs utilized here as: -

CN: -indicates Candidate Node that stands a chance to be promoted as CH

rr: -indicates Random variable ($0 < rr < 1$)

TT(nn): -indicates Threshold Value

ij and **ji**: -number of iterations 1,2.... n

GG: -indicates group of nodes in WSN.

Join_ad: -indicates Advertisement that combines cluster

AA: -indicates normal sensor node

Join_ad: -indicates request to combine the cluster

tt: -indicates Time slot for sending detected data

➔ : - indicates Broadcast messages

➔ : - indicates Unicast

3.4.1 Modify proposed approach

In this proposed work, we implemented highly secure network with BA-LEACHC approach with Objective Function. In particular, type of objective method that is utilized is explained, as an individual figure of advantage how near offered pattern solution is to achieving the set objectives. *FFn* (Fitness Function) are used in programming and algorithms to guide simulations towards optimized pattern solutions.

3.4.1.1 Objective function of proposed work

Objective fitness approximation might appropriate, normally in the following steps: -

- ✓ Calculation time of single solution is extremely high.
- ✓ Accurate model for fitness calculation is missing.
- ✓ The *FFn* is un-certain or distortion.

In objective function, we minimize and maximize a defined function under offered setting of constraints.

The *FFn* function is the method to optimize issues in the network. Optimization process, this is also called objective function. Each member node corresponding to failed cluster head compute *FFn*

for the genetic algorithm to cross-examine paths before relaying data packets to intended destinations and calling authentication mechanism if required. The probability to determine safe path for data packet transmission for each node is formulated on the basis of equation (3.1).

$$ffn = (1 - r) * (nn - Fss - Ftt) \quad (3.1)$$

Where, Fss represent each node, Ftt represent total processing nodes, nn represent number_of_nodes, and lastly r representing a wastage node (Error Memory).

3.4.1.2 Calculations

Cluster head is the node selected among the desired nodes in WSN. The hop node located in such manner that it is placed in a definite area for the processing of the CH. The CH corresponding to specific normal nodes has the definite value where BA-LEACHC algorithm is applied. The residual energy per node has location of cluster head and sink to the nearest neighbour node. Cluster F frequency value given by;

$$F = \sqrt{\frac{N^2}{\pi D}} \quad (3.2)$$

Where equation 3.2 shows how each cluster calculates its frequency value. The total energy of the displacement between the hop and the cluster head is also calculated by the given equation 3.2, then displacement between CH and BS is calculated by equation 3.3.

$$D^A = \sqrt{\frac{N^2}{2 \pi D}} \quad (3.3)$$

An additional value is given by the lifespan of the network and energy required for the node from the desired set of the nodes. $TT(nn)$ is multiplied through a factor signifying the current energy level of a node which is defined in the above equation 3.3.

$$TT(nn)_1 = \left\{ TT(nn) * \frac{N_1}{N_2} \right. \quad (3.4),$$

Where N_1 is the residual energy level of sensor energy for current round, and N_2 signifying initial node energy. $TT(nn)$ being the threshold value.

The generation of the network having same set of the values where the cluster head is given as the equivalent node value that is matched to base station. The threshold value is given by equation as,

$$TT(nn) = TT(nn)_1 * \left(\frac{E_{aver}}{E_{aver}-1} \right) \quad (3.5)$$

Where E_{aver} is the average value of the nodes given by the displacement among ordinary nodes and controller node. Selection of node to be member of cluster head and threshold value require the transmission of the node to be stable. The final threshold value given by designing of the distant node is described as,

$$TT(nn)_{prop} = \{TT(nn)_3 \times \frac{T*u}{cH}\}, \text{ Where CH is the cluster head,}$$

$$\text{Such that, } T = \frac{1 - \log_{10} f}{1 + \log_{10} f} + d1^2 + d1^4 \quad (3.6)$$

Where u is the number_of_nearest m^{th} nodes, CH representing the interval time to choose as a cluster head, $d1^2$ being the average distance of nodes in WSN to Data Center, and lastly $d1^4$ is node distance from the DC (Data Center) or BS.

The hop node will have maximum amount of energy with the set of the nodes with presence of the cluster control node. Along with that, the displacement between the sensor hop and controller is controlling node is incremented, the choice of the cluster head in current time is reduced. Each single hop present the random set of the values that related to 0 and 1.

A random pick of a number between 0 to 1 and compare this value with $th_val\ TT(nn)_1$, if the number is minimum than the $th_val\ TT(nn)_1$, then node become the CH for the current round otherwise node is calculated as a normal node. $TT(nn)$ is evaluated by formula 3.7:

$$TT(nn) = \begin{cases} \frac{PP}{1 - PP * r \bmod \left(\frac{1}{pp} \right)} & \text{If } nn \text{ belongs } GG \text{ otherwise } 0 \\ 0 & \end{cases} \quad (3.7)$$

Where PP represent cluster head percentage in current round in LEACH-C and has fixed the percentage of CH which is optimal percentage.

1. Calculating paths
2. Current_movement (Randomly).
3. If current_movement $\leq$ random_movements

Then calculate the fitness value base of th_val.

Different matrix generated by current_movement and array generated by minimum node value and position. If we find minimum different matrix, then fitness value generates based in 0 and 1.

CHAPTER 4

4. Simulation Results

4.1 Experiments and graphs

After various simulations, subsequent outcomes were collected. Basing upon the outcomes; the described study is defined as: -

The Figure 4.1 illustrates modified LEACH-C clustering approach in which nodes are deployed in WSN and subdivided in to clusters which act as a BA-LEACHC routing protocol that utilizes Biphasic Authentication Scheme and shows the cluster heads in blue colour and member nodes in red colour. The colour of cluster heads changes once the amount of energy is reduced during network operation, hence a member node indication high energy value stand a chance of promotion as CH.

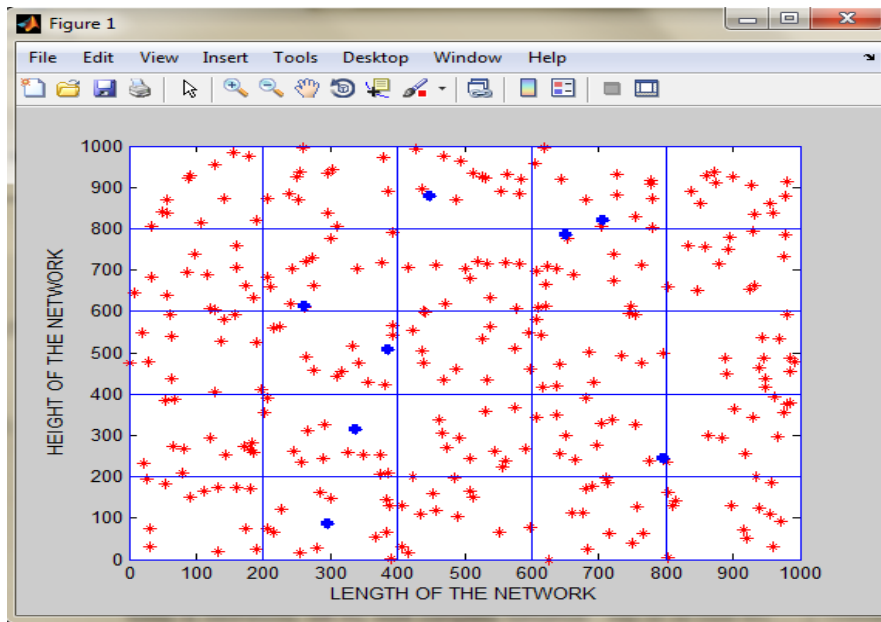


Figure 4. 1: Network deployments

The Figure 4.2 shows malicious node (double circle) in the network that will be authenticated after the genetic algorithm identifies safe path. The malicious node increases the number of nodes. Malicious node was created in a manner that it engages data packets in itself, same to slum which blocks everything that passes through. Some information in the network is lost or dropped more especially in the CH that connects new node. As nodes lose information, all the jam in the network

creates path exposure and the malicious node will be located through tracing involved paths. Once the node is identified, the authentication process takes place and decides on the node whether to block or accept.

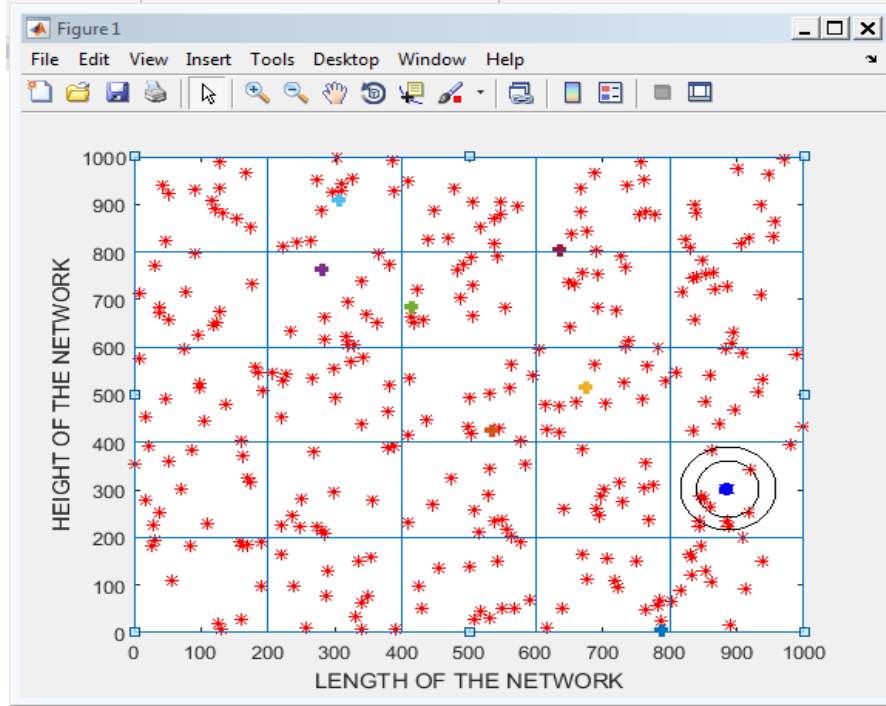


Figure 4. 2: Suspicious node

The Figure 4.3 shows the message box that the nodes should not be more than 300 nodes. The total quantity of nodes taken in the network or are sufficient for realization at first complete deployment strictly equals 300. On second round of cluster head selection, the current total number of nodes (CurTn) will be compared to previous total number of nodes (PrevTn) and if $CurTn > PrevTn$ cluster head fail and authentication scheme gets activated, otherwise if $CurTn \leq PrevTn$ means nodes are sufficient for realization of the WSN network. In cases where the $CurTn < PrevTn$, assumption is that nodes have no energy (dead nodes). And also, for $CurTn = PrevTn$ that means there was no introduction of a new node or suspicious node to the network.

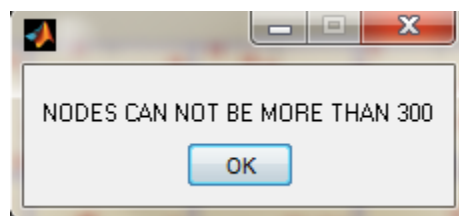


Figure 4. 3: Range of the sensor nodes

The Figure 4.4 shows the message box in which the cluster head fails to communicate the data from sender to receiver and there is requirement for the optimization, and shows that the cluster head fails and calls for objective function of the genetic algorithm. The genetic function predicts the malicious node and cluster head failure (inability to transfer packets) occurs to overcome the complete CH failure using three phases: (i) Selection (choose the sensor nodes) (ii) Crossover (divide data packets into SNs) and (iii) Alteration (Modify and detect the malicious node in the network).

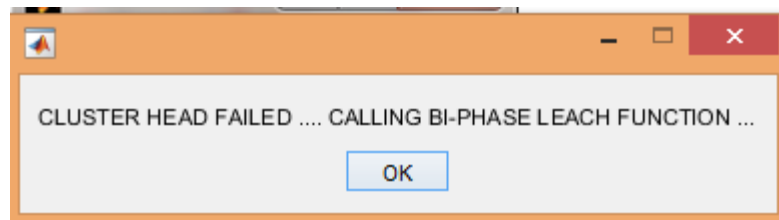


Figure 4. 4: Cluster head failure call for security scheme

The Figure 4.5 shows the dynamic path after applying objective function using BA-LEACHC algorithm. In this dynamic path, the sensor node identity (IDs) defines and predicts the safe route for data packets transfer of one source to destination SN.

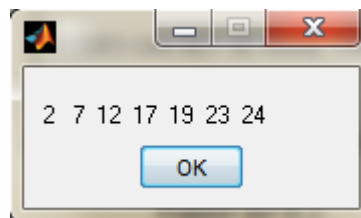


Figure 4. 5: Dynamic path

The Figure 4.6 shows the finalized path which is obtained by the fitness function of BA-LEACHC algorithm. This message box shows about the final secure route to transfer information in safe route in the WSN.

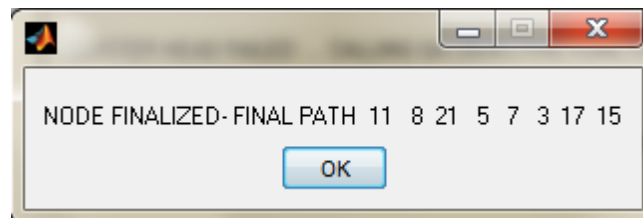


Figure 4. 6: Finalize route

The Figure 4.7 shows the destination block which is included in the finalized path as a destination node. The destination block shows the final destination node is 15 or end node to finish the data packets in the network.



Figure 4. 7: Finalize path as a destination node

The Figure 4.8 represents the throughput graph which shows performance in terms of data processing speed between LEACH-C and proposed approach (BA-LEACHC). The efficiency of the proposed approach is compared in throughput percentage and it indicates that the network throughput is increased when malicious node is separated from the WSN. Throughput factor is mostly affected by a form of DoS called selective forwarding. The effect of this attack in throughput is noticed through decreasing data packet exchange rate between member node and CH. WSN under attack of selective forwarding blocks some nodes from sharing crucial data packets across the network. Therefore, decreasing the throughput as well as misusing residual energy.

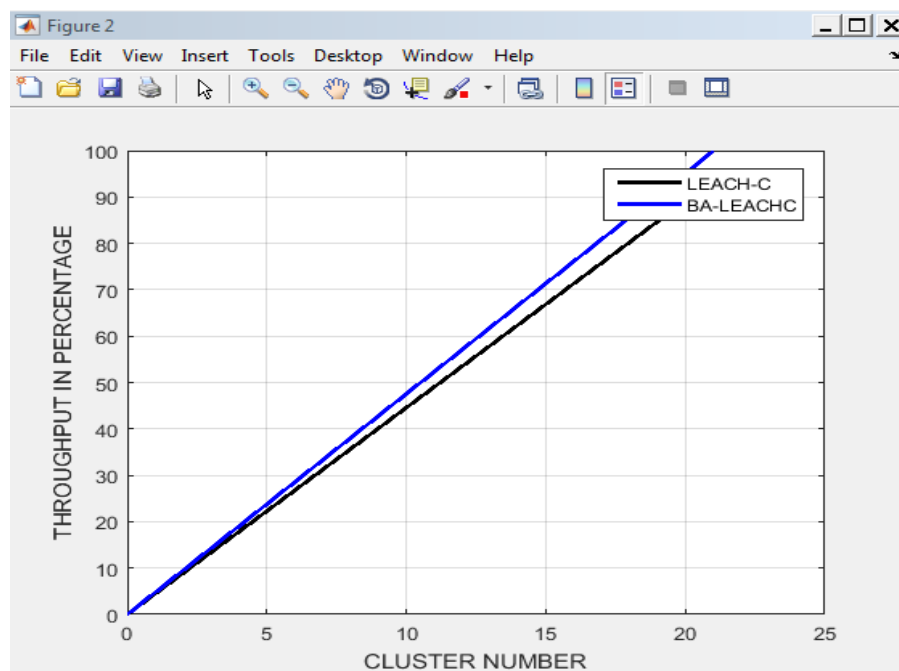


Figure 4. 8: Throughput (Per cent)

The Figure 4.9 depicts total time taken by data packets from sender to receiver which is known as end to end delay. In order to lessen network traffic which sometimes result in high consumption of energy due to time taken while delivering packets, this measure should be lowly maintained. Therefore, effective and efficient WSN depends on less delivery time when relaying packets from sender to receiver and vice versa. The effectiveness of our proposed method is computed basing on member node to base station delay (sec) and it demonstrated that sensor network time is optimized or minimized after isolating malicious node.

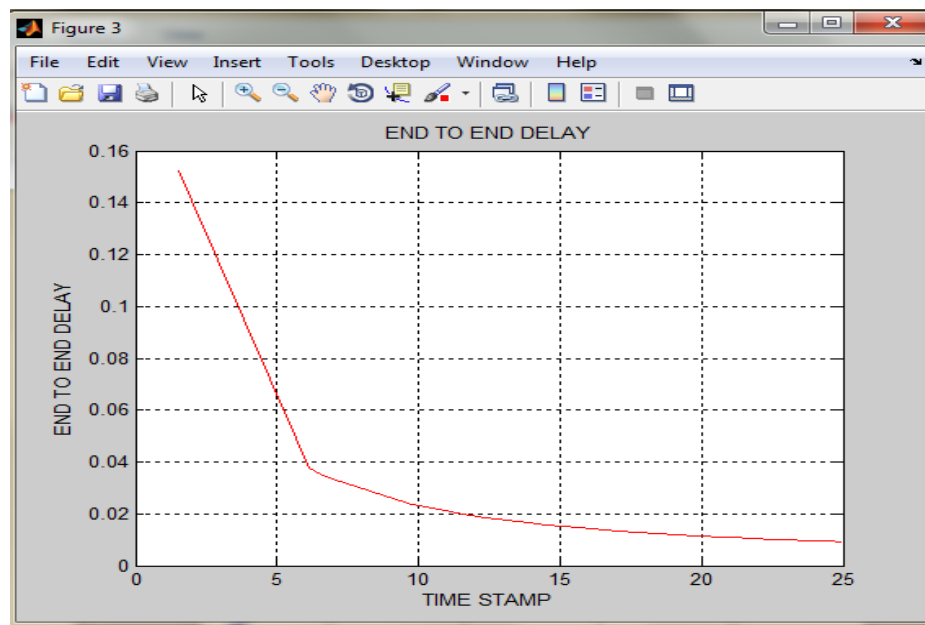


Figure 4. 9: End to end delay (second)

Figure 4.10 indicates energy consumption which is the major factor modified by BA-LEACHC protocol, the packets should traverse from sending node to receiving node with minimized power usage and after application of the proposed approach the consumption of power by nodes become low at time stamp 8.0(start point) to 17.0(end point). The energy factor of defined proposed method shows that when malicious node is detected and separated from the network sensor node, the energy consumption is minimized according to the time stamp. The time stamp 0.3(start point) to 8.0(end point) and 17.0(start point) to 21.0(end point) indicates high consumption of energy as the management or control of malicious node was not in place. There is a clear indication that malicious nodes are a cause for concern when it comes to node to node data packet delivery.

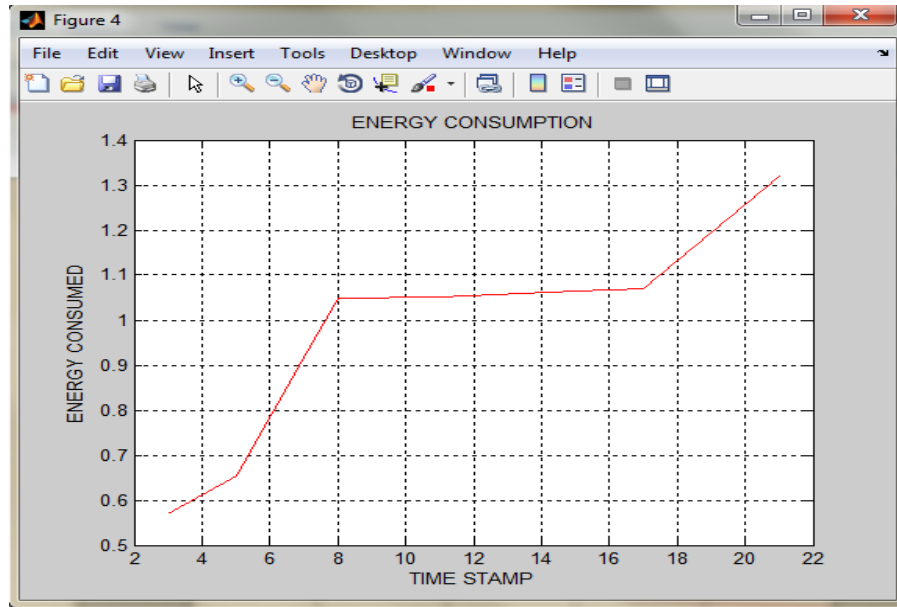


Figure 4. 10: Energy consumption (joules)

The Figure 4.11 shows significant network aspect named percentage of packet delivery. A delivery percentage of 99.6 proved by proposed approach communicates high success rate of data packets reaching destination or intended points. The positive performance by BA-LEACHC results in an increased network lifetime. The packet delivery ratio is a performance metric which considers a quantity of packet delivery getting transmitted in WSN. Due to malicious node isolation in the sensor network, PDR (packet delivery rate) increases.

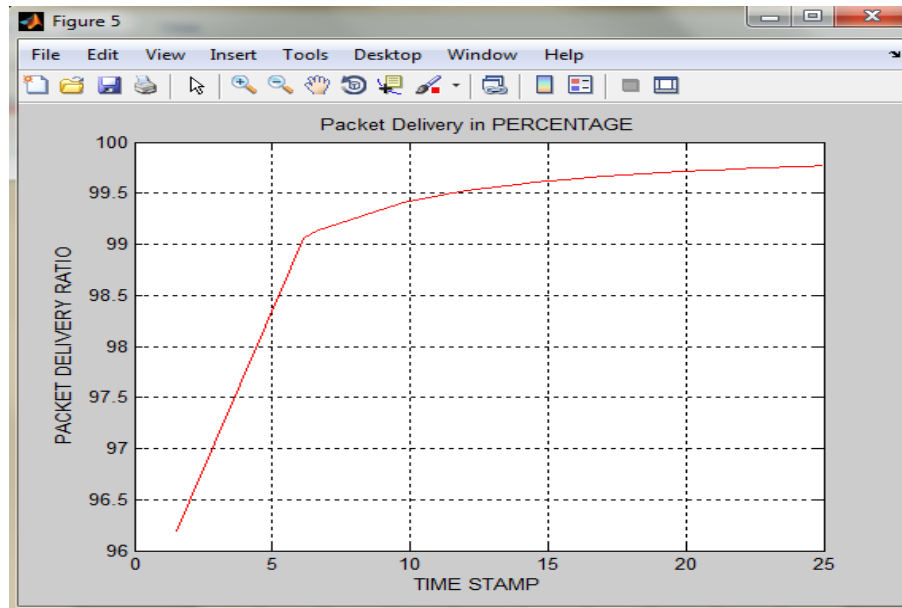


Figure 4. 11: Packet delivery rate (Per cent)

4.2 Evaluation and comparison of BA-LEACHC and LEACH variants

This portion of chapter five displays the result and experimental simulation of proposed approach against six LEACH variants. The evaluation is computed basing on power consumption as well as simulation time. Most importantly, there is evaluation and comparison between LEACH-C and BA-LEACHC in order to high light how the proposed method outperforms the unsecured LEACH-C.

Figure 4.12 defines the comparison between proposed and other existing clustering methods used in WSN. It offers the total network residual energy in all packet transmission time stamp. The WSN residual energy minimizes more speedily in the proposed methods based on BA-LEACHC and LEACH-V, LEACH- L routing methods etc. BA-LEACHC protocol is better than other methods, it considers the residual energy and chooses a node in case the energy of the cluster head minimizes when compared to the set average th_val . Figure 4.12 defines that the BA-LEACHC protocols consumed 10.6, 11.5, 13.5, 17.0, 18.41, 26.6 and 41.17 joules respectively.

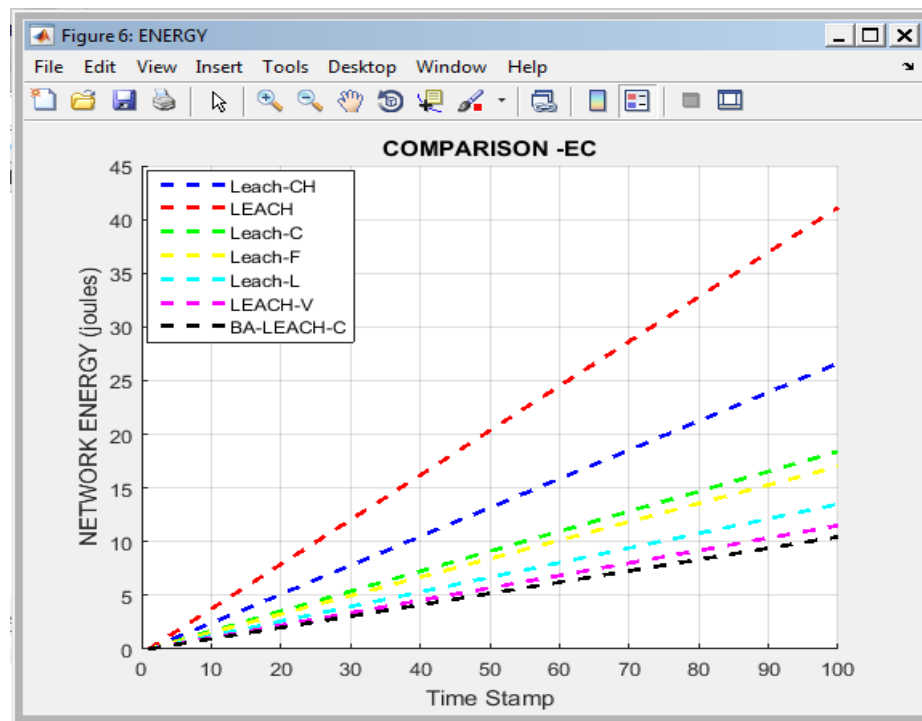


Figure 4. 12: Comparison in EC

Figure 4.13 defines the comparison between proposed security protocol and existing approaches. The proposed method is successful for division of cluster heads and does not need a huge

communication overhead and minimizing data transmission of redundant data to CHs. It reproduces the improvement of end-to-end delay as defined in Figure 4.13. The proposed method has reduced the delay when compared with various LEACH versions. Leach-f computes LEACH and LEACH-C since clusters are created only once, neglecting the energy cost due to the formation of the clusters at each round or phase. BA-LEACHC protocol is better than the other methods, because it considers the relative energy and chooses a node in case the energy of the cluster head minimizes when compared to the set average th_val . Figure 4.13 defines that the BA-LEACHC protocols recorded shortest time of 26.5, 31, 48, 56, 63, 67, and 70 seconds respectively.

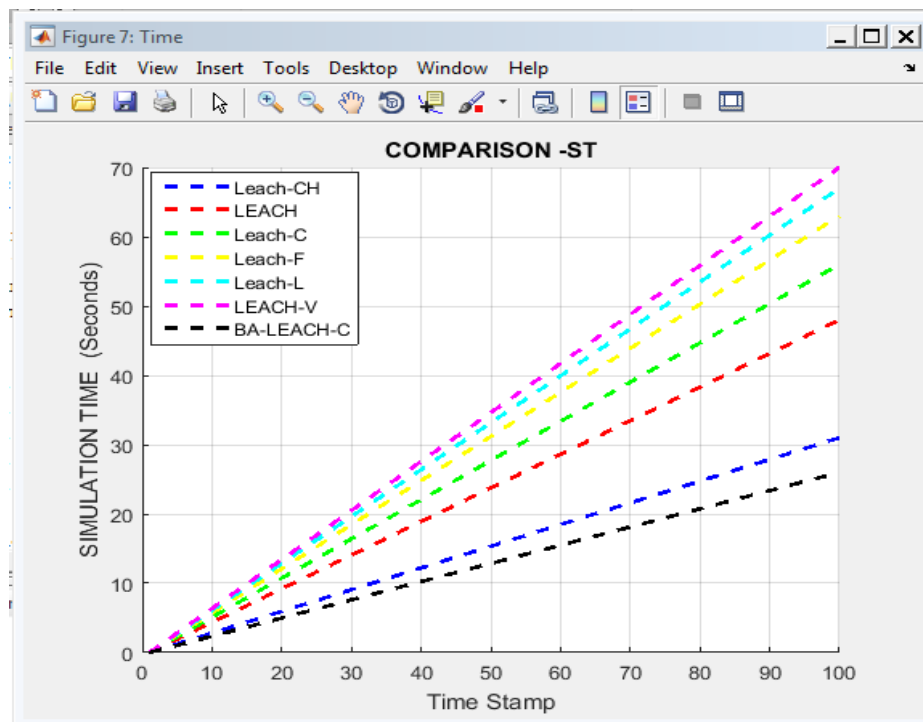


Figure 4. 13: Comparison in ST

CHAPTER 5

5. Conclusion and Future work

5.1 Introduction

Security is a fundamental subject in WSNs and involves protecting sensor nodes against internal and external attacks. In order for WSNs to provide full service, sensor node must be able to guard against any illegal network entry either by applying authentication techniques, using trust based approaches or by utilizing other protective measures.

The feature “resource constrained” in WSN nodes badly disrupts application of security measures. It is possible to apply standalone security scheme to protocols however, small memory and limited computation capabilities of nodes makes the integration difficult. Therefore, a possible alternative is to integrate security mechanism in routing protocols. Surprisingly, hundreds of cluster based approaches are proposed, but only a few addresses security problems. Majority of routing protocols dwell much on minimizing use of energy by nodes. Hence energy factor can be drained by malicious node sending copy of data packets repetitively. It is for that reason that this research work integrates LEACH-C approach with BAS for output identification of nodes that illegally joined or attempts to join existing network. Genuine communication among nodes is essential for the success of modern networks.

5.2 Summary of the study

In this Thesis, we express a need for concern that security aspect should also be prioritized in the same manner as reducing consumption of energy in protocols. Internal and external attacks should be dealt with before causing harm to network. That reason, led this research to proposition of BA-LEACHC approach which utilizes genetic algorithm to integrate BAS to LEACH-C. The information learnt from various sources and simulation observations on WSNs, indicates that an attacked protocol consumes more energy regardless of energy minimization techniques applied. Therefore, all unsecured WSN routing protocols can experience the following attacks: A malicious node can pretend to be CH to attain rights and send announcement messages. An attacker might join a cluster when setting up network consequently denying access to genuine nodes. The clustering processes can also be disturbed by bogus node hence initiating DoS.

5.3 Conclusion

In this study, we identified and authenticated a malicious node and evaluated the performance of BA-LEACHC: Biphase Authentication based Low Energy Adaptive Clustering Hierarchy Centralised protocol for WSNs. The approach has provided successful utilization of genetic algorithm (GA) in LEACH-C to examine paths for safe data transmission triggering BAS mechanisms to authenticate nodes linking to unsafe path. The new approach depend on regular checks and contrast of current total number of live nodes (CurTn) and previous total number of live node (PrevTn) as an alert or attention to the network security. It has discussed that a node is malicious if not included in safe path listing by GA and has failed to satisfy the BAS procedure. It has provided key technical trends for WSN security from literature and highlighted the importance of securing routing protocols. It has provided basic concepts and background of WSN and genetic algorithm (GA) including general areas of GA application.

The proposed approach improved the performance and increased the lifetime of network as follows; it presented packet delivery ratio increased to 99.6 percent after removing malicious node which improved network performance and ensured that data packets communicated in a trusted manner. The envisioned protocol performance was evaluated in MATLAB, and compared with a number of unsecured LEACH variants. BA-LEACHC outperformed LEACH-CH, LEACH, LEACH-C, LEACH-F, LEACH-L and LEACH-V by recording network energy consumption of 10.6 joules lower than comparatives. Based on simulation time, it was concluded that BA-LEACHC out performs LEACH-CH, LEACH, LEACH-C, LEACH-F, LEACH-L and LEACH-V by recording shortest time of 26.6 seconds during source to destination packet delivery.

5.4 Future work

The nature of wireless media exposes networks to several attacks and vulnerabilities. Some existing integration of authentication mechanisms in LEACH based protocol do not provide reliable solutions. Besides authentication there are other network requirements like data integrity and confidentiality that can possibly pose threats if unaddressed. Additional authentication mechanisms should be proposed or merged into frequently used protocols (i.e. LEACH variants) to provide inside and outside WSN security. This research work can be developed into several

versions to address various network security problems. Our grand future plan is to extend the proposed BA-LEACHC protocol to address some security threats like zero data freshness, zero data integrity and zero data confidentiality. The extended BA-LEACHC will then provide more effective and efficient network with extremely increased performance. This extended protocol includes extensive analysis of nondeterministic factors like cluster head remaining energy, node-to-node distance and so on. Furthermore, the improvement in our research work will include determining dead node in case current total number of nodes (CurTn) is less than previous total number of nodes (PrevTn). Lastly, in this extension we will include analysis of minimal node energy to determine if not a contributing factor to a node failing objective function satisfaction.

REFERENCES

- Abirami, T., & Priakanth, P. (2014). Energy Efficient Wireless Sensor Network using Genetic Algorithm based Association Rules. *International Journal of Computer Applications*, 91(10), 8–12. <https://doi.org/10.5120/15915-4783>
- Alshowkan, M., Elleithy, K., & Alhassan, H. (2013). LS-LEACH: A new secure and energy efficient routing protocol for wireless sensor networks. *Proceedings - IEEE International Symposium on Distributed Simulation and Real-Time Applications*, 215–220. <https://doi.org/10.1109/DS-RT.2013.31>
- Bagula, A. (2012). *APPLICATIONS OF WIRELESS SENSOR NETWORKS Why Use WSNs* [Classification] [Sensor Usage] [WSN Applications] [Future. February, 1–67.
- Baranidharan, B., & Santhi, B. (2015). *GAECH : Genetic Algorithm Based Energy Efficient Clustering Hierarchy in Wireless Sensor Networks*. 2015.
- Boyinbode, O., Le, H., Mbogho, A., Takizawa, M., & Poliah, R. (2010). A survey on clustering algorithms for wireless sensor networks. *Proceedings - 13th International Conference on Network-Based Information Systems, NBIS 2010*, 30, 358–364. <https://doi.org/10.1109/NBIS.2010.59>
- Chandrasekaran, K. (2014). *Trust Factor based LEACH-C protocol for Wireless Sensor Networks*. 105(18), 43–48.
- Dener, M. (2014). Security analysis in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2014. <https://doi.org/10.1155/2014/303501>
- Deshmukh, G. S., Khairnar, V. D., & Kadu, P. S. (2016). *Clustering Routing Protocol for Energy Efficiency of Wireless Sensor Network using Genetic Algorithm*. 2645–2651.
- Gavrić, Ž., & Simić, D. (2018). Overview of dos attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ingenieria e Investigacion*, 38(1), 130–138. <https://doi.org/10.15446/ing.investig.v38n1.65453>
- Guyeux, C., Makhoul, A., & Bahi, J. M. (2017). *A Security Framework for Wireless Sensor Networks : Theory and Practice*. June.
- Haque, E., & Yoshida, N. (2012). Clustering in Wireless Sensor Networks. *Internet and Distributed Computing Advancements*, 5, 197–211. <https://doi.org/10.4018/978-1-4666-0161-1.ch008>
- Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol

architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4), 660–670. <https://doi.org/10.1109/TWC.2002.804190>

Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2005). *Energy-efficient communication protocol for wireless microsensor networks*. 00(c), 10. <https://doi.org/10.1109/hicss.2000.926982>

Jan, M., Nanda, P., Usman, M., & He, X. (2017). *PAWN : a payload-based mutual authentication scheme for wireless sensor networks*. June 2016, 1–10. <https://doi.org/10.1002/cpe.3986>

Jasuja, V. (2017). Available Online at www.ijarcs.info *International Journal of Advanced Research in Computer Science VIRTUAL MACHINE MIGRATION : A COMPARATIVE STUDY*. 8(0976), 342–350.

Kaushal, K., & Kaur, T. (2015). A Survey on Attacks of WSN and their Security Mechanisms. *International Journal of Computer Applications*, 118(18), 1–4. <https://doi.org/10.5120/20842-3437>

Khan, A. S., & Khan, M. (2019). A Review on Security Attacks and Solution in Wireless Sensor Networks. *Am J Compt Sci Inform Technol*, 7(1), 31. <https://doi.org/10.21767/2349-3917.100031>

Kumar, S. R., & Umamakeswari, A. (2016). SSLEACH: Specification based secure LEACH protocol for Wireless Sensor Networks. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, 1672–1676. <https://doi.org/10.1109/WiSPNET.2016.7566424>

Michal, M. (2013). *Base Station for Wireless sensor network*. 64.

Mishra, A., Phulre, S., & Richhariya, V. (2015). Routing Protocols for Wireless Sensor Networks: A Survey. *International Journal of Computer Applications*, 118(1), 12–15. <https://doi.org/10.5120/20708-3022>

Monnet, Q., Hammal, Y., Mokdad, L., Ben-othman, J., Monnet, Q., Hammal, Y., Mokdad, L., & Fair, J. B. (2016). *Fair Election of Monitoring Nodes in WSNs* To cite this version : HAL Id : hal-01314197 *Fair Election of Monitoring Nodes in WSNs*.

Network, W. S., & Manaa, M. E. (n.d.). *WSN NETWORK ARCHITECTURES*. 1, 1–7.

Rahayu, T., Lee, S.-G., & Lee, H.-J. (2015). A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation. In *Sensors* (Vol. 15, Issue 7). <https://doi.org/10.3390/s150715127>

Rahmanian, A., Omeranpour, H., Akbari, M., & Raahemifar, K. (2011). A novel genetic algorithm in LEACH-C routing protocol for sensor networks. *Canadian Conference on Electrical and Computer*

Engineering, 001096–001100. <https://doi.org/10.1109/CCECE.2011.6030631>

Riaz, R., Chung, T., Rizvi, S. S., & Yaqub, N. (2017). *BAS : The Biphase Authentication Scheme for Wireless Sensor Networks*. 2017.

Rohbanian, M. R., Kharazmi, M. R., Keshavarz-Haddad, A., & Keshtgary, M. (2013). Watchdog-LEACH: A new method based on LEACH protocol to secure clustered wireless sensor networks. *Advances in Computer Science: An International Journal*, 2(3), 105–117.

Saadawy, M. El, & Shaaban, E. (n.d.). *Enhancing S-LEACH Security for Wireless Sensor Networks*.

Singh, S. K., Kumar, P., & Singh, J. P. (2017). A Survey on Successors of LEACH Protocol. *IEEE Access*, 5, 4298–4328. <https://doi.org/10.1109/ACCESS.2017.2666082>

Singh, S. P., & Sharma, S. C. (2018). *Genetic-Algorithm-Based Energy-Efficient Clustering (GAEEC) for Homogenous Wireless Sensor Networks*. 2063. <https://doi.org/10.1080/03772063.2017.1364981>

Sorout, N., & Singh, M. (2016). *Obtaining Security and Energy Efficiency for Leach-Clustering Protocol in Wireless Sensor Network*. 5(6), 2067–2072.

Tabassum, M. (2014). a Genetic Algorithm Analysis Towards Optimization Solutions. *International Journal of Digital Information and Wireless Communications*, 4(1), 124–142. <https://doi.org/10.17781/p001091>

Tseng, H. R., Jan, R. H., & Yang, W. (2007). An improved dynamic user authentication scheme for wireless sensor networks. *GLOBECOM - IEEE Global Telecommunications Conference*, 986–990. <https://doi.org/10.1109/GLOCOM.2007.190>

Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, 35(3), 867–880. <https://doi.org/10.1016/j.jnca.2011.03.005>

Zawaideh, F., & Salamah, M. (2019). An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *International Journal of Communication Systems*, 32(3), 1–13. <https://doi.org/10.1002/dac.3878>

Zhao, F., Xu, Y., & Li, R. (2012). *Improved LEACH Routing Communication Protocol for a Wireless Sensor Network*. 2012. <https://doi.org/10.1155/2012/649609>

PLAGIARISM REPORT

Thesis-10 march 2020

ORIGINALITY REPORT

12%	8%	7%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijmcs.info Internet Source	2%
2	Submitted to University Der Es Salaam Student Paper	1%
3	www.khaledelleithy.org Internet Source	1%
4	www.ijitee.org Internet Source	<1%
5	Submitted to Botswana Accountancy College Student Paper	<1%
6	Submitted to University of Alabama Student Paper	<1%
7	Submitted to Brunel University	<1%



BOTSWANA INTERNATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY, PRIVATE BAG 15 PALAPYE, BOTSWANA, PLOT 1055 TEL: +267 4900117 FAX: +267 4900102

UNIVERSITY WRITING CENTRE

CERTIFICATE OF EDITING AND PROOFREADING

This certificate confirms that the Master of Science in Computer Science and Information Systems Thesis was edited and proofread at the Botswana International University of Science and Technology (BIUST) University Writing Centre.

Thesis Title:

BA-LEACHC: Biphase Authentication Based LEACH-C Protocol for Wireless Sensor Networks

Author:

Mr Modisaotsile MAROPE
Student ID No: 16100031

Date Issued:

12/10/2019

Writing Specialist:

Ms Lebogang Euginia M. Morolong

Writing Specialist Signature:
