PREVENTION OF SYBIL ATTACK USING ISOLATION TECHNIQUE IN WIRELESS SENSOR NETWORK

A Dissertation

Submitted

In Partial Fulfillment of the Requirements

For the Degree of

Master of Technology

In

Computer Science and Engineering

Submitted by

Md Ajaz Rab

Roll No. 2001621006

Under the Supervision of

Dr. Jameel Ahmad

(Assistant Professor)

Department of Computer Science & Engineering

Faculty of Engineering

INTEGRAL UNIVERSITY, LUCKNOW, INDIA

July, 2022

CERTIFICATE

This is to certify that **Md Ajaz Rab** Enroll. No. 2000102891 a student of M. Tech CSE has carried out the research work presented in the dissertation titled **"Prevention of sybil attack using Isolation technique in wireless sensor network"** submitted for partial fulfillment for the award of the **Master of Technology Computer Science And Engineering Integral University, Lucknow** under my supervision.

It is also certified that:

(i) This dissertation embodies the original work of the candidate and has not been earlier submitted elsewhere for the award of any degree/diploma/certificate.

(ii) The candidate has worked under my supervision for the prescribed period.

(iii) The dissertation fulfills the requirements of the norms and standards prescribed by the University Grants Commission and Integral University, Lucknow, India.

(iv) No published work (figure, data, table etc.) has been reproduced in the dissertation without express permission of the copyright owner(s).

Therefore, I deem this work fit and recommend for submission for the award of the aforesaid degree.

Dr. Jameel Ahmad
Supervisor
(Assistant Professor)
Department of CSE,
Integral University, Lucknow
Date:
Place: Lucknow

DECLARATION

I hereby declare that the dissertation titled **"Prevention of sybil attack using Isolation technique in wireless sensor network"** is an authentic record of the research work carried out by me under the supervision of **Dr. Jameel Ahmad**, Department of Computer Science & Engineering, for the period from September 2021 to july 2022 at Integral University, Lucknow. No part of this dissertation has been presented elsewhere for any other degree or diploma earlier.

I declare that I have faithfully acknowledged and referred to the works of other researchers wherever their published works have been cited in the dissertation. I further certify that I have not willfully taken other's work, para, text, data, results, tables, figures etc. reported in the journals, books, magazines, reports, dissertations, theses, etc., or available at web-sites without their permission, and have not included those in this M.TECH dissertation citing as my own work.

Date: Signature_____

Name: **Md Ajaz Rab**

Enroll No: **2000102891**

RECOMMENDATION

On the basis of the declaration submitted by "**Md Ajaz Rab**", a student of M.Tech CSE, successful completion of Pre presentation on 24/6/2022 and the certificate issued by the supervisor, Dr. Jameel Ahmad, Assistant Professor, Computer Science and Engineering Department, Integral University, the work entitle **"Prevention of sybil attack using Isolation technique in wireless sensor network"** , submitted to department of CSE, in partial fulfillment of the requirement for award of the degree of Master of Technology Computer Science, is recommended for examination.

Program Coordinator Signature	HOD Signature
Dr. Faiyaz Ahamad	**Mrs. Kavita Agrawal**
Dept. of Computer Science &Engineering	Dept. of Computer Science & Engineering
Date:_____	Date:_____

COPYRIGHT TRANSFER CERTIFICATE

Title of the Dissertation: **Prevention of sybil attack using Isolation technique in wireless sensor network**

Candidate Name: **Md Ajaz Rab**

The undersigned hereby assigns to Integral University all rights under copyright that may exist in and for the above dissertation, authored by the under signed and submitted to the University for the Award of the Master of Technology Computer Science degree.

The Candidate may reproduce or authorize others to reproduce material extracted verbatim from the dissertation or derivative of the dissertation for personal and/or publication purpose(s) provided that the source and the University's copyright notices are indicated.

MD AJAZ RAB

ACKNOWLEDGEMENT

I am highly grateful to the Head of Department of Computer Science and Engineering for giving me proper guidance and advice and facility for the successful completion of my dissertation.

It gives me a great pleasure to express my deep sense of gratitude and indebtedness to my guide **Dr.Jameel Ahmad, Assistant Professor, Department of Computer Science and Engineering,** for his valuable support and encouraging mentality throughout the project. I am highly obliged tohim for providingme this opportunityto carry out the ideas and work during my project period and helping me to gain the successful completion of my Project.

I am also highly obliged to the Head of department, **Mrs. Kavita Agarwal (Department of Computer Science and Engineering)** and PG Program Coordinator **Dr. Faiyaz Ahamad, Assistant Professor, Department of Computer Science and Engineering,** for providing me all the facilities in all activities and for his support and valuable encouragement throughout my project.

My special thanks are going to all of the faculties for encouraging me constantly to work hard in this project. I pay my respect and love to my parents and all other family members and friends for their help and encouragement throughout this course of project work.

MD AJAZ RAB

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND SYMBOLS

WSNs : Wireless Sensor Networks

CPU : Central Processing Unit

RAM : Random Access Memory

ROM : Read Only Memory

SDRAM : Synchronous Dynamic Random Access Memory

SRAM : Static Random Access Memory

EPROM : Erasable Programmable Read Only Memory

USB : Universal Serial Bus

ADC : Analog to Digital Converter

DVD : Digital Video Disk / Digital Versatile Disk

I/O Device : Input Output Device

ID : Identity Document

OSI : Open System Interconnection

DoS :- Denial Of Service

DDoS : Distributed Denial of Service

NTOM : Node Trust Optimization Machine

ECC : Eliptive Curve Cryptography

ROR : Real Or Random

BAN : Burroughs Population Needham

SBS : Sequence Backward Selection

WSN-DS : Wireless sensor Network Detection System

MATLAB : Matrix laboratory

ABSTRACT

A network that does not contain any central controller within it and is self-configuring in nature is known as a wireless sensor network. It is difficult to maintain the security and energy consumption of these networks due to such properties. When any kinds of malicious nodes enter the network, a scenario of attack occurs in that network. There are several types attacks found in the network which are all categorized into active and passive types depending upon the manner in which they attack. This research work is based on an active type of attack which is commonly known as sinkhole attack. In the sink hole attack the malicious nodes spoof identification of the base station and act like base station. The sensor nodes start transmitted data to malicious nodes instead of base station. In order to identify and eliminate such malicious nodes, this research proposes a new technique that uses identity verification in order to provide a secure environment for communication in the network. Simulations are performed by implementing the proposed technique in NS2. The proposed technique gives results better as compared to existing techniques in terms of certain parameters

Chapter 1

Introduction

WSNs (Wireless sensor networks) have become quite popular these days as they provide low-cost solutions to many real-time challenges. WSNs consist of compact-size, comparatively low-cost computational nodes. These nodes or motes measures local environmental parameters or other conditions and relays such information to a centralized point for suitable processing. Wireless Sensor Networks are generally defined as an interesting emergent field of intensely networked structures of low-energy wireless nodes with a small number of CPU and memory, and big unified networks for high-resolution sensing of the surroundings. The domain is continuously growing due to recent advancements in technical grounds and the emergence of countless potential applications.

1.1 Description of WSNs

The collection of numerous sensing devices such that the information related to the surrounding environment of a specific region can be known is called a WSN. The sensing devices which are otherwise known as nodes are very small in size and also have least cost. Initially, these networks were only deployed within the military regions in which keeping a track on the activities of opposite parties was very important. Each of their movements were tracked and the vital information was used by authorities to take appropriate actions [1]. There are several such applications in which it is not easy to observe the activities or mobility in such wide regions. Thus, the deployment of WSNs is very helpful in such applications. Today, there are extensive scenarios in which these networks can be deployed. They have been performing certain operations such as sensing, processing and communicating of data within the regions. The region that is to be monitored is deployed by WSN such that the sensor nodes are randomly dispersed all across the region. Mainly the applications of WSN are large and hostile due to which certain constraints also arise for them. Figure 1 illustrates the typical architecture of a wireless sensor network.

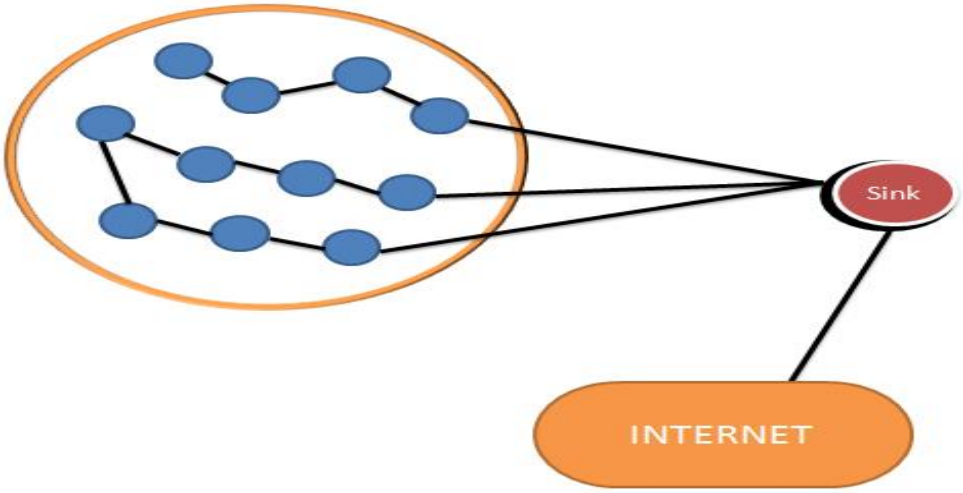


Figure 1.1: Wireless Sensor Network

There occurs only certain amount of battery in the installed sensing devices, since these nodes are very small in size. WSNs are deployed within acoustic or underground applications that are inaccessible for the human such that the activities of those regions can be kept under track. The devices deployed within such regions have higher costs in comparison to those deployed in terrestrial areas. The multimedia sensor networks deploy several microphones and cameras within them as well along with the less costly nodes. For processing the data in appropriate way, higher bandwidth, energy and quality of service are vital factors. Within the acoustic regions, the networks are deployed by placing the sensor nodes underwater such that sparse environment is created. The signal fading, delay as well as propagation are few of the various issues that are being faced by these wireless networks [2].

WSNs are deployed within complicated regions without any permanent infrastructure. The deployment of around hundreds to thousands of numbers of sensing devices is done such that the tasks needed to be performed can be accomplished. Since these networks are heterogeneous is nature, it is possible to deploy them in several regions. Numerous types of operations are performed by the sensing devices deployed within WSNs. To gather the information from certain regions, it must be ensured that the network is distributed all across it. To carry out the overall analysis, it is important to monitor the areas in cooperative manner such that all the relevant data is collected. WSN comprises two important components within it which are aggregation and base station. From the sensors present around the regions, the information is collected and it forwarded to other devices to be passed on to authorities. Sink or base station

is the device towards which all the collected data is passed on. It is responsible to transfer the information further.

1.2 Sensor Node Architecture

There are five major components that are included in a sensing device. They are memory transmitter or receiver, power unit, sensing unit, embedded processor. Figure 2 shows the general architecture of a wireless sensor node.

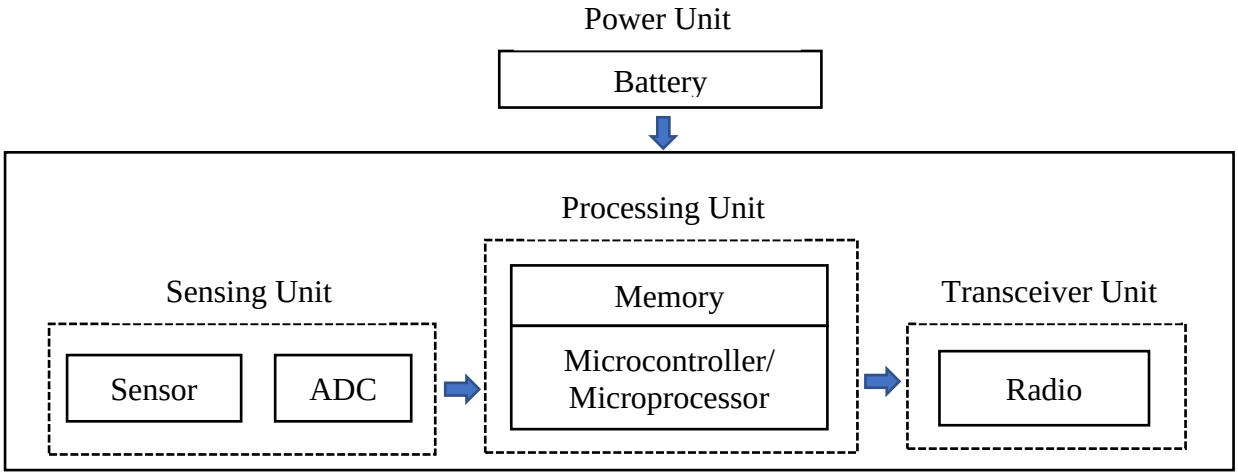


Figure 1.2: General Architecture of a Wireless Sensor Node

The description of each of these components has been given below:

i. Microcontroller Unit: The microcontroller unit is responsible for various functions, data processing, and controls other elements in the node [3]. This unit is in charge to manage all other components being the main controller of the wireless sensor node. The controller unit may comprise an on-board memory or may be connected with a small storage unit integrated into the embedded board. This unit controls the processes allowing the sensor node to carry out sensory operations, run associated algorithms, and work together with other nodes via wireless channel.

ii. Transceiver Unit: A sensor node communicates with other nodes and other components of the wireless sensor network through the transceiver unit. This unit consumes most power among all units.

iii. Memory Unit: The memory unit stores the sensed data temporarily and can be RAM, ROM and their other memory types (SDRAM, SRAM, EPROM, etc.), flash or even exterior storage devices like USB.

iv. Power Unit: The power unit responsible for supplying energy to nodes, is a very critical component [6]. It is possible to store energy in batteries (most common) rechargeable or not or in capacitors. Natural resources such as solar power can be used in forms of photovoltaic panels and cells, wind power with turbines, kinetic energy from water, etc. for more power supply and recharge.

v. Sensor unit: The last one is the sensor unit. This is one of the core components of a wireless sensor node and is different from any other embedded system in terms of communication proficiencies. This may typically include multiple sensor units, which provide the ability to collect information from the real world. Each sensor unit is meant to collect a certain type of information, such as temperature, humidity, or light. This unit generally consists of two subunits: a sensor and an analog-to-digital converter (ADC). The ADC, on the basis of monitored episode converts the analog signals generated by the sensor. These signals are later applied into the processing unit.

1.3 Characteristics of WSNs

At present, the wireless networks consist of numerous networks such as mobile communications network, wireless local area network, network of Bluetooth, Ad hoc network etc. The sensor network includes many features that are similar to the Ad hoc networks [4]. The mobility, switching character and the battery power limitation are some of the features. Wireless sensor network comprises some typical properties as compares to these wireless networks. These features of WSN are mentioned below:

a) Computing capabilities: The sensor's space for program and memory is very limited due to the limited cost, size and consumption of battery power.

b) Battery energy: The sensor nodes are made invalid and abandoned frequently due to the battery exhaustion. At that time, the conservation of battery energy is possible using the protocols and algorithms. The nodes that transmitted the data information consume more energy than the energy consumption of nodes that implement computing. The main issue is

related to the saving of power during network processing in order to increase the lifetime of WSN.

c) Communication capabilities: The communication bandwidth of sensor network is narrow and variable. The effect of natural environment influences the sensor. The storms, rain, lighting, the terrain obstacles and the weather are comprised in this natural environment. The management of running of wireless sensor network is very complicated. Thus, the robust as well as fault-tolerant software and hardware are required for WSN.

d) Dynamic: When the battery is exhausted and other failures occur, the sensor node is exited from the networks [5]. There is a need to add and move some new sensor nodes into networks due to the task's requirement. As a result, the changes will appear in the network's topology. The reconfiguration, dynamic and self-adjustment functions are comprised in the topology of wireless sensor networks.

e) No center, self-organization: The deployment of wireless sensor nodes does not need preinstall any network infrastructure. Sensor node, which it can collaboratively adjust itself perform and distribute algorithm, can rapidly and automatically form an independent network after nodes switch on. The WSN is an equal network.

f) Multi-hop communications: Only the sensor node is capable to communicate with direct neighbors in wireless sensor network. The multi-hop route is carried out so as the one node that is away from coverage of the radio frequency of node is communicated with other nodes using the intermediate nodes. For this, the gateways and the routers are employed in the multi-hop route in the conventional wired networks. The nodes of WSN play the role of data collector and sender as well as the information router.

g) Application relevance: The wireless sensor network is centralized the data gathering, multi-hop communication and many-to-one traffic pattern. There is a difference between the WSN and conventional networks as WSN depends upon the applications. To obtain the environment data is its major work.

1.4 WSN Applications

Research and development in the field of sensor networks is driving advancements in many high-tech areas. The applicability of sensor networks has been in discussion since long time by

emphasizing potential applications that can be realized using wireless sensor networks. A discussion on certain applications developed for WSNs has been given below:

a. Military or Border Surveillance Applications: Wireless sensor networks have become an essential part of military command, control, communications and intelligence schemes. The rapid deployment of sensor networks and the need for self-organization characteristics have made them a very favorable sensing technology to serve military relevant purposes. The idea of sensor network is emerged as a better approach to the battlefield as in sensor networks the disposable and low-cost sensor nodes are deployed densely. It is possible to deploy sensors in a war zone to observe the presence of forces and vehicles, to track their movements, and bringing opposing forces under surveillance.

b. Environmental Applications: The independent coordination proficiencies of wireless sensor networks are used to realize a huge number of environmental applications [6]. Some environmental applications of wireless sensor networks are to track the movements of birds, small animals, and insects; monitor ecological conditions affecting crops and livestock; temperature, humidity and lighting in office buildings; irrigation; comprehensive earth monitoring and planetary study. It is also possible to unify these monitoring modules with actuator units, which are liable to control, for example, the level of nourishment in the soil, or the level of temperature in a building, in accordance with dispersed sensor measurements.

c. Health Care Applications: The elderly and patients can be monitored and tracked for health care purposes using wireless sensor networks, which can overcome the acute shortage of health care staff and make healthcare in existing health care systems inexpensive. For example, the behavior of a patient can be monitored by deploying sensors in his/her home. If the patient falls and needs instant medical attention, these sensors can alert doctors. Moreover, the emergence of implanted biomedical tools and smart inbuilt sensors makes it possible to use sensor networks for biomedical application.

d. Home Intelligence: A very convenient and smart living atmosphere can be provided to users using wireless sensor networks. For instance, wireless sensors networks make the remote reading of home utility meters such as water, gas, electricity possible. Further, readings can be delivered to a remote center through wireless channel. In addition, intelligent sensor nodes and actuators may be embedded in different devices such as vacuum cleaners, microwave ovens, refrigerators, and DVD players. These sensor nodes integrated into domestic devices can

perform communication with one another and with the exterior network through the Internet or satellite. They facilitate end-users to control home appliances more easily from local and remote locations. Consequently, these networks allow the interaction of multiple devices at residential locations by controlling various homely applications conveniently.

e. Industrial Process Control: The use of wired sensor networks is not new in industrial arena to serve different purposes such as industrial sensing and control applications, constructing automation, and access control. However, these systems have become less applicable due to the costs related with deployment and preservation of wired sensors. The sensor-based systems, on the other hand, suffer from high deployment costs, less accurate manual systems, and require personnel. As an alternative, WSNs present a impressive solution for these systems because of their easy deployment, high granularity, and high accuracy delivered through wireless communication units powered by batteries.

f. Agriculture: The use of wireless sensor networks is common within the farming sector. The use of wireless networks frees the farmer from maintaining wiring in difficult environments. Using pressure transmitters for observing water tank levels, controlling pumps using wireless I/O devices, measuring water usage and transmitting readings back to a central control center wirelessly for billing is monitored by gravity feed water systems [7]. Irrigation computerization allows the use of water more efficiently and

1.5 Constraints of WSNs

The resource-constrained based sensor nodes collectively generate a WSN although there is limited amount of processing potential and storage capacity available within them. Based on the resources, the bandwidth is also provided in these networks. These networks have been facing several issues since the small power and magnitude of sensing devices. Due to such constraints, introduce security approaches within these networks can be designed easily. For improving the conventional security algorithms, the various constraints of sensing devices are important to be considered. Few important constraints that are being seen in WSNs are given below:

i. Energy constraints: The most important constraint is the energy constraint. Following are the power level based three broader categorizations consumed by certain components:

- Sensor transducer utilized certain amount of energy.
- To perform communication, the sensing devices consumed certain power level.
- The computations are performed by microprocessors which also require energy.

Every bit that is being communicated across the network consumes around 800 to 1000 instructions of power. Therefore, in comparison to computation, the energy price for performing communication is higher here. In case when kind of message expansion occur because of security mechanisms, certain amount of cost should be paid. To optimize the protection levels of networks, higher power is consumed by the cryptographic functions. Therefore, several security steps are presented in the networks depending on the energy cost they require.

ii. Memory limitations: A sensing device is expressed as a small device that comprises limited memory as well as storage area. The memory of sensor node includes a flash memory and RAM in it [8]. In this memory mainly the downloaded application code is stored. The RAM stored within it the application programs, sensed data as well as the calculations being performed at high speed. The execution of complex algorithms is not possible in case when the Operating system and application code are loaded completely because of unavailability of storage space. Thus, providing several security algorithms in these sensors is important.

iii. Unreliable communication: The unreliable communication that is being held in this network is another issue to be studied. Packet-based routing is generally provided according to connectionless protocols provided. Therefore, inherently, the routing provided here is very unreliable. When devices are highly congested the errors can be generated or the packets can be dropped. This results in disrupting the complete message within the packets. As a result of unreliable wireless communication channel, it is possible to either damage or disrupt the packets. Because the error rate is high within these networks, several robust error handling approaches are utilized in the networks. This results in causing higher overhead in the networks. If a reliable channel is provided in the network, the incidence of such errors will result in providing unreliable network communications. Packet collisions might occur due to the transmission in networks, the retransmission of these packets is done which creates this issue to another level.

iv. Higher latency in communication: As a result of multi-hop routing, congestion and processing, higher latency occurs within the networks when the intermediate nodes transmit

the packets. Due to this, synchronization can be performed. at the time of synchronization, various issues might arise at security level since critical event reports and cryptographic key distribution completely effect the efficiency of certain approaches [9].

v. Unattended network functions: Several nodes remain unattended within the network as WSNs are installed in hostile regions. Thus, the occurrence of a physical intrusion within these situations is very likely possible. the remote management systems cannot virtually see any kind of physical tampering since the regions in which a WSN is deployed is very large. Therefore, establishing a secure WSN is highly difficult task.

1.6 Organization of thesis

Chapter 1: In chapter 1, the introduction is given related to WSNs. This chapter gives an overview of WSNs in terms of their applications, characteristics, and constraints.

Chapter 2: In chapter 2, various types of routing protocols are described in detail and also detail is given related to sink hole attacks

Chapter 3: In chapter 3, the literature survey is given related to sink hole attack. The research community has proposed various schemes for the detection, prevention and mitigation of sink hole attacks.

Chapter 4: In the chapter 4, the proposed work, aim of project, objectives are written related to sink hole attack.

Chapter 5: This chapter involves result analysis, comparative study, and discussion on the proposed methodology. The efficiency of proposed model is tested with regard to certain parameters.

Chapter 6: This chapter provides conclusion of the conducted research work along with future work.

Chapter 2

Security Background

The communication performed within WSNs is unprotected and not private since the networks are deployed in hostile regions in which only limited number of resources can be available. The deployment of security techniques within these networks is not easy. However, protection of security is essential since the information being processed and transmitted is very critical. Regarding security, several issues are being faced by WSNs since they have very unique properties.

2.1 Security Requirements in WSN

It is very important to make certain that these networks are highly secure. For this, there are certain requirements that are to be taken care of. The sensing device requires certain types of bounded resources within it which will help in guaranteeing that the highly sensitive data is protected completely. The functionalities help in keeping these networks alive. Because of certain vulnerability and opportunities, the networks might be attacked by adversaries very easily due to which the users can suffer great loss. The main security requirements of WSNs are discussed as follow:

a. Data Confidentiality: This property defines the process that may hide information completely to protect it from adversaries. For the encryption of data, a secret key is available through which the info can be made completely invisible [10]. There are only certain authorized users that assist to import the data. In relevance to the confidentiality of WSNs, there are certain important factors to be considered.

b. Data Authentication: For several applications of WSN, the major factor to be considered is message authentication. The blocking of any kinds of illegal parts is possible here in the networks and the original nodes simultaneously focus on identifying any kinds of unauthorized nodes or users. It is required to receive the data from an accurate source. Further, the destination must be ensured during communication which can make sure that data is not passed on to any unauthorized adversaries.

c. Data Integrity: The intruders may either modify or change the data. Therefore, it must be guaranteed the recipients are not modified by the unauthorized users when transmission is being held. This property which helps in ensuring that no such modifications are caused is termed as data integrity.

d. Data Freshness: This feature defines the freshness of network data. Some chances occur when the previously existing data is replayed in the network, and to make certain that it does not happen, its freshness is computed. Even in case when the data is ensured to be integral and confidential, its freshness must be ensured. Further, it also makes certain the malicious user is not replaying the existing data.

e. Access Control: Access control is provided to make sure that the resource is not accessible to the unauthorized users. Within the property, any kind of unauthorized participation is not allowed [11].

f. Availability: When the adjustment of traditional encryption algorithms is done within WSNs, the overall cost is increased. As a result of certain approaches, the code must be modified such that the code reutilization can be well supported. Further, additional communication is needed by some techniques to satisfy the goal. There are restricted number of approaches proposed to reduce the complexity of algorithms. However, these approaches reduce the level of availability of nodes. The availability can be affected as a result of few reasons amongst which few are:

- Because of additional processing included in the network, the power consumption is also maximized. The exhaustion of overall energy results in data loss.
- The additional communication operations increase the energy exhaustion. There is increment in the likelihood of collision in case with massive communications performed.
- In case when a centralized scheme is provided, a single point occurs. Therefore, huge threats are faced if WSN is made available.

Therefore, when the interference occurs during the operations, the network may turn out to be unavailable. Hence, appropriate security scheme must be designed for WSNs.

2.2 Security Attacks on WSN

WSNs are known to be very different from other networks since they have highly unique properties from others. The possibility of attacks to enter these networks is also high. The vulnerability and susceptibility lead to other security attacks since they include broadcasting communication. The entrance of attacks is higher in the networks because of their installation

in higher and dangerous regions. Several attacks can occur at different layers since all these layers work in different manner and perform different functions. Several routing algorithms are included without any suitable security mechanism. Hence, it is very easy for the attackers to breach the security of networks. Following are many sorts of intrusions identified in each layer [12]:

2.2.1 Physical Layer attacks

Following are the most common physical layer attacks in wireless sensor networks:

i. Jamming: Since the radio frequencies face interference with the devices, a direct attack may be launched. Therefore, a jamming attack is caused. This sort of attack is completely different than normal radio propagation since the networks face huge kind of problems and the networks are resented completely. The denial-of-service conditions are faced because of this intrusion.

ii. Tampering: This intrusion compromises the node completely. There is huge possibility of this attack and the effects caused are very dangerous. The modification of sensing devices is done and the network is destructed because of this.

2.2.2 Link layer attacks

Following are the most common link layer attacks in wireless sensor networks:

i. Collision: Neighbor-to-neighbor message faced by the channel negotiation in the link layer is the main reason of this intrusion. There will be disruption of complete packet in case when collisions occur in any region of the deployed network. Therefore, there is a need to retransmit the packet since single bit error is caused.

ii. Exhaustion: There is exhaustion of battery power when an interrogation attack occurs. The power exhaustion is very high here because the packets are transmitted repeatedly. This gives rise to complete exhaustion of the battery of nodes [13].

2.2.3 Network layer attacks

Following are the most common network layer attacks in wireless sensor networks:

i. Hello flood attack: Higher transmission power is needed to replay or transmit the hello packets such that the neighbors can be discovered during this intrusion. The attacker creates an illusion by presenting a device in neighbor of other devices. thus, the routing protocol included here will completely be disrupted and higher no of intrusions will occur here. The attacker uses hello packet as a weapon to encourage the sensing devices to trust the compromised device. The intruder device consists of higher radio transmission rage and processing power due to which various sensor nodes receive hello packet. The partitioning of these nodes is done within large areas. The sensors assume the adversary to be their neighboring node.

ii. Wormhole attack: In the networks, a low-latency link is created due to which at huge speeds using multi-hops the packets are forwarded. This leads to a wormhole intrusion within WSN [14]. This intrusion is a huge threat for any routing protocol available in the networks. Detecting or preventing such attack is extremely hard. The wormhole indicates that though the device is very distant, is very near to its neighbor, which is however an adversary. This might create a confused situation in the network and the communication will initiate which causes sharing of personal data to malicious users. Figure 3 depicts the general composition of wormhole attack.

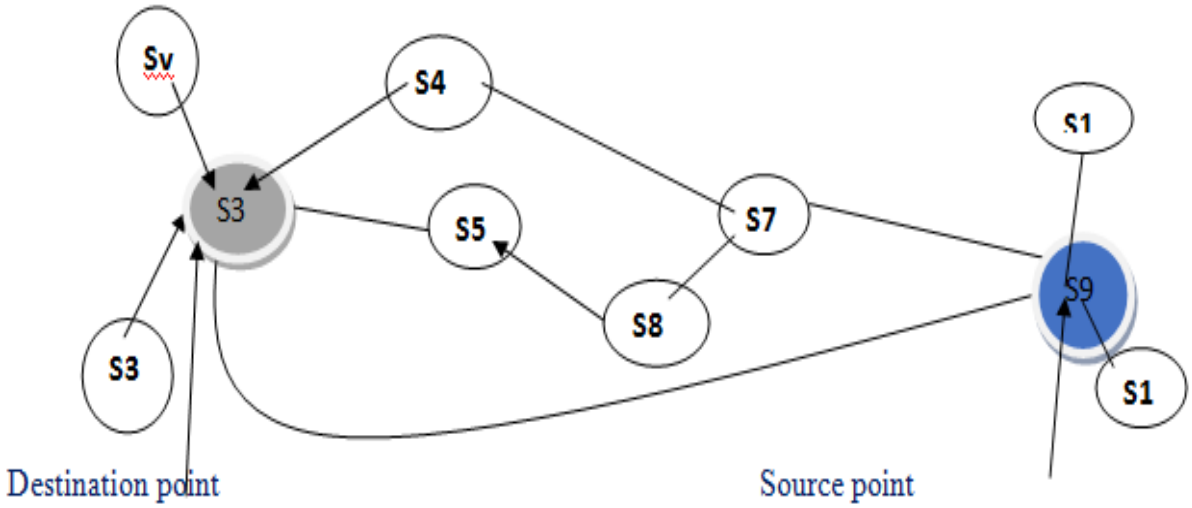


Figure 2.1: Wormhole Attack

iii. Sybil attack: An attack uses a malicious node to create an influence on the network's traffic. Thus, numerous entities are created which result in causing Sybil attack. An ID is generated in

case when any fake additions are made or the duplicates of already available legitimate identities are created [15]. Sybil attack targets the multi-hop routing along with the fault tolerant approaches. A legal node generates various identifies and these identifies may be used by a single or many network devices due to this attack. A single node thus results in creating multiple identities.

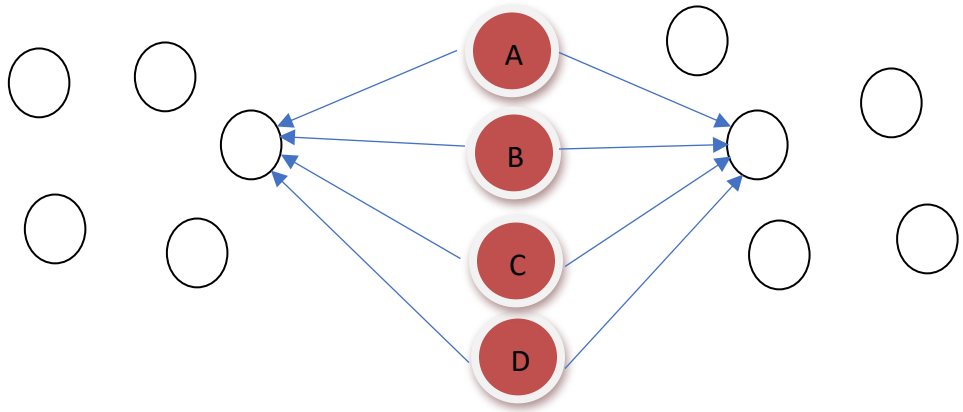


Figure 2.2: Sybil attack

Figure 4 depicts the general composition of sybil attack. This attack results in disrupting the integrity, security and resource utilization provided. An external user can result in causing any type of Sybil attack. The system that holds either an authentication or encryption technique within it can be prevented from such attack only. Public key cryptography is applied against such internal attacker. However, the systems are highly costly in case when resource-based networks are deployed. The likelihood of a Sybil node may be calculated through the equation given below as:

$$s_r(detection) = 1 - s_r(nondetection)^r_{1round}$$
$$= 1 - (1 - s_r(nondetection)_{1round})^r$$
$$= 1 - \left(1 - \sum_{allS,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S - (m - M)}{c}\right)$$

iv. Sinkhole attack: Because of the presence of such intrusion, sink cannot achieve complete and accurate sensing data. This presents a serious threat within the higher-layer applications. The attacker here attracts entire network traffic towards itself. The adversary is made to look highly attractive in comparison to other devices [16]. When a sinkhole intrusion occurs, sink cannot receive correct sensing data. A huge threat is thus faced by the higher layer applications.

The malevolent device appears to be more striking as compared to other sensing devices, because of which all the sensed data is transmitted towards it. A sinkhole is said to be generated when such adversary is present at the center. The compromised node attracts the information in the neighboring nodes. thus, every bit of information being exchanged across the neighboring nodes is eavesdropped here. With respect to the routing protocol involved, the adversary is made to look as highly attractive. Thus, data is forwarded towards it across the network. For establishing a high quality of route towards the sink, the adversary can perform spoofing.

2.2.4 Transport layer attacks

Following are the most common transport layer attacks in wireless sensor networks:

i. Flooding Attack: This intrusion is generated in case when huge amount of data is flooded within the complete network. Flooding corresponds to the continuous receiving of numerous packets. For initiating the incomplete connection requests, the longer processing of genuine connection requests is done. Innumerable such connections are established by the memory buffer because of flooding which is unable to be accomplished. When buffer is completely full, the making of further connections is impossible.

ii. De-synchronization Attack: De-synchronization attack is a type of communication reliability attack. A reliable transport protocol must ensure that it can detect each packet loss, and each lost packet can be retransmitted until they reach its destination node [17]. In the de-synchronization attack, an attacker forges packets with control flags or sequence numbers. Once a sensor node receives a bogus packet, it will request the sender to retransmit the lost packet. If this process continues, it will impact normal communications between source nodes and destination nodes, and consume a lot of energy.

2.2.5 Application layer attacks

Following are the most common application layer attacks in wireless sensor networks:

i. Denial of Services: there are certain limitations caused within the functioning of sensor network. There are more chances for this attack to occur within a OSI layer. For the destruction of infrastructure configuration, all the resources may be exhausted. DoS completely interrupts the efficacy of networks here. The physical disruption of network components is seen here

when this attack occurs. Further, this attack also results in destroying the wireless transmission. This attack generates noise, collision or interference at the receiver's end. The attacker has certain targets to be focused on amongst which few are the infrastructure of network, the sever application and the network access. The prey device transmits the extra un-required data in DoS attack [18]. There is draining of network resources in such scenario as the users cannot access the services completely. In some conditions, there is complete destruction of the network by adversary. It completely destroys the network potential to perform certain tasks. This intrusion can possibly occur within various layers. Jamming and tampering occur within the physical layer are DoS sorts of intrusions. Crash, battery collapse and unreasonableness are seen in link layer which also belong to this categorization. In transport layer, flooding and de-synchronization occur due to this attack.

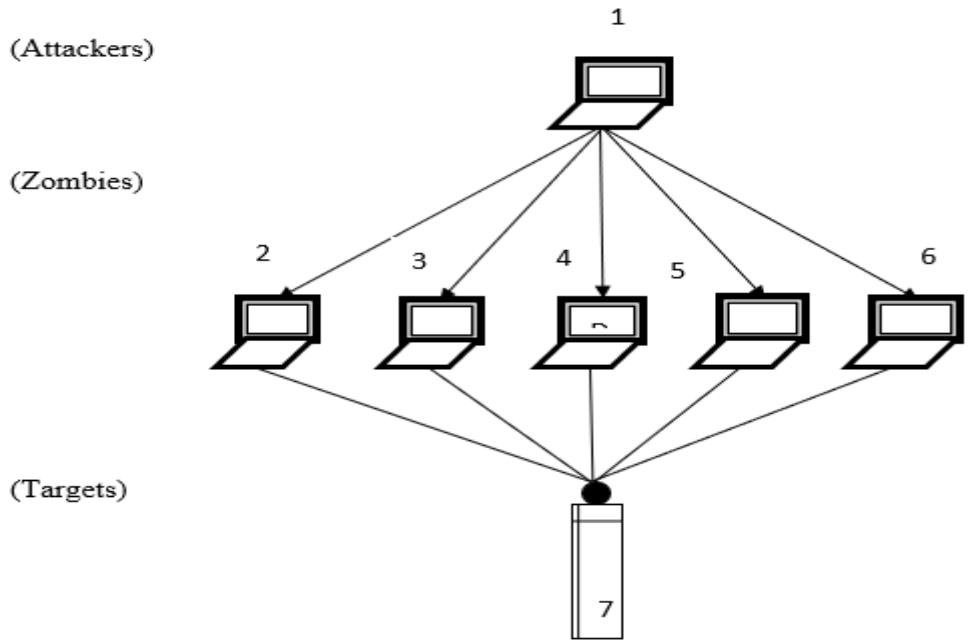


Figure 2.3: DoS attack

Figure 5 depicts the general composition of DoS attack. To make sure that DoS attacks do not occur, the network resources must be secured and the traffic requirements must be authenticated. Several techniques have been proposed to secure the reprogramming process. The network utilizes the authentication within itself to make is secure. The DoS provides a choice to rekey the request packet. Thus, this intrusion is possible when two consecutive keys are invalidated in the nodes or keys. When there is frequent rate of rekeying of requests, DoS attack occurs. From the devices, packets are plunged within a configurable duration.

Retransmission of packets is done and DoS initiates when identification of re-keying request packet is done.

ii. Cloning attack: This intrusion occurs when capturing and compromising the sensing devices is very easy. Creating unlimited numbers of clones is done for the compromised nodes here. It becomes easy for all the clones to participate within any of the operations as a result of legitimate access [19]. There is generation of various internal attacks or destructed when this intrusion is generated. If network is unable to identify the close, the network can be easily accessed by attackers. Thus, various other intrusions may also enter this network very easily. An effective and efficient solution is thus needed to be implemented to prevent it from these kinds of intrusions and provide secure environment for communication.

2.3 Miscellaneous Attacks in WSN

Wireless sensor networks face miscellaneous attacks which are discussed as follow:

a. Energy drain attack: For providing power in the networks, there are batteries available. The networks are installed in a dynamic manner. Recharging or replacing nodes is essential once they run out of power [17]. There is draining of fixed energy level in case of battery powered networks. The attacks can possibly occur in case when the intruder node transmits the packets at constant rate. The sensing devices destroy completely as well as degrades the performance of network. A complete partitioning of network grid is done and for controlling the part of sensor, a new sink node is added here. For minimizing the damage of this intrusion, the reports that are en-routed are dropped here.

b. Data Integrity Attack The compromising of data that is being transmitted across the devices is done as changes made in data that is available within the packets or because of addition of false data [18]. The adversary has higher processing memory and energy power as compared to rest of the devices. Depending upon the objectives of attacks, the data is falsified. This compromises the research of the victim. The falsification of routing data is done for disturbing the normal operation of sensor network which results in making the network completely destructive. The incidence of such attacks can be prevented by applying asymmetric keys through which encryption can be provided.

c. Sniffing attack: This attack is caused when any interception or listening occurs in the channels. In the proximity of sensor grid, the compromised is placed to capture data. The gathered data is sent to the intruder to perform processing with the help of some mechanism [20]. There are however, no affects caused on the normal functioning of protocol. These types of attacks can be caused by an external attacker to gather valuable data from the sensors.

d. Interference and Jamming: The radio signals are jammed or interference is caused which leads to loss or corruption of messages. When an attacker includes a powerful transmission, a signal is generated. This strong signal causes overwhelming of targeted signals. This disturbs communications being performed.

Chapter 3

Literature Review

It is very necessary to design an efficient mechanism to detect malicious attack in order to balance the energy usage and to extend the lifetime of the network. Attackers launch different types of attacks on WSN such as sinkhole attack, cibile attack, eavesdropping and denial of service attack. The attacks in WSNs are generally divided into two groups: external attacks and internal attacks. An attacker launches external attacks on an external entity that is injected into the network. This attack is launched to corrupt the entire operation of the network. In an internal attack, an attacker launches attack on the domain or trigger another attack by penetrating a sensor node.

3.1 Review of Different Works in the Area of WSN Security

H. Xie, et.al (2019) first briefly described WSNs and presented protocol stack layers-based taxonomy of assaults in WSNs. In order to measure the security of WSNs, this work researched the assault identification detection techniques of eleven typical assaults [21]. This work pulled out security data that contributed significantly in security glitch detection. This work adopted several performance measures to describe the pros and cons of tradition detection techniques. At last, this work highlighted several real-time concerns in the domain of this article on the premise of exhaustive study and concluded this work with feasible research guidelines in the time ahead.

M. A. Al-Naeem, et.al (2021) concentrated on Distributed Denial of Service (DDOS), particularly on DDoS-PSH-ACK (ACK & PUSH ACK flood) in WSNs [22]. The presented scheme approach conducted a number of experiments and applied them for identifying the operation of DDoS assault. The study-based experimentation attracts steaming traffic within multiple transferring periods including "usual transferring within sensing motes and cluster heads" along with "transferring and retransferring conditions within sensing motes and cluster heads" with varied amplitude of signals. The maximum ideal latency determined between broadcasts was found 23 milliseconds to guarantee that the receiver side was underloaded. The outcome of the existent review emphasized the time of the overloading of the transferring period, that affected the achievement of DDoS assaults.

S. Lata, et.al (2021) analysed security threats against WSNs and IoT in a comprehensive manner, and also presented solutions to prevent, detect and mitigate those dangers [23]. Familiarity with the details of these attacks can help build a secure IoT extension and comprehensive interpretation of relevant countermeasures. This work was aimed at addressing

and demonstrating the effect of security concerns on WSNs in terms of IoT and its implementations. The analysis performed for this task also included a taxonomy of existent assaults and dangers against these necessities.

Z. Teng, et.al (2022) put forward the proposal of a detection algorithm combined with the Node Trust Optimization Model (NTOM-DA) against wormholes in WSNs to provide resistance to such assaults and increase network productivity [24]. Firstly, the node whose number of nearby nodes crossed the threshold were added to the catalogue of distrustful nodes. Thereafter, the unique nearby nodes of the suspected nodes interacted with one another. Marking the route with number of hops more than the wormhole threshold was the next task to test the required route. Next, a trust model was established to measure the trust of node and estimate route reliability. NTOM-DA yielded outstanding results in identifying wormhole assaults in the simulations. The new approach obtained a high detection rate and less false-positive rate regardless of a network with large number of nodes and high attack scale, which ensured the secure and trustable functioning of WSNs efficiently.

J. Lee, et.al (2020) introduced a secure and effectual three aspects-based authentication protocol by making use of biometric traits [25]. In the meantime, the developed protocol protected network against brute force and stolen smartcard assaults using a honey_list technology. The newly developed proposed protocol was able to protect the security of network even during the collusion of two out of three aspects. This work used only hash functions without the public key supported ECC (elliptic curve cryptography) to develop an effective protocol in view of the restricted productivity of the sensing device. This work analyzed security informally along with prescribed security examination based on Real-or-Random (ROR) model and Burroughs Population Needham (BAN) logic.

S. Jiang, et.al (2020) presented a novel technique of detecting attacks called SLGBM for WSNs. This work initially implemented the Sequence Backward Selection (SBS) algorithm to the mitigate the dimensionality of data on the attribute of the feature space of real-time flowing data thereby reducing the computing cost [26]. A variety of network intrusions were detected using a LightGBM algorithmic approach. The WSN-DS dataset based tested outcomes demonstrated the clear supremacy of the F-measurement of the presented technique over existent particular detection techniques which obtained attack detection rate of 99.8% in normal, 99.4% in blackhole, 99.1% in grayhole, 96.5% in flooding and, 96.1% under flooding and scheduling (TDMA) scenarios.

L. Xiong, et.al (2021) prepared a blend of pseudonym ID, single-use hash chain and tag methods to build LAASFS for WSNs scenario [27]. The presented algorithm showed high flexibility to asynchronous assaults. Moreover, it had potential to resisting a large number of given assaults such as SCLA and incorrect password login assault. This work used BAN logic and ProVerif mechanisms to validate the security features of the presented algorithm by performing experiments properly. Different from many preceding relevant approaches, the introduced algorithmic approach possessed clear benefits in terms of computational and transmission overhead.

X. Huan, et.al (2021) introduced a novel node detection method known as Node Identification Against Spoofing Attack (NISA) to protect against spoofing assaults [28]. This work used a reverse time synchronization architecture, where the clock skews of sensing devices were assessed on top of the WSN, and spatially interrelated wireless link information for identifying nodes and detecting assaults simultaneously. This work further offered central and dispersed NISA to cover both one-hop and multiple-hop environments. The earlier one employed one-input and multi-output ConvNets. This work examined the recognition of clock skewers during the alterations in temperature and voltage using a real-time testbed containing TelosB sensing devices running TinyOS to assess the productivity of both central and dispersed NISAs. The tested outcomes depicted that both centralized and distributed NISAs could help identifying nodes and detecting spoofing assaults accurately.

M. Alotaibi, et.al (2021) focussed on introducing a new safe routing framework by selecting nearly best route and encryption [29]. Firstly, this work selected nearly best routes or nodes in the presence of best possible link-state multipath routing to transmit data securely. This article designed and presented a Crossover Mutated Marriage in Honey Bee (CM-MH) algorithmic approach for optimally selecting destination and source route. Next, there was encryption which helped in transmitting data securely. This work presented an improved blowfish algorithm (IBFA) for secure verification. The last step was the monitoring of updates. In conclusion, a large number of evaluation criterion were used to validate the dominance of the devised methodology over many state-of-the-art methodologies.

Panagiotis Sarigiannidis, et.al (2016) presented there are numerous applications in which this technology of WSN has been utilized. The area where this technology has been utilized is military region, hospitals and unattended operation. The implementation of sensor nodes is done randomly within the hostile region where human reach is difficult. This network has open

communication environment due to which this network is more prone to the attacks. A number of attacks are available that affect the functionality of this network such as blackholes, selective forwarding and many mores [30]. Sybil attack is taken as the major threat. In this attack, numerous identities are declared unlawfully by one or more than one malicious node. If the malicious nodes show that Sybil nodes are directly connected to them, than attack become more worsen in this condition. Therefore, they performed detailed study on the Sybil attack for the examination. They calculated the performance of WSN when Sybil attack is launched. Depending on various sensor nodes and their intensity, the probability of Sybil-free WSN is measured.

Yali Yuan, et.al (2015) presented that due to the initiation in the technology, there is development in the WSNs technology has been widely utilized currently in all applications. The location of the sensor motes must be correct in the hostile environment of WSNs because of the location-aware applications within network. The WSN has the open communication environment due to which it is more prone to the attacks. In these attacks, several identities are shown for the single node due to which there is reduction in the localization accuracy that caused the damage of the entire network system [31]. They suggested a new lightweight SF-APIT algorithm that assists in the reduction of the attack. This method is popular because of its range free method and can bale to perform in even at the individual node. There is minimum overhead, in the wireless devices due to this proposed method the efficient results are obtained from it on the basis of Received Signal Strength (RSS).

Noor Alsaedi, et.al (2015) presented the emerging technology of Wireless Sensor Network is widely utilized in almost every application. Sensor nodes are deployed at random within the network because of which it has dynamic network topology. There are some limitations as well in this sensor such as small processing power and limited battery cause various major issues that exploit the network sometimes. This network has open communication environment due to which it is more inclined to the attacks. Several attacks are occurred that affected the working of this network such as Sybil attack, which is the major attack [32]. There is disruption in the whole network due to the presence of multiple identities originated from malicious node. They developed a lightweight trust system to minimize all the issues in which energy is utilized as metric parameter for a hierarchical WSN. The presented technique is evaluated by carrying out experiments that represented that this technique is efficient. There is mitigation in the communication overhead in the network due to this method.

Sepide Moradi, et.al (2016) presented with the growing technology of WSN and its applications, it is been widely utilized currently in almost every area. In the hazardous environments these nodes are distributed for the collection of data. The data is gathered with the distribution of sensor nodes of sensor nodes in hazardous environments [33]. The security of WSN is very essential due to the insecurity of these environments. It is imperative to detect the attacks in these networks so that the security is offered. A variety of attacks have warned WSN, the Sybil attack is one among them. It may be a big threat for geographical routing algorithms and multi-path routing. The mobile agents and local information regarding every sensor is deployed for suggesting a distributed technique so that the attack can be detected. The simulation outcomes demonstrate that this technique is efficient as compare to earlier techniques.

Salavat Marian, et.al (2015) presented the emerging technology of WSN is deployed as it has widespread applications. This network has open communication due to which it is more prone to attacks. consider. In this attack, the packets are broadcasted with multiple nodes are IDs and provided the false identity of other motes to gain network access. This attack is the main cause of other attack when it gains the access of WSN. They presented a security solution to detect the Sybil attack easily on the basis of received signal strength indicator (RSSI) method [34]. Otherwise, previously proposed method was planned on the basis of the random key distribution. For estimating the link quality, there are two known indicators in WSN such as RSSI and Link Quality Indicator (LQI). The experiments were carried out in order to quantify the suggested technique and concluded the efficiency in static environment with good transceivers. The received power should be function of distance as per the wireless channel models that can be utilized to localize the Sybil nodes.

Ruixia Liu, et.al (2014) presented the growing technology of body sensor network (BSN) is widely deployed in a variety of applications due to which there is change in the lifestyle of people. The physiological health of the user information and privacy are some parameters associated with this network therefore, security is taken as major issue. In this network, multiple node identifiers are used as communication medium to broadcast messages due to which it is easy to Sybil attack to hamper the functionality of WSN [35]. They suggested a novel received signal strength indicator (RSSI) using which all the present Sybil motes are identified while regulating their transmission power. Therefore, this method performed better than other methods. Each node maintains its own identity certificate due to which any

symmetric key encryption technology is not required for this mechanism. They performed simulations to compute the presented technique and concluded that this technique is effective with respect to high detection rate and limited overhead.

Imran Makhdoom, et.al (2014) studied that it is easy for an unauthorized user to enter the WSNs as they offer free inlet and outlet of users. Several attacks are available today which affect the network's efficiency. The protection against the external attack is provided using classic cryptographic. However, they are incapable of diminishing the insider attacks in which node is compromised [36]. Sybil attack is the major attack among all other attacks as it had the compromised node. They analyzed all the suggested technique utilized for lessening this attack. They suggested a new One-Way Code Attestation Protocol (OWCAP) for this wireless network for the recognition of the merits and demerits. The suggested technique is performed effectively as it minimizes not only the Sybil attack but also major attacks present in this network.

Bayrem TRIKI, et.al (2014) proposed a system using which Sybil attacks in MWSNs is detected and prevented easily. There are 2 categories of authentication techniques that are utilized to identify the Sybil attacker. For the authenticity of Soldiers, they embedded the RFID tags in the first part for the certification. In the second case, the soldiers utilize the certificates to show their authenticity to their neighbors [37]. Therefore, using this technique, this attack is prevented from the network as the soldiers 2 certificates at the same time. The authentication of soldiers is proved by the heartbeat of the soldier use as authentication soldier's team leader are the only using which Sybil attack is detected by preserving the privacy of soldiers. This helps in detecting the attack with the identification of real identity of the soldier.

P. Raghu Vamsi, et.al (2014) presented with the advent in the technology, there is developments in the WSN technology. The communication in this network is open due to which this network suffers from various attacks. There are very limited lightweight models in the existing solutions [38]. Therefore, they proposed a LSDF for diminishing its affects. Two components are included in this framework such as evidence collection and evidence validation. The activities of neighboring nodes are observed by each node for collecting the proofs. They run the sequential hypothesis test in order to authenticate the method and to know the position of the node whether it is benign node or Sybil node.

Bin TIAN, et.al (2013) presented due to the emerging technology, there is development in the microelectronics technology and wireless communication technology using which low power,

low price, multifunction sensor, and WSNs can be developed easily. The exchange of data here is completely done in open manner which causes unauthorized users to enter it. Therefore, security is the major issue in WSN. The distribution of nodes is done across the region that is to be monitored in such manner that the dynamicity is maintained. Sensor nodes have finite resources and battery power due to which this network is breakdown sometimes. In this network Sybil attack is more important in comparison with other. They proposed Sybil detection methods based on ranging in WSN [39].

Xun Li, et.al (2013) presented currently there is development in the Underwater WSNs because of its widespread applications in different applications. Therefore, security is imperative issue for this network [40]. Sybil attack is common and harmful attack. Therefore, for detecting the Sybil attack, it is required to propose an effective method. Hence, they suggested a new method for detecting the Sybil attack for which MATLAB tool was used. The obtained simulation result shows that the suggested technique was effective using which this attack is detected effectively.

James Harbin, et.al (2011) presented there is need of enhancing the WSN technology as it has finite energy efficiency and signal jamming attacks. Therefore, the Distributed beam forming clusters are proposed using which this technology can be improved. There are smaller numbers of nodes participating in transmission process and cause link failure within the network [41]. The communication in this network is open due to which it has more susceptibility for attacks in which malicious nodes exaggerate their identities. For measuring the impact of these nodes, they presented an analytic model.

BinZeng, et.al (2010) presented the WSN has been widespread application in almost every field. Therefore, security of the network is taken as essential factor for instance, in peer-to-peer networks. There are major attacks that affect the working of the network and Sybil attack is one among them. It is the attack in which fake multiple identities are created by the distributed system and show that they are multiple and separated nodes in the system. If the malicious node tries to fool the honest node, then there exists an edge between a Sybil node and an honest node. They recommended a new protocol using which Sybil attack affects are minimized in which ant colony optimiDtion (Am) algorithm is used [42]. It is the algorithm in which nodes are randomly distributed where they can leave the network or join at any time. The trails of the first node left on each node become diluted due to this random work after which it is fades away at the end of the routing. The number of edge attack can be limited effectively and

efficiently on the basis of the nature of the Am. Therefore, with the help of this technique it is ensured that honest node must be accepted with high probability and the Sybil nodes are rejected at greater extent.

Shanshan Chen, et.al (2010) proposed the Wireless Sensor Network has the widespread application in almost every field due to which is more popular currently [43]. There are major issues faced by this network such in the condition of maximum number of cluster-heads is over a threshold in Wireless Sensor Network than this technology has been utilized. Experiments were performed in order to compute the presented technique with regard to the security and energy consumption.

Ren Xiu –li, et.al (2009) intended a technique for detecting the Sybil attack easily in terms of ranging. The neighbor nodes range is checked out by every node available within the network for identifying the malicious node [44]. There is exchange of information between the nodes using which Sybil node is recognized easily. With performed experiment, it is concluded that propose method has performances in comparison with other methods. This intended technique is less costly and provides accuracy but is extremely precise. Therefore, this technique is used mainly for the low-cost network and which has limited resources.

Annie Mathew, et.al (2017) proposed which communication within a shortest range is accomplished easy that makes the sensing process easier [45]. Security is the major issue in this network as a result of its open communication environment. Several attacks are present in this network that affects the networking capability of the network such as sinkhole attack, wormhole attack, grayhole attack and many more that affects the functionality of sensor node. There exists a shortest path by the sinkhole node in between the sink or destination node due to this sinkhole attack within the network. There are various methodologies proposed so far by many researchers using which sinkhole attack can be detected easily. Therefore, they discussed the sinkhole attack along its classification and methods using which this attack is detected using the parameters.

Mahmood Alzubaidi, et.al (2017) presented those various kinds of internal attacks are discussed for the clear understanding and also discussed their effects. This sinkhole attack and their attack on the RPL are mainly discussed [46]. They proposed various mechanism and IDS in order to detect the sinkhole attack easily. They analyzed and studied each mechanism for highlighting the FPR and resource consumption with their advantages and drawbacks. They

showed a table which gives the previous representation for the detection mechanisms for sinkhole attack. After comparison the most effectual method was observed.

Manpreet kaur, et.al (2016) presented because of the progress of the technology, there is development in the WSN has been utilized in various applications such as public and military area. There are numerous sensor motes utilized in this network which has the limited resources in it. These nodes include the sink and low cost, low power sensor nodes with the help of which monitoring are done [47]. The small size and large quantity of sensor nodes within a network is the reason due to which these networks are more affected by the attacks. Therefore, sinkhole attack is the most destructive routing attack among. All the routing information is captured by this sinkhole attack and advertised by the malicious node using which nodes are forced to route the data towards it. Therefore, there is degradation in the network's performance caused by the adverse effect of the sinkhole attack. Thus, to perform the analysis and detect the sinkhole attack in WSN is the main objective.

Gauri Kalnoor, et.ai (2016) presented there are number of sensors node are embedded in the Wireless Sensor Network that are distributed randomly in the network. A variety of parameters including the pressure, temperature, motion, sound and many more that are monitored and the environmental conditions. Sensors are utilized to pass out all the information throughout the network. There is the maximization in the internet traffic in the condition of increases in the network size and the number of nodes. Security is main issue network due to major attack as the communication within this network is open due to which security plays a vital role in saving the essential information [48]. Therefore, with this security concern they used the IDS. The major challenge faced in the Wireless Sensor Network is the consistent QoS assistance such as reliability, congestion control and end-to-end delay. There is various security routing algorithms that has been utilized for protecting the QoS of WSN and also used to detect the intruder. They discussed various routing algorithms in order to enhance the network performance.

Jianpo Li, et.al (2018) studied about the wormhole attack and reviewed what kinds of aftereffects are caused when it occurs. They proposed AWDV-hop that is a secure mechanism, using which various issues are tackled easily and also the effects of the wormhole attack [49]. They created the neighbor node relationship list (NNRL) by utilizing the broadcast flooding used by the first algorithm. NNRL helps in assigning certain IDs to the nodes that surround each other. The theoretical and actual number of the neighbor nodes was compared for

recognizing the imagined beacon nodes. Utilizing this imagined beacon node, the distance to another beacon is calculated within the NNRL. It is possible to recognize the attack that was actually performed. Here, marks are placed in the scenarios. Some unknown nodes are available as well which also mark themselves as beacon nodes. The outcomes are achieved by simulating the suggested method.

RanuShukla, et.al (2017) presented the WSN an emerging technology due to which it has been utilized in almost every field. It is the popular technology because of its widespread applications. Several areas make the deployment of this technology. Security is main concern as it includes open communication environment therefore it is more inclined to the attacks. Along with security, several problems are being faced commonly in these networks which result in slowing down the overall performance. The environment remains no longer secure for exchanging the data amongst users [50]. The involvement of secure routing algorithm is required within these networks. Designing an appropriate protocol for a particular scenario is also more challenging. For providing the security to the WSN, the technology of the cryptography is not possible to utilize as it is heavy. Therefore, for dealing with this major issue they proposed an optimal solution called as TESRP. Even though the attack is not prevented from occurring here, this is known as the best trust-based protocol available. The sequence number is used with the trust algorithm for offering secure scenario within the networks.

Bharat Bhushan, et.al (2017) discussed that a few physical constraints of a specific region are computed by deploying a sensor network that uses wireless communication mode to transmit the data across its nodes. However, the communication being performed is free due to which this network is not much secure [51]. The chances of an attack to occur in the network are high. The users have highly private data that needs to be sent or received. Thus, a secure scenario must be provided. An attack in which no nodes are affected but the important information is stolen is called wormhole type of attack. The bits that are being forwarded across the network are tracked down through malicious user and then replayed. There is only one path available using which it is possible to transmit the data across the network. This path is however, wormhole. The user however, transmits the data through this path and the data is no longer secure. To provide a secure scenario inside these networks, it is esential to propose a novel design. This design helps in providing an environment in which data can be exchanged securely.

Mayank Kumar Sharma, et.al (2016) presented the WSN is termed as the scenario that provides communication by linking nodes amongst themselves. The physical conditions are sensed by applying the sensor nodes in the hostile environment. Therefore, the implementation of routing algorithm is required to create a suitable path. This is employed to forward the data packets across the network. Depending upon the constraints of network, routing algorithms are constructed. There are limited resources in this network because of which it is necessary to have efficient and fast routing process that minimize the resource overhead [52]. The communication mechanism followed here is open due to which it is affected by various different attacks. They discussed the wormhole attack and considered it as major attack in comparison with all other issues. Therefore, they utilized the routing protocols for mitigating the effects of this wormhole attack. For ensuring that the rink is minimized, comparative analysis is made amongst the techniques that were designed earlier and the new designed approach. This paper aims to reduce the effects of high transmission power which are resulted as attack is present. They also introduced more methodologies using which all these issues are reduced easily.

Ali Modirkhazeni, et.al (2016) presented a major area has been covered by this technology. It is growing technology, has been utilized in a range of applications. Any kinds of physical constraints are recognized with sensing devices that are used in the regions that are to be monitored. The information is gathered by these sensing devices which are further transmitted to the base station to perform further processing. The battery in these devices is finite. Thus, wireless media was used in order to achieve this. The possibility of attacks to occur is high since the open communication scenarios are available. These attacks affect the communication of the entire network [53]. In this WSN network, the conventional security mechanisms have been not utilized as they are heavy and have inadequate nodes. They discussed the wormhole attack and considered it as the major attack among others as it breakdown the functionality of whole network. The attack scenario results in creating a tunnel from which the data is transmitted. Within the networks, it becomes very difficult to identify such an attack. This paper designs a new distributed network discovery mechanism that applicable easily. The outcomes achieved after conducting experiments clearly depict that the new designed approach is highly secure and keeps the attacks away from private data transmissions.

Swati Bhagat, et.al (2016) presented the widespread application of this technology is commonly utilized in almost every application nowadays. Today, diverse fields have been

deploying these networks to ease their work and provide improvements in their technologies. However, the surety that these scenarios are secure is also essential. For this, various attacks which can possibly occur in the network are studied and solutions are provided to prevent them from making any destruction. A wormhole attack also results in degrading the overall performance of network because of which solutions are present by applying which it is easy to remove it [54]. A wormhole can be recognized using a powerful transmission as per this proposed approach.

Mostefa BENDJIMA, et.al (2016) reviewed that lately, Wireless Sensor Networks applied commonly within various fields. Using this technology, information is collected from different hostile environments by simply sensing. There are present various malicious threats that degrades the working of the network by affecting the nodes present within the network. There are various limitations such as limited resources, limited power source, large number of nodes, and infrastructures less, dynamic network topology that left various serious issues. The problems that are commonly being faced need to be solved which is done by introducing a new mechanism. Security is the major concern to obtain which they split the network into two sectors. They also utilized the mobile agents in order to reject the traffic intruders which are the reason of having the wormhole attack [55]. Attack is triggered which causes huge impact on the performance of network. To secure the network, the research is proposed through which a new technique is designed. They used the SINALGO simulator for this purpose. Experiments are conducted which help in evaluating what improvements have been made.

ShaoheLv, et.al (2008) presented the communication in the wireless network is open and it is an infrastructure less network. Sybil attack is the major attack discussed in this paper, it is the threat introduced by one or more malicious node due to which network is collapsed the network applications [56]. They proposed a new detection mechanism called as CRSD in this paper for static wireless sensor networks. In this network, the received signal strength (RSS) has been utilized to understand the distance between two identities. With the help of this RSS information the position relation of the interesting identities can be determined easily as this information taken from multiple neighbor nodes. In the condition of the same position, more than two identities are detected by the Sybil attack. Therefore, the system performance is degraded by this attack after doing analysis. They performed simulation for the evaluation of the method and concluded the effectiveness of CRSD method by which effective performance is provided.

Jiangtao Wang, et.al (2007) proposed a new method using which Sybil attack can be detected easily in the wireless sensor network (WSN) on the basis of received signal strength indication (RSSI). The real network space situation of WSN is followed in which Jakes channel model is established that estimated the effects of Sybil Attack [57]. They also proposed two methods in this paper with the help of which Sybil attack on head nodes and member nodes can be minimized. There are wide range of applications offered by this method and also achieve effective results.

3.2 Sinkhole Attack Detection Techniques

Huda A. Babaeer, et.al (2020) suggested a lightweight, secure technique on the basis of Threshold Sensitive Energy Efficient Sensor Network protocol and watermarking methods for ensuring the data integrity during its transmission [58]. A less power was consumed when the sensor nodes were recognized using a quick and effective technique named, HE (homomorphic encryption). Hence, the sinkhole attack was detected. The OMNET++ was implemented to quantify the suggested technique so that its performance was computed with respect to delay, PDR (packet delivery ratio) etc. The outcomes depicted that the suggested technique was led to improve the security for which it detected the sinkhole attacker node prior to launching the attack.

Guangjie Han, et.al (2015) intended a new IDASA (Intrusion Detection Algorithm based on neighbor information against Sinkhole Attack) [59]. Unlike the conventional algorithm, this algorithm utilized the neighbor information regarding sensor nodes for detecting the sinkhole nodes. The MATLAB was applied for computing the intended algorithm concerning accuracy to detect the malicious node, PLR (packet loss rate), power utilization etc. the simulation results revealed that the intended algorithm performed more efficiently in comparison with other algorithms. Moreover, this algorithm was capable of balancing the power consumed by the sensor nodes due to which the duration of network was maximized.

U Prathap, et.al (2016) projected a solution PCAD (Power control attack detection) for detecting the malicious nodes that activated the sinkhole attack in WSN (wireless sensor network) [60]. The data was forwarded in various rounds which were divided in equal time duration. A parent node was selected by every node at the initialization of the round to transmit the packet towards the base station. The child node was responsible for observing the parent, handling the acknowledgement from 2-hop distance node and deciding the trust on parent on

the basis of successful and unsuccessful transactions. NS-3 tool was applied for simulating the projected algorithm and comparing it with other methods. The simulation results exhibited that the projected algorithm had potential for detecting the malicious nodes in efficient manner and in advance.

3.3 Techniques for the Prevention of Sinkhole Attacks

K. Karthigadevi, et.al (2019) introduced a new decentralized approach for preventing and detecting the sinkhole attack named NDET (Network Density Estimation Technique) [61]. All the nodes utilized this approach for maintaining the neighbor table so that the details of neighbor were stored. This detail was gathered through every node. The network density was estimated and the availability of malicious node was recognized in the region with the help of these factors. This distribution of this information was done among the neighbor nodes in order to ignore the malicious node in the further transmissions. The introduced approach was assisted in diminishing the overhead and maximized the network throughput.

Prakash C Kala, et.al (2020) recommended a novel method of mutual authentication for recognizing and isolating the malicious nodes that launched the sinkhole attack through identity verification with the purpose of providing a secure environment to establish communication in the network [62]. NS2 simulator was exploited to deploy this method and conduct simulations. The simulation results indicated that the recommended method outperformed the other techniques. This technique mitigated the packet loss, delay and maximized the throughput.

S. Ranjeeth Kumar, et.a; (2016) developed a generic specification based IDS (intrusion detection system) known as SSLEACH (Low-energy adaptive clustering hierarchy) for resisting the sinkhole attack in WSN [63]. A more security was added to the LEACH protocol with the objective of protecting the network using least energy consumption and higher PDR (packet delivery ratio). NS2 tool was utilized for performing the simulation on this technique. The results validated the superiority of the developed approach over tradition techniques in terms of energy consumption, PDR (packet delivery rate), overhead and residual energy.

3.4 Défense against Sinkhole Attack

Ghazaleh Jahandoust, et.al (2017) established a distributed adaptive model on the basis of subjective logic and probabilistic extension of timed automata for investigating the probability

of each node at which the sinkhole attack was occurred [64]. The probabilities of the next hops of nodes were adjusted in the probabilistic extension of AODVv2-12 routing protocol for routing the packets over the most reliable nodes. The probabilities iteratively were evaluated on the basis of positive and negative observations related to the behaviors of nodes using subjective logic models. An efficient adaptive algorithm was attained by integrating traditional models that had robustness for the dynamics of network with low PLR (packet loss rate) due to the selection of routes over the reliable nodes. Moreover, the FNR and FPRs were mitigated with the convergence of network.

Abdul Razaque, et.al (2017) designed a SDAACA (secure data aggregation using the access control and authentication) protocol for detecting the sinkhole [65]. Two novel algorithms were contained in this algorithm known as SDF (secure data fragmentation) and NJA (node joining authorization). The initial algorithm assisted in hiding the data from the adversary. The latter algorithm employed an authorization process prior to allow the entry of any new node in the network. The simulation results exhibited that the designed protocol was effective for mitigating the sinkhole attack.

M. T. Kurniawan, et.al (2017) emphasized on planning a defense against sinkhole attack for Wireless Sensor Network on the basis of a general path attack path [66]. Afterward, a defense strategy was introduced for matching the distribution of resources in order to generate a realistic defense strategy. The attacked phases were monitored in order to localize the focus of attack at every phase. The efficiency of the introduced strategy was proved for preventing the attacker from launching the sinkhole attack on the system.

Chapter 4

Proposed Work

4.1 Research Methodology

The performance of the network is reduced due to the presence of malicious nodes. This malicious node causes black hole, wormhole attacks just by entering inside the network. The Sinkhole is one of the most common active types of attack in which attacker node floods the rough packets and keeps the sensor nodes busy in sending the route packet reply. In this work, the isolation of malicious nodes when it enters in the network has been proposed. The technique works according to the following steps: -

Step1: The network contains finite number of sensor node.

Step 2: While loop will be executed in each node in the network.

- Base station will determine the node localization by using node localization process.

- Each node is assigned with the unique Armstrong number by the base stations.
- Unique ID is also assigned to every node by the base stations.

  While End

Step 3: Cluster heads developed is start in the networks.

- The cluster head is selected in the network on the basis of distance and energy
- The unique ID, Armstrong number of volunteer nodes are then send to the base station.
- Execution of if loop takes place.

Step 3.3.1 all information matched

The node is select as cluster heads

Else

Node gets isolate

4.2 Aim of this Research

The sensor nodes deployed in WSNs sense information from the nearby environment. Thereafter, the information sensed is forwarded to the base station. WSNs are decentralized type of networks which have no central controllers. These controllers are responsible to find malicious nodes in the network which trigger various types of active passive attacks within the network. The sinkhole attack reduces the performance of network in the context of throughput, energy consumption and packet loss. The malicious nodes are flooded by the sinkhole attack on the channel in which communication takes place. This research is completely based on the detection of malicious nodes which activate sinkhole attacks in WSNs.

4.3 Objectives

This work has following objectives:

1. To study and analyze various schemes for the detection of sink hole attack in wireless sensor networks.

2. To present a new method for the detection of sinkhole attack in a WSN.

3. To deploy new scheme and compare it with existent schemes in terms of certain parameters.

4.3.1 Explanation of Flow Chart

Figure 6 illustrates the proposed methodology in the form of a flowchart.

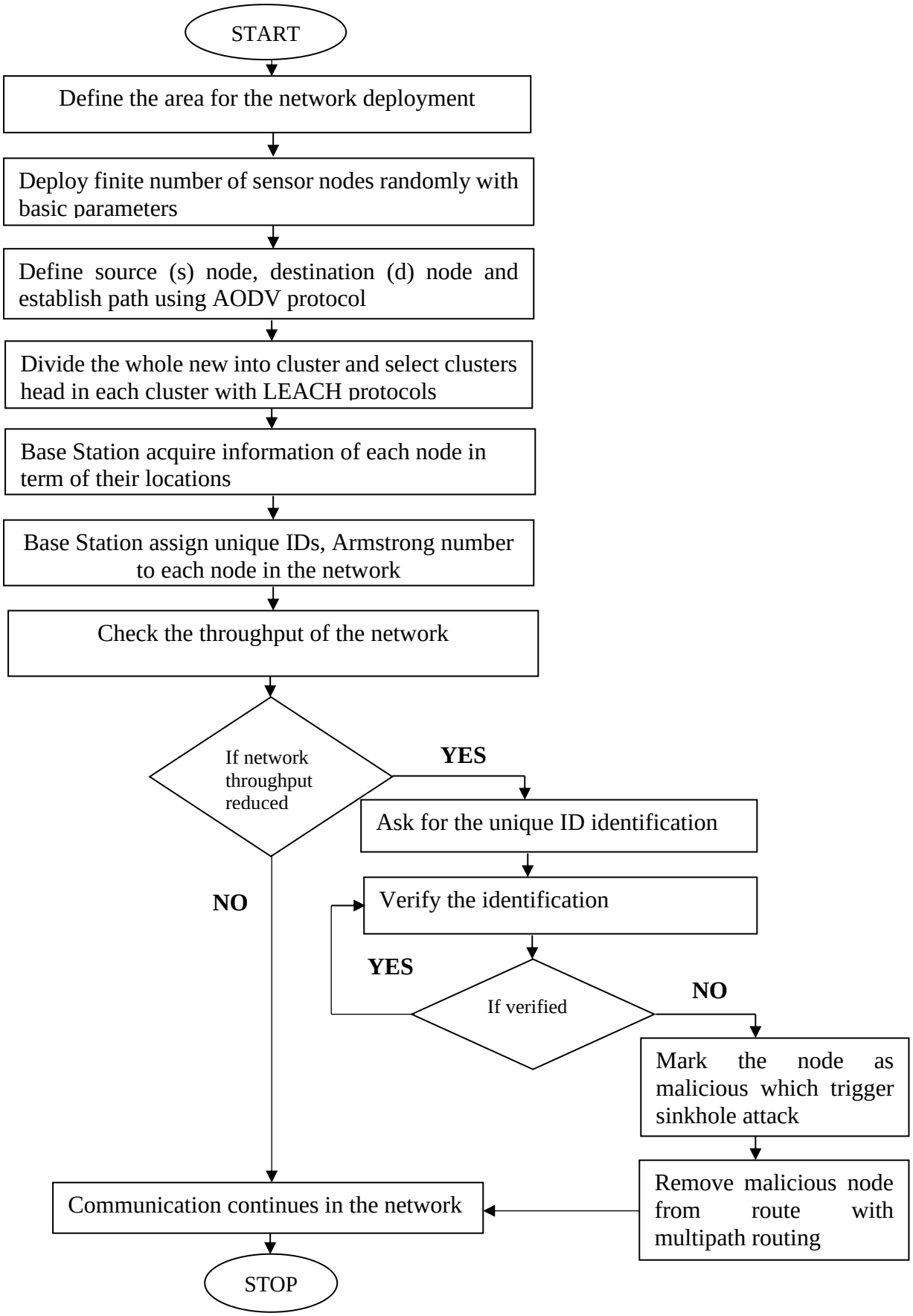


Figure 4.1: Proposed Flowchart

The different steps of proposed approach are explained below:

1. Network Deployment: WSN is a self-configuring type of network in which sensors node sense the information and passes the information to base station. Such types of networks, various types of active attacks are possible in the network. Among all the type of attacks the sink hole attack is the attack which is difficult to detection and isolation from the network due to its unique properties.

2. Key Distribution of the Base station: The novel approach is implemented in this research work for the detections of malicious node. In techniques of intrusion detection system, require extra software for the detection of malicious nodes which affect performance of technique for the detection of malicious nodes. The second technique which is popular for the detection of malicious nodes is the Delphi technique. This technique does not include any parameter of quality of service due to which we are not able to detect malicious nodes accurately. The technique which is proposed in this research work does not require any extra software and also includes the quality-of-service parameters for the detection of malicious nodes.

In the proposed technique, the sensor nodes are deployed in the finite area with the basic configuration. In the network, the source and destination nodes are defined randomly and also the path from source to destination is selected with AODV protocol. The AODV protocol is the reactive routing protocol; in which source node send the route request packets and nodes which are adjacent to destinations replies back with the routes replies packet. The paths from sources to destinations is selected on the basis of hop count and sequence number. In the communication, the malicious node spoofs the identification of the base station and sensor nodes pass data to malicious node instead of base station. The base stations perform the task of node localization and key distribution. The base station distributes keys to all sensor nodes in the network and also define the virtual keys. The sensor nodes when transmit the data to the base station, it will ask for the unique key of the base station. The base station calculates the key with Armstrong number. The Armstrong number is calculated with equation number 1, 2 and 3.

First number (n) = $\int_{i=0}^{i=n} node\ number\ mod\ 10$ --- (1)

Second number (n) = $\int_{i=0}^{i=n} first\ number * first\ number * first\ number$ -- (2)

Armstrong Number (n) = $\int_{i=0}^{i=n} Second\ Number\ /10$ --- (3)

In the equation 1, the node number is taken as input and maximum number of nodes which considered in the network is 10, the first value which is calculated in each 1 is used in equation 2 for the calculation of final Armstrong number.

3. Detection of Malicious node: - The original base station is able to provide its identification but the malicious node is not able to provide its identification. When the malicious node is not able to provide its identification, it is detected as the malicious node. The keys which are distributed in the network, to generate such keys the concept of Armstrong number is applied in this work. The Armstrong number is the unique number 16 bits which is generated from the various color combinations. The 16-bit Armstrong number of hard to crack and also the unique identification of each node is concatenated with the key to form final key.

4. Isolation of Malicious nodes: - Multipath routing is performed at the end which helps in removing the malicious node completely from the network. An echo message is sent to all of the nodes that exist in the network in case when a malicious node is recognized. It will remove malicious node from the network through the multipath routing.

$$(\emptyset|r)=(\sum_{j=1}^{N} r(j)p(j))/\ (\sum_{j=1}^{N} Nr(j)p(j))\text{----(4)}$$

Where, N is the number of disjoint paths between the source and the sink, and p(j) is the product of the path cost, which is the sum of the individual link costs along the path j. $\bar{r}$ is the Nr(j) allocated to the available routes and r(j) is the Nr(j) allocated to the path j. When the malicious node is detected from the network, then the source node which detect the malicious node will inform all the nodes about the malicious nodes.

1. Input : Sensors node, Malicious node

2. Output : Establishment of secure path

1. Source send the route request messages to all sensor nodes in the network

2. The sensor nodes which are adjcant to destination reply back with the reply packets

3. Check the route reply messages

    If (route reply comes from the malicious nodes)

    Discard the route reply

    Else

    Process the route reply

4. If route reply process ==true

    If (main nodes exist in the paths)

    Discard the paths

    Else

    Proces the paths

5. Select the better paths on the basis of hop counts and sequences numbers

Chapter 5

Result Analysis

5.1 Result Analysis

This research work is focused on finding the spiteful motes from WSNs. There are various performance analysis parameters like energy utilization, throughput and packet loss. Table 1 consist of some simulation specifications.

Table 5.1: Simulation Specifications

Parameter	**Value**
Nodes' amount	100
Area	800*800 meters
Standard	802.11
Queue Type	Priority Queue
Queue Size	50
Antenna Type	Omi-directional
Range	18 meter

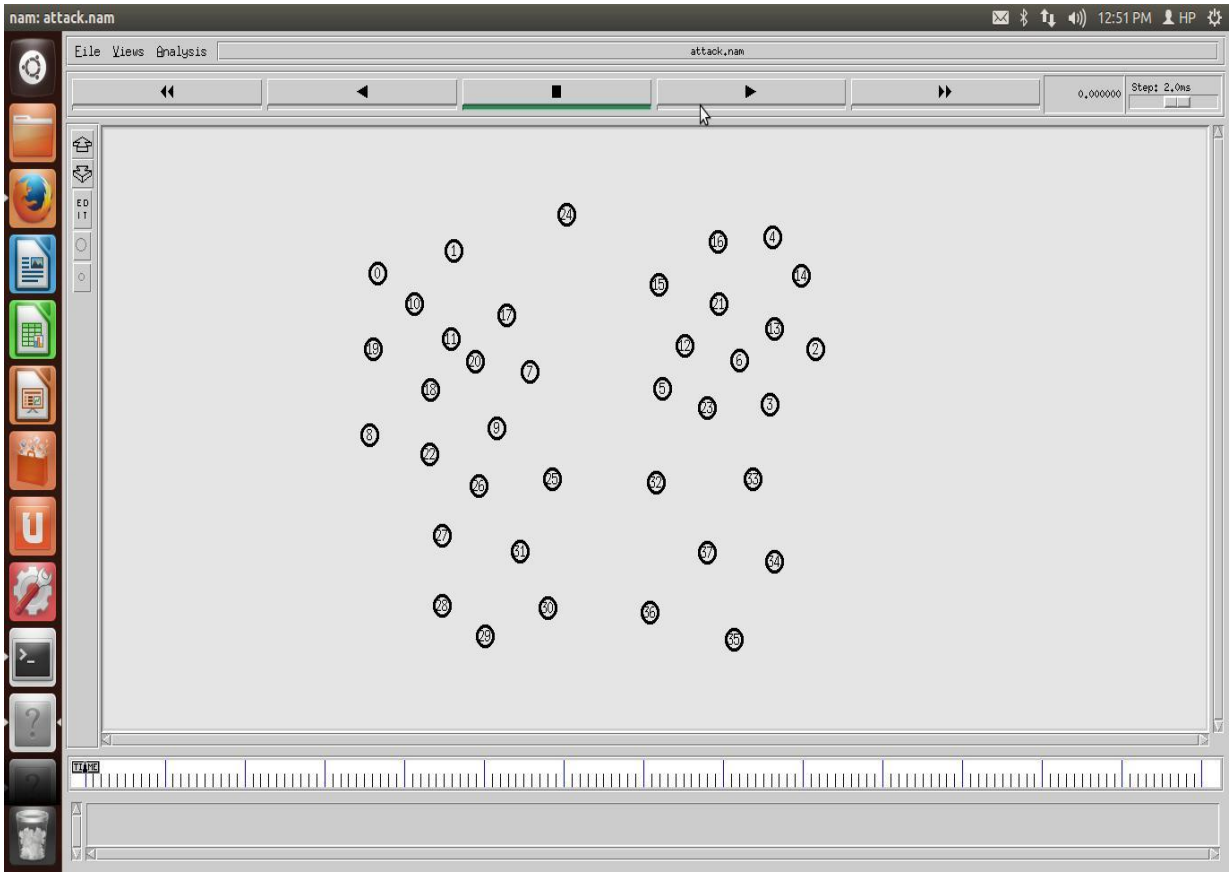


Figure 5.1: Network Deployment

As evidenced in fig. 5.1, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location.

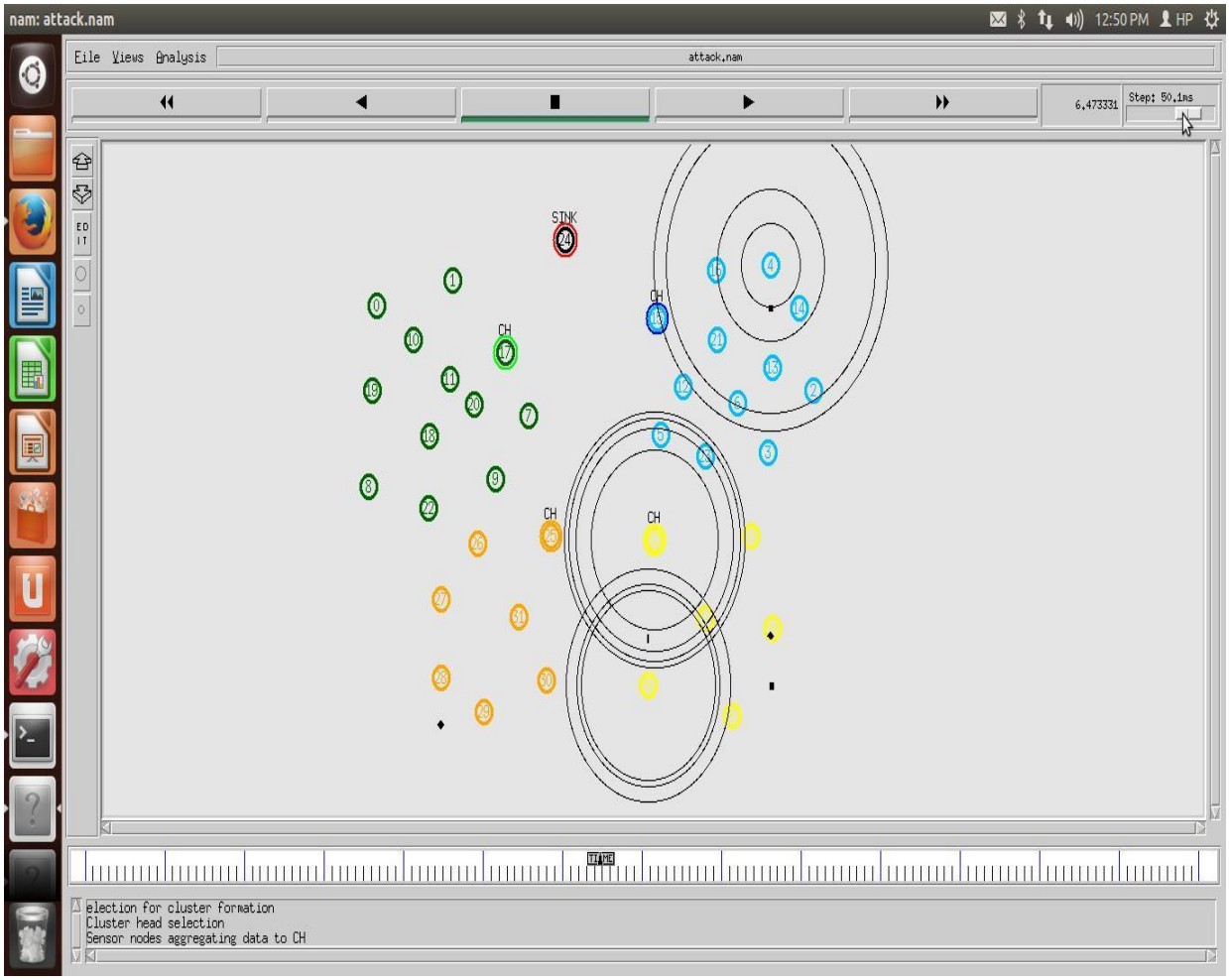


Figure 5.2: Network Deployment

As evinced in fig. 5.2, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH. Distance and energy are the deciding factors in the selection of cluster heads.

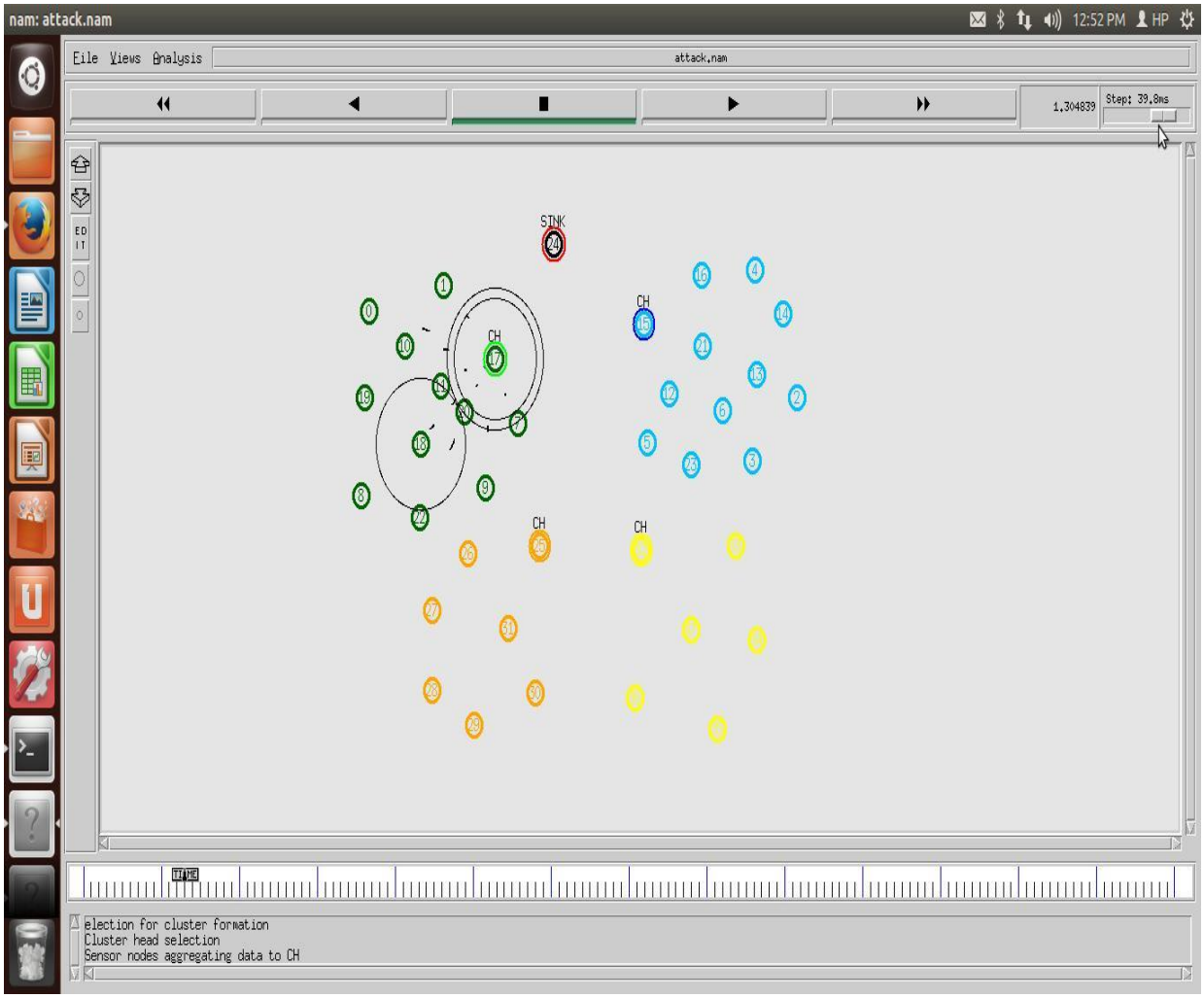


Figure 5.3: Data Aggregation

As evinced in fig. 5.3, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH. Distance and energy are the deciding factors in the selection of cluster heads.

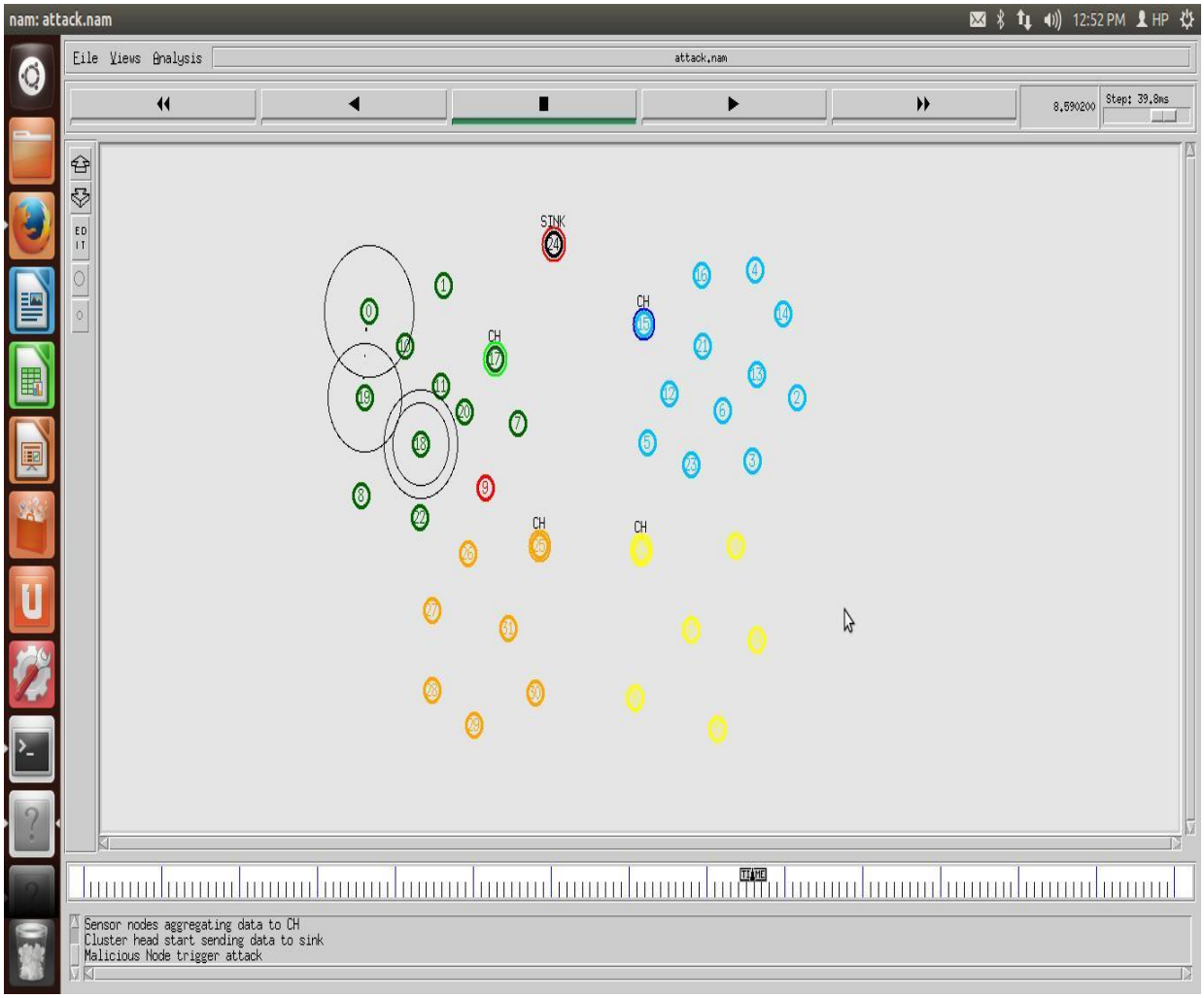


Figure 5.4: Trigger attack

As evinced in fig. 5.4, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH. Distance and energy are the deciding factors in the selection of cluster heads. The job of cluster head is to pass desired data to the base station. The two cluster heads in the network are connected through a direct route. The enroute attacker node can trigger the sinkhole attack.

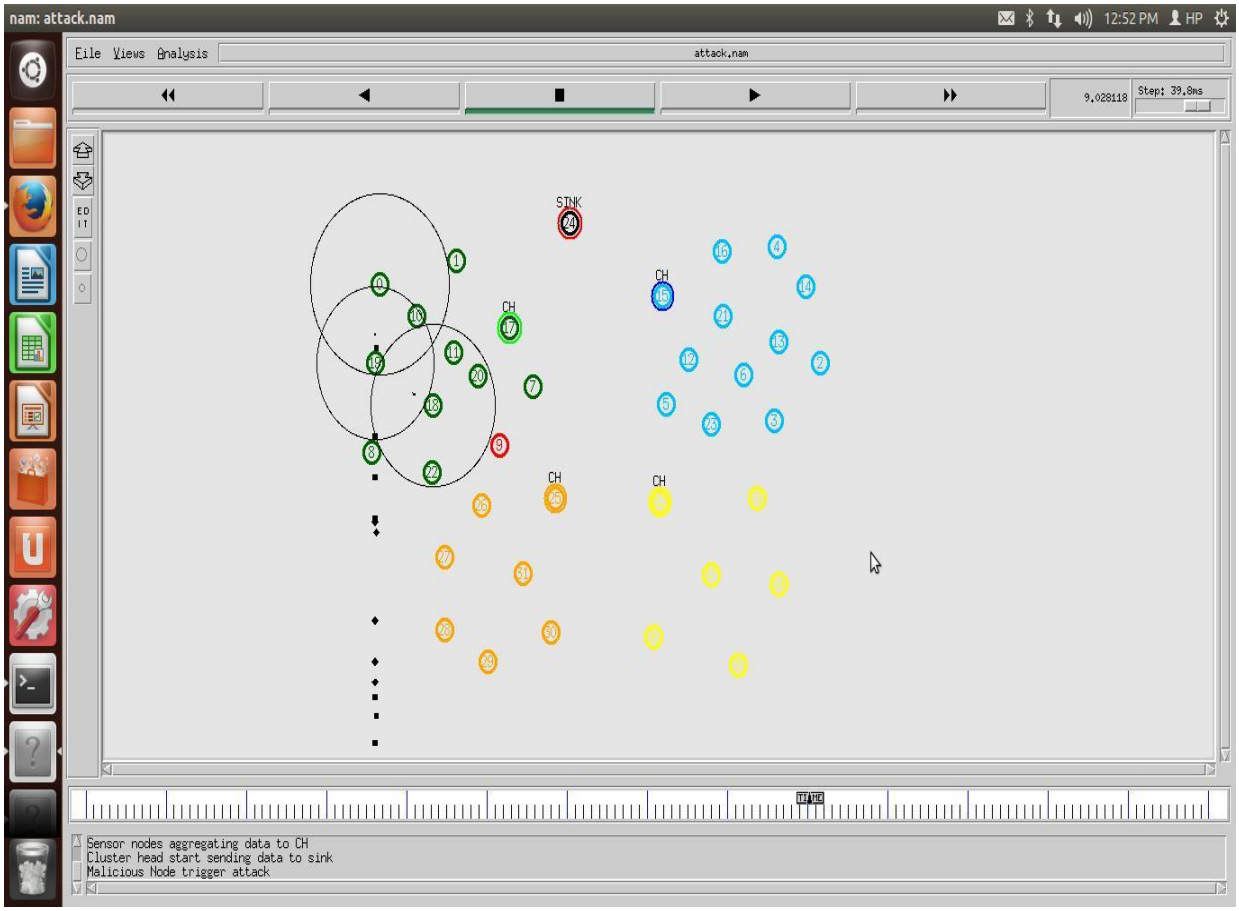


Figure 5.5: Trigger attack

As evinced in fig. 5.5, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH. Distance and energy are the deciding factors in the selection of cluster heads. The job of cluster head is to pass desired data to the base station. The two cluster heads in the network are connected through a direct route. The enroute attacker node can trigger the sinkhole attack.

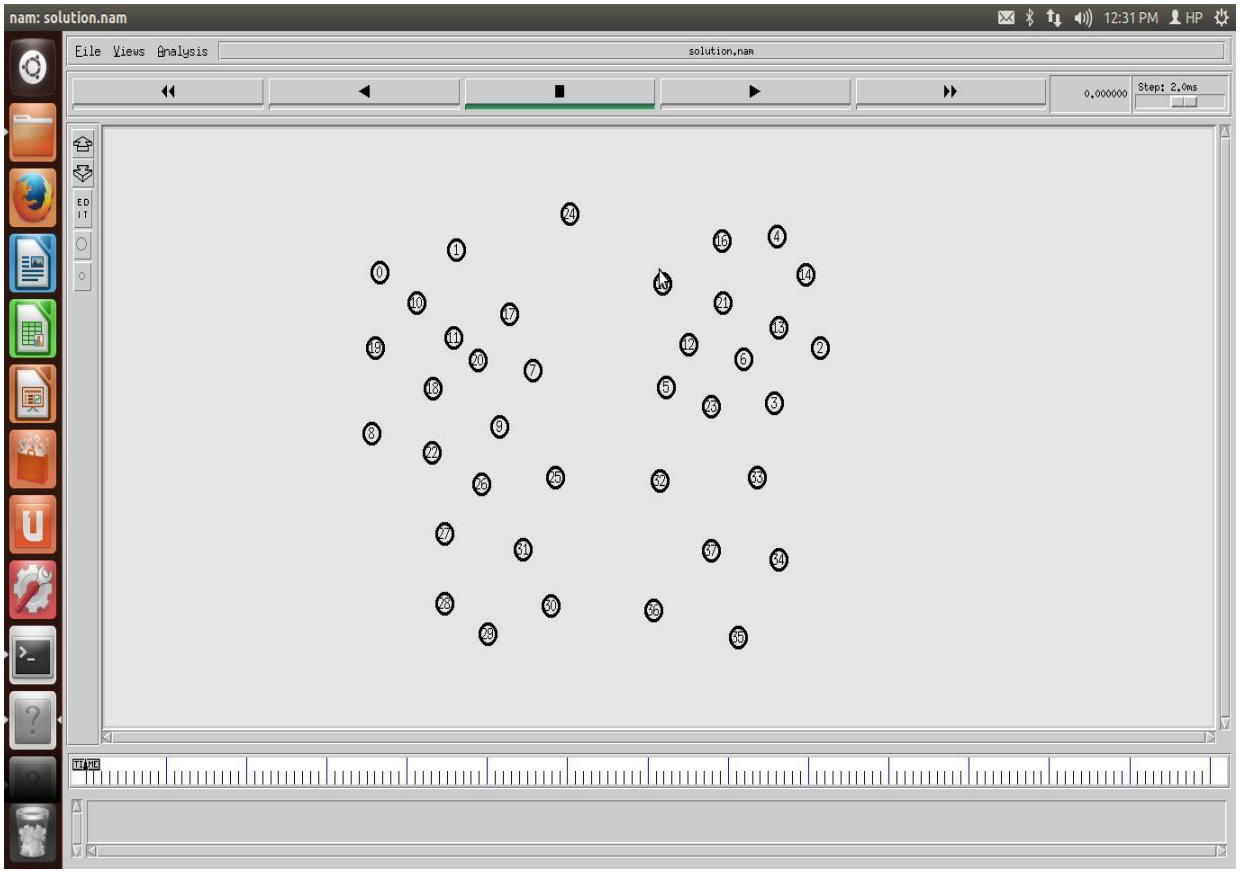


Figure 5.6: Deployment of Sensor nodes

As evinced in fig. 5.6, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH. Distance and energy are the deciding factors in the selection of cluster heads.

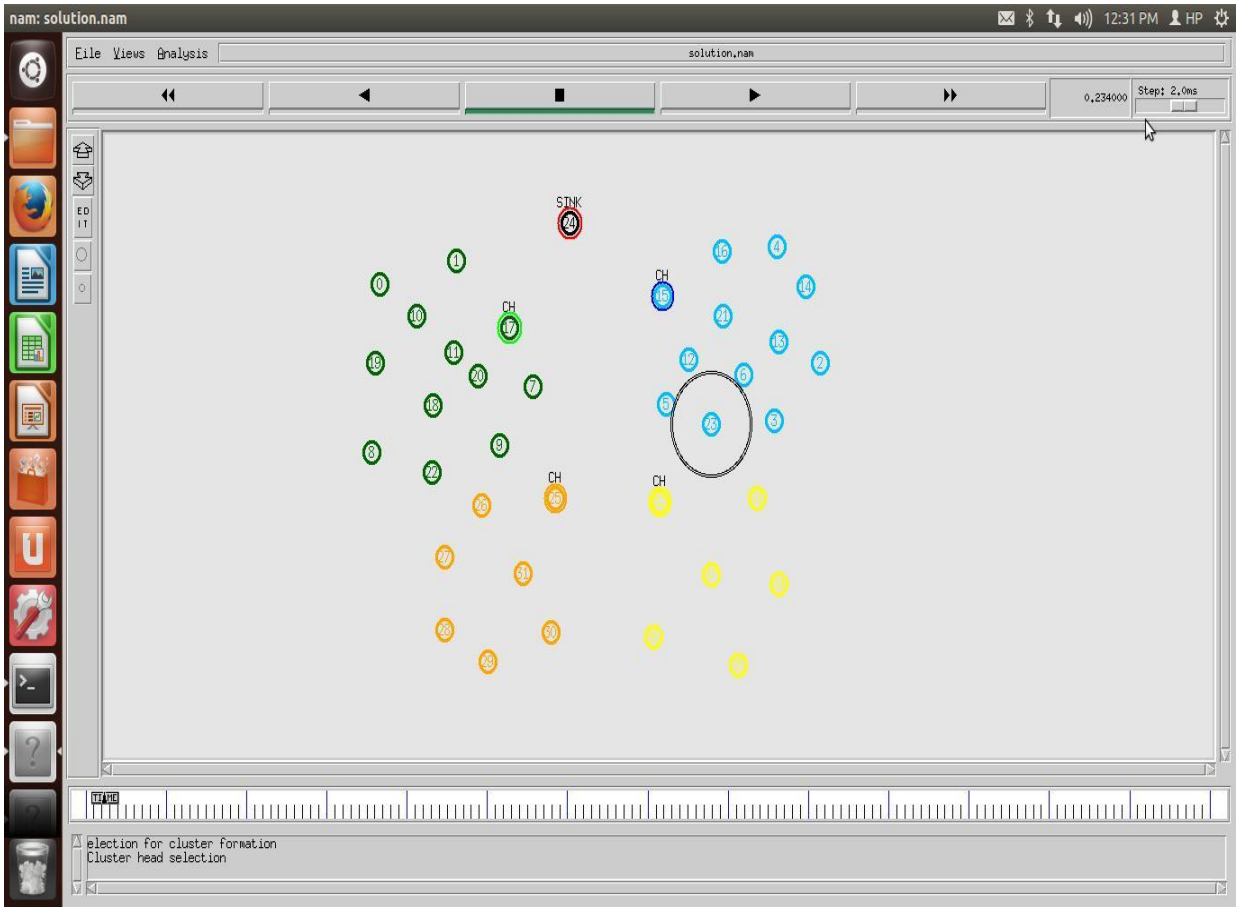


Figure 5.7: Deployment of Sensor nodes

As evinced in fig. 5.7, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH.

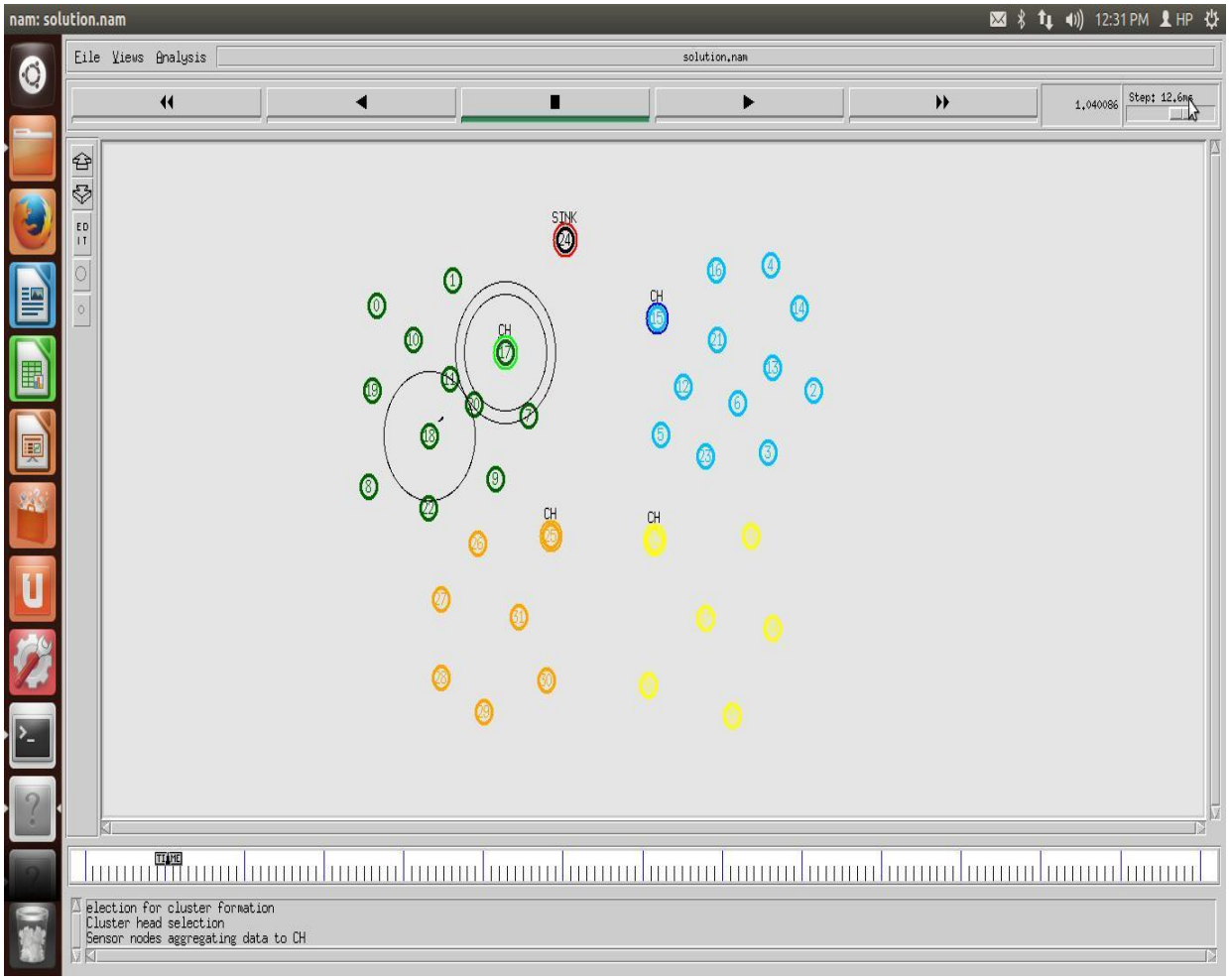


Figure 5.8: Finding assailant nodes

The whole network is divided into various amounts of sensor nodes as evinced in figure 4.9. Each sensing device has a unique ID assigned by the sink. A node without an ID is declared as the assailant node.

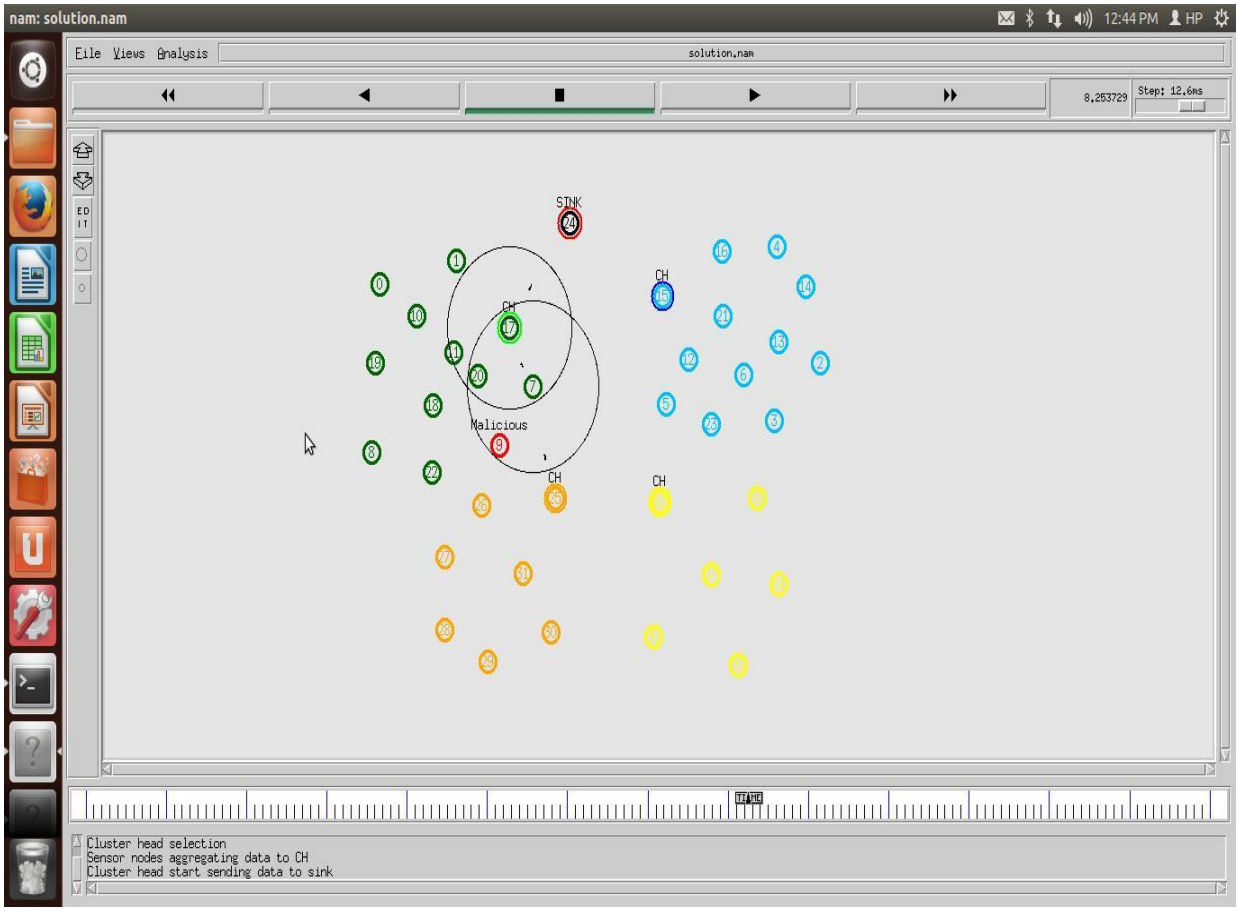


Figure 5.9: Malicious node isolation

As evinced in fig. 5.9, a WSN has sensor nodes in limited number. The whole network also has clusters of fixed size. The clustering approach applied in this network is based on location. To select cluster head, the protocol used in this work is LEACH. Distance and energy are the deciding factors in the selection of cluster heads. The job of cluster head is to pass desired data to the base station. The two cluster heads in the network are connected through a direct route. The enroute attacker node can trigger the sinkhole attack.

5.2 Comparative Analysis

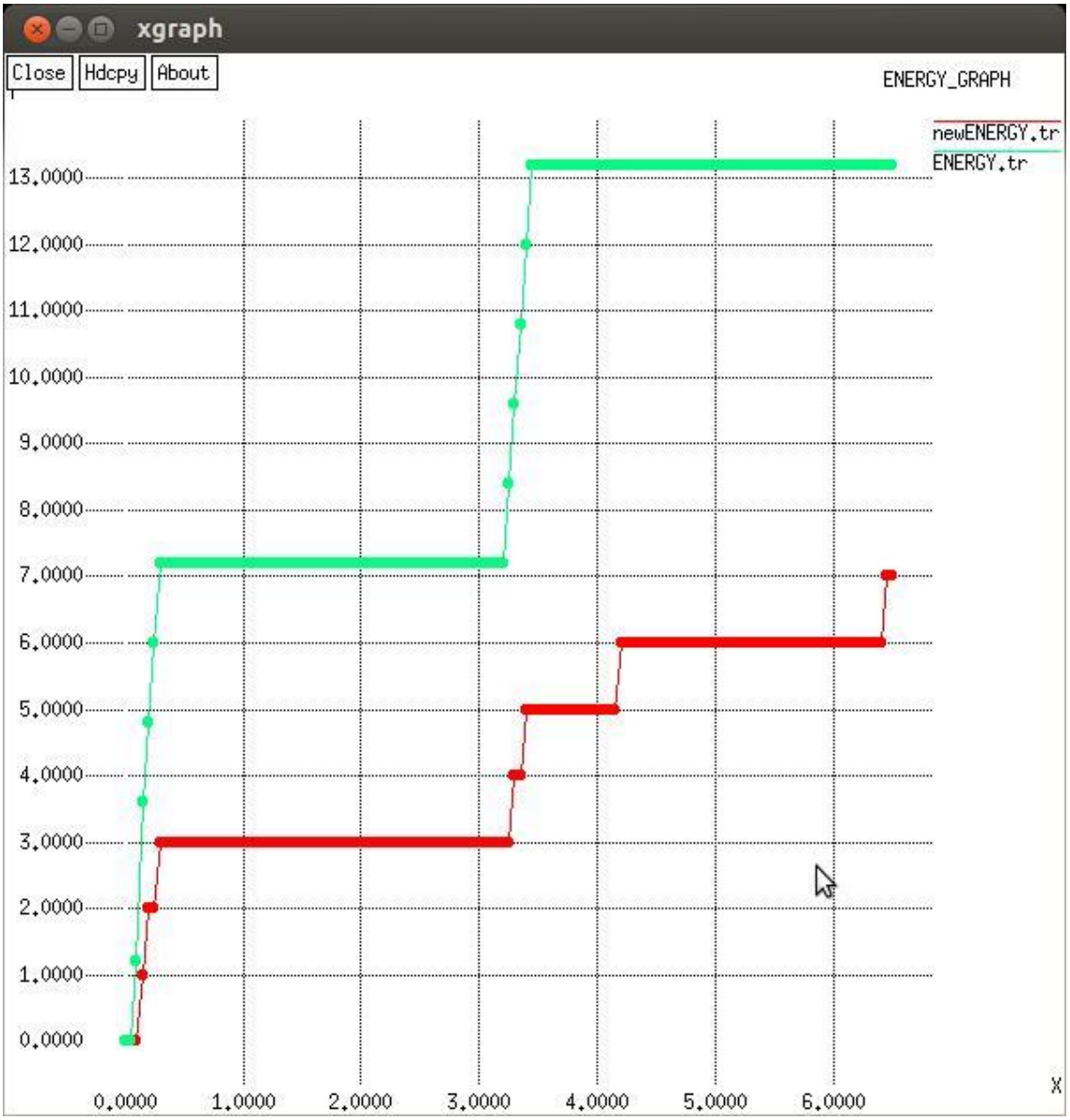


Figure 5.10: Energy Comparison

The figure 5.10 illustrates the energy consumption of the introduced model with the node localization scheme for the malicious node detection. It is analyzed that proposed model consume less energy for the malicious node detection as compared to existing model.

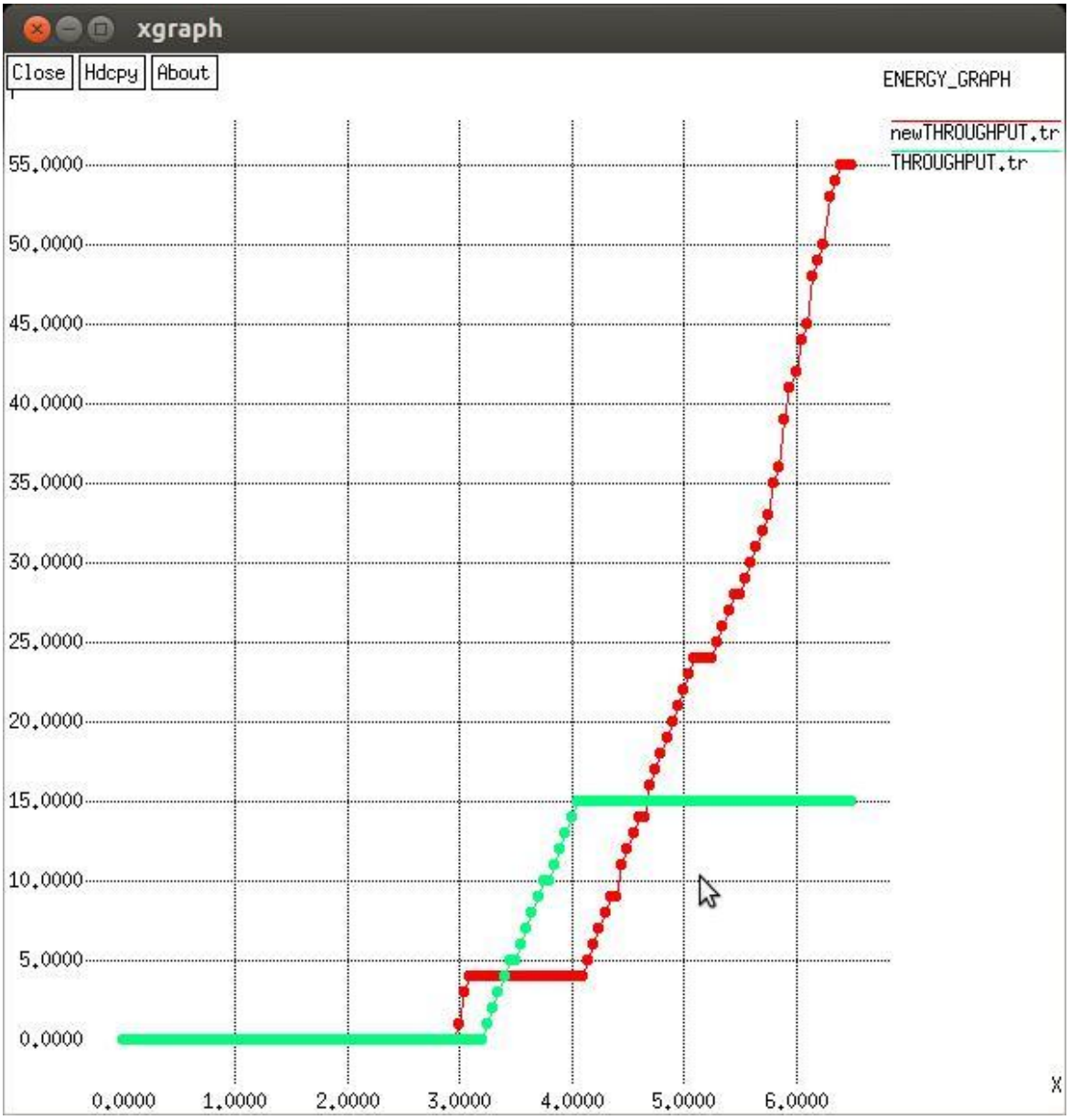


Figure 5.11: Throughput Comparison

The figure 5.11 depicts the comparison of the throughput of the introduced model with the node localization scheme. Post discovering the attacking node, the throughput rises to highest level.

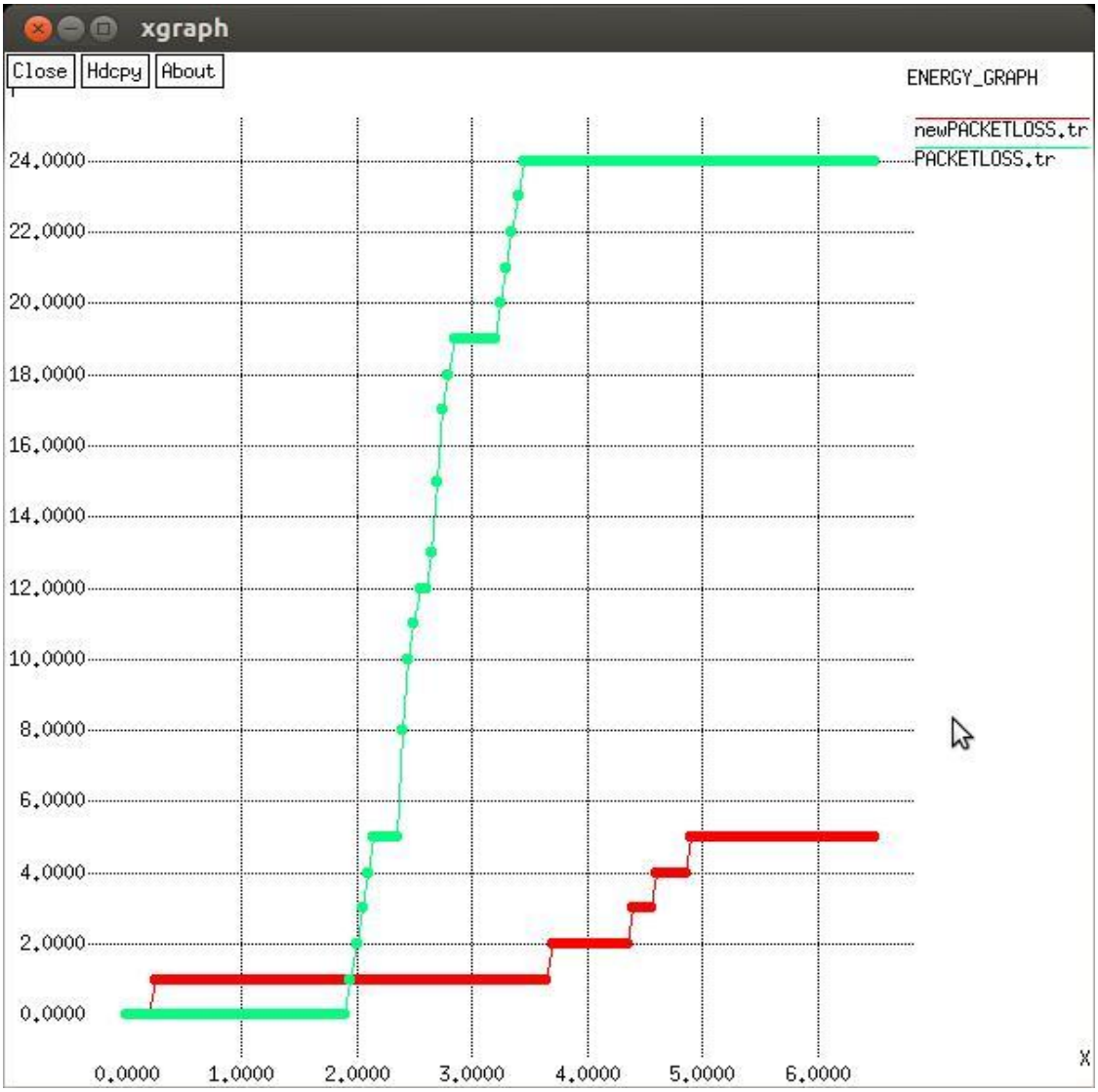


Figure 5.12: Packet loss Comparison

Figure 5.12 evinces that old approach is compared with the proposed scheme in the context of packet loss. The new model is better than the existing scheme in terms of this aspect.

5.3 Discussion

The sink hole attack spoofs the identification of the malicious nodes which affect network performance. The impact of sink hole attack is shown in the form of throughput , packet loss and energy consumption. Any malicious nodes available in the network can be recognized using the new technique. It detects malicious node and increases network performances in terms of throughput, packet loss and energy consumption.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In this work, it is concluded that the LEACH protocol is most effective technique used to reduce energy consumption of the wireless sensor networks. it is the network. The small sizes of sensor nodes are responsible for the reduced life time of these sensor nodes. The sinkhole attack is one of the active types of attack which reduces the LEACH protocol's performance. The technique of mutual authentication has been proposed in this thesis work, which detects and isolates the sinkhole attack. The outcomes achieved show that there is minimum packet loss and energy consumption rate achieved when the proposed approach is implemented. Further, there is improvement in the throughput value of network. The malicious nodes that exist in the network are identified and isolated completely from the network. Depending upon the threshold value, the delay per hop is analyzed by base stations. Depending upon the delays found in the nodes, it is possible to recognize the malicious node. A malicious node is considered to be the one which causes the highest delay. Thus, the proposed technique helps in reduction of energy consumption, increment in the throughput and reduces the delay time.

6.2 Future Work

The proposed approach can be implemented to detect various types of attacks like Sybil attack in the network. It can be used to make comparisons between the other secure techniques in order to test their reliability. In WSNs no central control is present which result in reducing the efficiency of the network since the security and energy consumption are affected. Sinkholes attacks is one of the actives type of attacks which reduces the performance of WSNs according to the various parameters being used. The framework can be designed in the future in which data aggregation is used to reduce the energy consumption of the network. This developed protocol can also be compared with other data aggregation protocols in order to check their authenticity.

REFERENCES

[1] S. Prasanna, Srinivasa Rao, “An Overview of Wireless Sensor Networks Applications and Security”, 2012, International Journal of Soft Computing and Engineering (IJSCE), Volume-2 Issue-2

[2] Chiara Buratti, Andrea Conti Davide Dardari and Roberto Verdone, “An Overview on Wireless Sensor Networks Technology and Evolution”, 2009, Sensors

[3] Navreetinder Kaur, Tarandeep Singh, “A Review of Wireless Sensor Network with Its Applications”, 2016, International Journal of Computer Science and Information Technologies, Vol. 7 (1), pp. 211-214

[4] Hong Tao ZHANG, “Key Technologies of Wireless Sensor Networks: A Review”, 2014, First International Conference on Advanced Algorithms and Control Engineering

[5] S. V. Chavan, B. P. Ladgaonkar and S. K. Tilekar, “An Overview of Sensor nodes for Wireless Sensor Network Applications: a review”, 2018, Journal of Emerging Technologies and Innovative Research (JETIR), Volume 5, Issue 1

[6] G.H. Raghunandan, B.N. Lakshmi, “A Comparative Analysis of Routing Techniques for Wireless Sensor Networks”, 2012, In Innovations in Emerging Technology (NCOIET)

[7] Arash Tayebi, Setevan Berber, Akshya Swain, “Wireless Sensor Network Attacks:An Overview and Critical Analysis”, 2013, 2013 Seventh International Conference on Sensing Technology

[8] Dr.Nipin Gupta, Dr. Sandeep Tayal, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, “Attacks on Wireless Sensor Networks: Review”, 2017, Advances in Wireless and Mobile Communications, Volume 10, Number 3, pp. 493-503

[9] Waleed Al Shehri, “A Surveyon Security IN Wireless Sensor Networks”, 2017, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.1

[10] Murat Dener, “Security Analysis in Wireless Sensor Networks”, 2014, International Journal of Distributed Sensor Networks

[11] Aqeel-ur Rehman, Sadiq Ur Rehman &Haris Raheem, “Sinkhole Attacks in Wireless Sensor Networks: A Survey”, 2018, Springer

[12] Ranjeeth Kumar, Sundararajan and Umamakeswari Arumugam, “Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks”, 2015, Journal of Sensors

[13] Ashwini V. Jatti, V. J. K. Kishor Sonti, “Intrusion Detection Systems”, 2019, International Journal of Recent Technology and Engineering (IJRTE), Volume 8, Issue 2S11

[14] Md. Ibrahim Abdullah, Mohammad Muntasir Rahman, and Mukul Chandra Roy, “Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count”, 2015,International Journal of Computer Network and Information Security, Volume 3

[15] Tejinderdeep Singh, Harpreet Kaur Arora, “Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool”, 2013, International Journal of Advanced Computer Science and Applications, Volume 4, Issue 2

[16] KesavUnnithan, Lakshmi Devi, SreekuttanUnnithan, “Survey of Detection of Sinkhole Attack in Wireless Sensor Network”, 2015, International Journal of Computer Science and Information Technologies, Volume 6, Issue 6, PP. 4904-4909

[17] Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia, “Threat Models and Security Issues in Wireless Sensor Networks”, 2013, International Journal of Computer Theory and Engineering, Volume 5, Issue 5

[18] Tejaswi Singh, AatishGandotra, “Replication of Attacks in a Wireless Sensor Network using NS2”, 2015, International Journal of Research in Engineering and Technology, Volume: 04 Issue: 10

[19] Neelam J. Patel, “Detection & Prevention Techniques of Sinkhole Attack in Mobile Adhoc Network: A Survey”, 2016, International Journal of Latest Research in Engineering and Technology (IJLRET), Volume 2 Issue 4

[20] Waleed Al Shehri, “A Survey ON Security in Wireless Sensor”, 2017, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.1

[21] H. Xie, Z. Yan, Z. Yao and M. Atiquzzaman, "Data Collection for Security Measurement in Wireless Sensor Networks: A Survey," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2205-2224, April 2019

[22] M. A. Al-Naeem, "Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS," in IEEE Access, vol. 9, pp. 87070-87078, 2021

[23] S. Lata, S. Mehfuz and S. Urooj, "Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies," in IEEE Access, vol. 9, pp. 161103-161128, 2021

[24] Z. Teng, C. Du, M. Li, H. Zhang and W. Zhu, "A Wormhole Attack Detection Algorithm Integrated with the Node Trust Optimization Model in WSNs," in IEEE Sensors Journal, vol. 22, no. 7, pp. 7361-7370, 1 April1, 2022

[25] J. Lee, S. Yu, M. Kim, Y. Park and A. K. Das, "On the Design of Secure and Efficient Three-Factor Authentication Protocol Using Honey List for Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 107046-107062, 2020

[26] S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in IEEE Access, vol. 8, pp. 169548-169558, 2020

[27] L. Xiong, N. Xiong, C. Wang, X. Yu and M. Shuai, "An Efficient Lightweight Authentication Scheme with Adaptive Resilience of Asynchronization Attacks for Wireless Sensor Networks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 9, pp. 5626-5638, Sept. 2021,

[28] X. Huan, K. S. Kim and J. Zhang, "NISA: Node Identification and Spoofing Attack Detection Based on Clock Features and Radio Information for Wireless Sensor Networks," in IEEE Transactions on Communications, vol. 69, no. 7, pp. 4691-4703, July 2021

[29] M. Alotaibi, "Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN," in IEEE Access, vol. 9, pp. 159187-159197, 2021

[30] Panagiotis Sarigiannidis, Eirini Karapistoli and Anastasios A. Economides, “Analysing Indirect Sybil Attacks in Randomly Deployed Wireless Sensor Networks”, IEEE, 2016

[31] Yali Yuan, LiuweiHuo, Zhixiao Wang and Dieter Hogrefe, “Secure APIT Localization Scheme against Sybil Attacks in Distributed Wireless Sensor Networks”, JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015

[32] Noor Alsaedi1, 2, Fazirulhisyam Hashim, A. Sali, “Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks”, 2015 IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia (23 - 25 Nov 2015)

[33] Sepide Moradi, MeysamAlavi, “A distributed method based on mobile agent to detect Sybil attacks in wireless sensor networks”, 2016 Eighth International Conference on Information and Knowledge Technology (IKT)

[34] Salavat Marian, Popa Mircea, “Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator detection scheme”, 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics • May 21-23, 2015

[35] Ruixia Liu, Yinglong Wang, “A New Sybil Attack Detection for Wireless Body Sensor Network”, IEEE, 2014

[36] Imran Makhdoom, Mehreen Afzal, Imran Rashid, “A Novel Code Attestation Scheme Against Sybil Attack in Wireless Sensor Networks”, 2014 National Software Engineering Conference

[37] Bayrem TRIKI Slim Rekhist Noureddine Boudriga, “An RFID based System for the detection of Sybil attack in Military Wireless Sensor networks”, IEEE, 2014

[38] P. Raghu Vamsi and Krishna Kant, “A Lightweight Sybil Attack Detection Framework for Wireless Sensor Networks”, IEEE, 2014

[39] Bin TIAN, Yizhan YAO, Lei SHI, Shuai SHAO, Zhaohui LIU, Changxing XU, “A NOVEL SYBIL ATTACK DETECTION SCHEME FOR WIRELESS SENSOR NETWORK”, IEEE, 2013

[40] Xun Li, Guangjie Han, Aihua Qian, Lei Shu, Joel Rodrigues, “Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks”, 2013

[41] James Harbin, Dr Paul Mitchell, “Reputation Routing To Avoid Sybil Attacks In Wireless Sensor Networks Using Distributed Beamforming”, 2011 8th International Symposium on Wireless Communication Systems, Aachen

[42] BinZeng, Benyue Chen, “SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless Sensor Network”, 201O International Conference on Computer and Communication Technologies in Agriculture Engineering

[43] Shanshan Chen, Geng Yang, Shengshou Chen, “A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks”, 2010 International Conference on Communications and Mobile Computing

[44] Ren Xiu –li, Yang Wei, “Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network”, IEEE, 2009

[45] Annie Mathew and J.Sebastian Terence, “A Survey on Various Detection Techniques of Sinkhole Attacks in WSN”, International Conference on Communication and Signal Processing, April 6-8, 2017

[46] Mahmood Alzubaidi, Mohammed Anbar, Samer Al-Saleem, Shadi Al-Sarawi, Kamal Alieyan, “Review on Mechanisms for Detecting Sinkhole Attacks on RPLs”, 2017 8th International Conference on Information Technology (ICIT)

[47] MANPREET KAUR, AMARVIR SINGH, “Detection and Mitigation of Sinkhole Attack in wireless sensor network”, IEEE, 2016

[48] Gauri Kalnoor, Jayashree Agarkhed, “QoS based Multipath Routing for Intrusion Detection of Sinkhole Attack in Wireless Sensor Networks”, 2016 International Conference on Circuit, Power and Computing Technologies

[49] Jianpo Li, Dong Wang, Yanjiao Wang, “Security DV-hop localisation algorithm against wormhole attack in wireless sensor network”, IET Wirel. Sens. Syst., 2018, Vol. 8 Issue 2, pp. 68-75, the Institution of Engineering and Technology 2018

[50] RanuShukla, Rekha Jain, P. D. Vyavahare, “Combating against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network”,

Proceeding International conference on Recent Innovations is Signal Processing and Embedded Systems (RISE -2017) 27-29 October,2017

[51] Bharat Bhushan, Dr. G. Sahoo, “Detection and Defense Mechanisms against Wormhole Attacks in Wireless Sensor Networks”, IEEE, 2017

[52] Mayank Kumar Sharma, Brijendra Kumar Joshi, “A Mitigation Technique for High Transmission Power based Wormhole Attack in Wireless Sensor Networks”, ieee, 2016

[53] Ali Modirkhazeni, SaeedehAghamahmood, Arsalan Modirkhazeni, NaghmehNiknejad, “Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks”, IEEE, 2016

[54] Swati Bhagat, TrishnaPanse, “A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network”, IEEE, 2016

[55] Mostefa BENDJIMA, Mohammed Feham, “Wormhole Attack Detection in Wireless Sensor Networks”, SAI Computing Conference 2016 July 13-15, 2016

[56] ShaoheLv, Xiaodong Wang, Xin Zhao and Xingming Zhou, “Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks”, 2008 International Conference on Computational Intelligence and Security

[57] Jiangtao Wang, Geng Yang, Yuan Sun, Shengshou Chen, “Sybil Attack Detection Based on RSSI for Wireless Sensor Network”, IEEE, 2007

[58] Huda A. Babaeer, Saad A. Al-Ahmadi, “Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking”, 2020, IEEE Access

[59] Guangjie Han, Xun Li, Jinfang Jiang, Lei Shu, Jaime Lloret, “Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks”, 2015, The Computer Journal

[60] U Prathap, P Deepa Shenoy, K R Venugopal, “PCAD: Power control attack detection in wireless sensor networks”, 2016, IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)

[61] K. Karthigadevi, S. Balamurali, M. Venkatesulu, “Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to Detect and Prevent the Sinkhole Attack in Wireless Sensor Network”, 2019, IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)

[62] Prakash C Kala, Arun Prakash Agrawal, Rishi Rajan Sharma, “A Novel Approach for Isolation of Sinkhole Attack in Wireless Sensor Networks”, 2020, 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)

[63] S. Ranjeeth Kumar, A. Umamakeswari, “SSLEACH: Specification based secure LEACH protocol for Wireless Sensor Networks”, 2016, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)

[64] Ghazaleh Jahandoust, Fatemeh Ghassemi, “An adaptive sinkhole aware algorithm in wireless sensor networks”, 2017, Ad Hoc Networks

[65] Abdul Razaque, Syed S. Rizvi, “Secure data aggregation using access control and authentication for wireless sensor networks”, 2017, Computers & Security

[66] M. T. Kurniawan, Setiadi Yazid, “Mitigation strategy of sinkhole attack in Wireless Sensor Network”, 2017, International Workshop on Big Data and Information Security (IWBIS)

The Survey of Various Security Schemes of Wireless Sensor Networks

Abstract

A network that does not contain any central controller within it and is self-configuring in nature is known as a wireless sensor network. It is difficult to maintain the security and energy consumption of these networks due to such properties. When any kinds of malicious nodes enter the network, a scenario of attack occurs in that network. There are several types attacks found in the network which are all categorized into active and passive types depending upon the manner in which they attack. The various schemes are designed to improve security of wireless sensor networks. The designed techniques are reviewed in terms of methodology and performance.

Keywords

WSN, Security Attacks, Thrust mechanism, PLC, RTU

1. Introduction

A wireless sensor network (WSN) can be defined as a group of sensor nodes with finite resources that achieve a common purpose by working in coordination. Typically, the main functions of sensors include sensing and monitoring their area of deployment, collecting sensor information from the environment, processing data, and communicating with other devices [1]. Sensor nodes are deemed as one of the three main constituents that are included in the deployment framework in a WSN, which are: (1) sensor nodes, (2) radio co-ordinators, and (3) a programmable logic controller (PLC) or any human-computer interface (HCI) backing up a Remote Terminal Unit (RTU). Sensor nodes can have faults and due to their exposure on the web, they can become unreliable in no time and anyone gets physical access to them for free. A typical sensor consists of four basic units: a power source, a radio, a processor, and an actuator. At the other side, they have many limitations with respect to energy, data transmission, computation and storing. It is possible to deploy thousands of such nodes in some target locations to collect data for upcoming purposes, such as meteorological purposes, smart homes etc [2].

1.1 Cybersecurity Attacks in Wireless Sensor Networks

The classification of cyber security attacks can be done in two general modes, which are: (a) passive attacks and (b) active attacks. Cyber security is the practice of providing security to networks, devices, and data from illegal accessibility. It is basically an art to ensure the data confidentiality, integrity and accessibility.

i. Passive attacks: The attackers activate passive attacks only to overhear communications (hence eavesdropping) and analyse the traffic shared without modifying the vulnerable system [3]. This attack variant is extremely perilous and complex to locate as it is performed silently without affecting the system. Consequently, the assailant aims to collect some private information simultaneously, as well as gain knowledge about expressive nodes in the network (cluster head nodes) to get ready for an active attack, which can be devastating.
ii. Active attacks: In active attacks, the adversary tries to delete or replace messages exchanged over the network. The assailant can do anything damaging if he has the potential to execute his purpose.

1.2 Security of WSN in Healthcare Sector

Wireless healthcare networks have brought revolution in the way of patient monitoring in the healthcare domain by presenting a more efficient substitute of the conventional way of managing patient health. Since every technology has some shortcomings along with advantages, the free-access characteristic of the network brings its

confidentiality under question [4]. Illegal access actions and unrestricted threats can develop security issues for the healthcare data of the patient. The data gathered by the devices implanted on the patient's body for healthcare monitoring may lead to security concerns. The exposure of sensor nodes to the internet increases their vulnerability to different variants of attacks, for example, distributed denial-of-service (DDoS) attack. This attack type is deemed as one of the major concerns as adversary can collapse the security of the network and can further activate a clone node attack, or a replication attack which is amongst the most threatening assaults. When the sensor node transferring the patient's sensitive health data is attacked, the attacks not only swap the sensor nodes with duplicates of the sensor nodes but also displace the real data with bogus data and install the sensor node on the database again. Wireless healthcare systems are available to everyone across the world, and have ensured their reach to every part of the globe [5]. The free-access characteristic of the technology of the wireless healthcare network and its wireless channels increases the insecurity of the data transmitted over the network.

1.2.1 Node Replication or clone Node Attack

The dynamic operational nature of WSNs make them often unrecoverable, therefore they are prone to a variety of new attacks. For example, an adversary can listen to all network communications. In addition, a malicious node can capture all the information stored therein by the receiving nodes. Sensors are generally not considered forgery-proof [6]. Since a clone contains valid information (code and cryptographic material), it can join in network operations in the similar fashion as a normal node; therefore, cloned nodes are able to active a vast range of attacks. For example, a clone can generate a black hole, launch a wormhole attack with an allied opponent, or insert false data or aggregate data so as to manipulate the ultimate result. In addition, clones can perform information leakage. The following two important points may help illustrate the severity of a clone attack [7]:

- A clone can pretend to be completely truthful to its surrounding nodes. Truthful nodes indeed may not be aware of the truth without global counterexamples that there is a clone among their surroundings.
- In order to have a vast number of colluded nodes [8], it is not required for an adversary to compromise a large number of nodes. In fact, upon acquiring and contaminating one node, the main cost of the attack persists. It may be considered cheaper to make more clones of the similar node.

1.2.2 Diagrammatic Representation of replication attack in WSN

A node replication attack or clone node attack is a security concern where an adversary reprograms or regenerates WSN sensor nodes and connects to the target network by pretending to be valid nodes of that specific network. Considering cost, these sensors tend to lack tamper resistance hardware [9]. Figure 1 shows a node replication attack in a WSN.

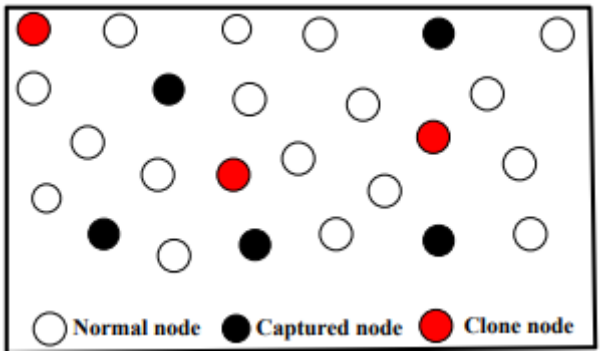


Fig. 1. A WSN with clone nodes

After the attacker has captured the honest node, all information is obtained from the honest node. The assailant then reinjects this acquired node into the network with no modifications. Typically, when an assailant activates a node replication attack, the duplicates are installed in the relevant and appropriate position in the WSN [10]. In a

static wireless network, the nodes are immobile, which means that their location remains unchanged after deployment. However, the situation differs from that of mobile wireless sensor networks where the nodes are dynamic in nature, without any static location. From this viewpoint, it is clear that the methods adopted for detecting node replication attacks in static WSNs may be different from those of mobile WSNs [11].

1.3 Replication or Node Clone Detection Techniques in WSN

Clone attack is amongst the most important security attacks in sensor networks. After a sensor node is compromised, a malevolent user can install fake sensor nodes in WSNs to activate a rage of deceptive attacks. Therefore, tracing clone nodes in less cost is essential to guarantee the network security. Several clone detection protocols exist in the literature [12]. Generally speaking, clone detection protocols can be categorized into two classes, known as, centralized and distributed protocols:

a. Centralized clone detection protocol: Sensor nodes use a centralized clone detection protocol to transmit their privacy information to the base station, and the node at the base station determines the authenticity of the sensor node by making comparison of the privacy information to its already saved records. This kind of scheme has less communication overhead and intricacy. In the centralized clone detection protocol [13], malevolent users can listen to the communication between the sink node and the sensor nodes, and obtain the privacy information of the sensor node, then it can masquerade as the sensor to collapse the protocol. In addition, sensor nodes closer to the sink suffer from a more traffic load in contrast to other sensor nodes and their energy is dissipated sooner, leading to a shorter network service period [14].

b. Distributed clone detection protocols: With a distributed clone detection protocol, each sensor node chooses onlookers for clone discovery, making it problematic for malevolent users to overhear the communication between the sink and the sensor nodes. There exist three types of witness selection approaches [15]: i) deterministic selection, ii) random selection, and iii) quasi-random selection which are elaborated as follows:

i. The clone detection protocols applying deterministic witness selection approach, such as the Randomized Efficient and Distributed Protocol (RED) allow all sensors to choose the same group of witnesses. The communication overhead can be reduced and a higher clone detection probability can be yielded by selecting similar deterministic group of witnesses [16]. Nevertheless, malevolent users have potential to contaminate some sensor nodes by overhearing communications between the source node and its witnesses in order to gain mapping functions and active spiteful assaults [17].
ii. To remove the shortcomings, clone detection protocols using random witness selection strategy have been proposed, such as the Line-Select Multicast Protocol (LSM). Each sensor's witnesses are randomly mapped to a node's identity, making it more challenging for malevolent users to get the witnesses' information, even if they overhear the communication between the sensor node and the sink node. At the other side [18], the randomness in the mapping function makes it challenging for the source node to efficaciously notice its witnesses, which reduces the chances of clone finding. Thus, clone detection probability is amongst the fundamental performance measures for security assessment in the clone detection protocols implementing random witness selection strategy.
iii. Clone detection protocols implementing semi-random witness selection strategy like single deterministic cell (SDC) [19] aim to create a balance between the random and deterministic witness selection schemes. In the semi-random scheme, the mapping function produces a deterministic region for every sensor device, and witnesses are chosen from this region on random basis. This scheme needs huge communication overhead and intricacy because the sensors have different sets of witnesses [20]. In addition, because of the restricted power of battery, network service period is a crucial performance parameter in wireless sensor networks [21].

2. Literature Review

2.1 Detection of Replication Attack using Optimization Techniques and Machine Learning

S. Anitha, et.al (2020) suggested an effectual application in which diverse techniques such as EMABRD (Exponential Moving Average based Replica Detection), SACOP (Secured Ant Colony Optimization) and FZKA (Fingerprint based Zero Knowledge Authentication) were presented on the real time environment [22]. The results of comparison revealed the superiority of the SACOP over others for offering higher probability to detect the malicious nodes with regard to maximum storage and communicating overheads. Moreover, the EMABRD performed more effectively with regard to overheads.

L. S. Sindhuja, et.al (2018) discussed that the HCMS (healthcare monitoring system) faced a major issue of security due to the vulnerability of this system towards diverse attacks and the node replication was a main attack that led to impact the reliable and confidential data [23]. An AIS (Artificial Immune System) based technique recognized as EHIP-HOP technique was introduced on HCMS for detecting the node replica attack in an environment having limited resources and at lower cost. The results demonstrated that the introduced technique was resisted against the attacks more robustly with regard to overhead, throughput, PDR (packet delivery ratio) and energy usage.

P. Sherubha, et.al (2019) developed a technique for detecting a number of replica attacks in WSN (Wireless Sensor Network) [24]. Moreover, this technique emphasized on formulating an adaptive RF-MOCS (Random Forest based Multi-Objective Cuckoo Search) algorithm for recognizing the source of clone attack. The developed technique was quantified on KDD cup dataset. The developed technique performed well concerning accuracy, sensitivity, specificity and F-measure. The results exhibited that the developed technique outperformed the traditional methods.

Table 1: Detection of Replication Attack using Optimization Techniques and Machine Learning

Author	Year	Technique Used	Findings	Limitations
S. Anitha, et.al	2020	EMABRD (Exponential Moving Average based Replica Detection), SACOP (Secured Ant Colony Optimization) and FZKA (Fingerprint based Zero Knowledge Authentication)	The results of comparison revealed the superiority of the SACOP for offering higher probability to detect the malicious nodes with regard to maximum storage and communicating overheads. Moreover, the EMABRD performed more effectively with regard to overheads.	The suggested application attained misdetection in case of arrival of events at random.
L. S. Sindhuja, et.al	2018	EHIP- HOP technique	The results demonstrated that the introduced technique was resisted against the attacks more robustly with regard to overhead, throughput, PDR (packet delivery ratio) and energy usage.	The issue related to the failure of single point was often occurred in such technique.
P. Sherubha, et.al	2019	RF-MOCS (Random Forest based Multi-	The developed technique performed well concerning	This technique provided poor performance on other

		Objective Cuckoo Search) algorithm	accuracy, sensitivity, specificity and F-measure. The results exhibited that the developed technique outperformed the traditional methods.	datasets while predicting the presence of clone attack in WSN (Wireless Sensor Network).

2.2 Detection of Replication Attack using Key Management Techniques

L. Li, et.al (2020) established a SRKD (secure random key distribution) technique which was focused on generating an innovative technique to defend against the replication attack [25]. In particular, a localized algorithm was integrated with a voting system for detecting and eliminating the malicious nodes. The replica attack was prevented by changing the meaning of metric. The results of experiments depicted that the established technique offered success rate of 90% above for detecting the replicate nodes in the availability of two hundred nodes in network. Moreover, the established technique was proved efficient and secure, and provided more enhanced storage and communicating efficacy as compared to the conventional techniques.

M. Buragohain, et.al (2018) constructed a new key management technique. The fundamental goal of this technique was to diminish the computing overhead, mitigate the communicating overhead, lessen the impact of node capture attack, and protect the node from known attacks such as clone attack and replay attack [26]. The identity-based cryptography was put forward in which the bilinear pairing was employed on ECs (elliptic curves). Strand Space model was exploited to illustrate that the constructed technique was secure. The simulation results indicated that the constructed technique performed well in comparison with other protocol concerning computing time.

M. Perez-Jiménez, et.al (2019) projected a novel technique to allocate the signature in WSN (Wireless Sensor Network) on the basis of magnetic PUF (Physical Unclonable Function) [27]. The Physical Unclonable Function utilized the physical properties for generating the private keys. It was not possible to access these keys and replicate them. This resulted in inserting the intrinsic complexity magnetic phenomena using which an unbreakable signature technique was described. The simulation was conducted for evaluating the projected technique. The results revealed that the projected technique provided higher entropy and had potential for producing a huge catalogue of diverse keys.

Table 2: Detection of Replication Attack using Key Management Techniques

Author	Year	Technique Used	Findings	Limitations
L. Li, et.al	2020	SRKD (secure random key distribution) technique	The results of experiments depicted that the established technique offered success rate of 90% above for detecting the replicate nodes in the availability of two hundred nodes in network. Moreover, the established technique provided more enhanced storage and communicating efficacy.	This technique had not offered surety for the connectivity of network and unable to prevent the attack in complex some scenario.

M. Buragohain, et.al	2018	A new key management technique	The constructed technique was inefficient to enhance the energy utilization and to optimize the energy efficacy.	The simulation results indicated that the constructed technique performed well in comparison with other protocol concerning computing time.
M. Perez-Jiménez, et.al	2019	Magnetic PUF (Physical Unclonable Function) based technique	The results revealed that the projected technique provided higher entropy and it had potential for producing a huge catalogue of diverse keys.	The projected technique was not able to produce complex keys.

2.3 Detection of Replication Attack using Watermarking Techniques

V. -T. Nguyen, et.al (2018) suggested a new watermarking technique with the objective of resisting against fake or clone node ID attacks and protecting the sensed data at the same time [28]. The suggested technique proved more secure and robust, and it was easy to integrate this technique with a practical routing algorithm on the basis of dynamic watermark. The suggested technique offered higher energy efficacy when this technique was integrated with LEACH (Low Energy Adaptive Clustering Hierarchy) protocol. The results obtained in analyzing the security validated that the suggested technique was efficient.

T. Hoang, et.al (2020) described that the node replication attacks led to generate a conflict of inside intrusions due to which the efficacy of the sensor networks was damaged at large extent [29]. Thus, a new lightweight mixed secure technique was investigated on the basis of watermarking method with the purpose of protecting sensory data and resisting against node clone attacks. The investigated technique was evaluated by conducting numerical and security analysis. The simulation results confirmed that the investigated technique provided consistency and resistance.

Mojtaba Jamshidi, et.al (2020) presented a three-stage methodology for detecting the replica nodes [30]. The watchdog nodes were considered in this methodology which was planned on the basis of concept that the similar opportunity was given to all nodes for meeting with the watchdog nodes. The network traffic was monitored and the channel was observed using the watchdog nodes. The J-SIM simulator was applied to conduct a series of simulations so that the efficacy of the presented methodology was computed with respect to the probability to detect the replication node and false detection probability. The simulation results depicted that the presented methodology was applicable for detecting the replicated nodes and mitigating the false detection probability 0.005% below.

Table 3: Detection of Replication Attack using Watermarking Techniques

Author	Year	Technique Used	Findings	Limitations
V. -T. Nguyen, et.al	2018	A new watermarking technique	The results obtained in analyzing the security validated that the suggested technique was efficient.	The suggested technique was not changed the duration of the WSN (wireless sensor network) as much after its integration with the watermark procedure.

T. Hoang, et.al	2020	A new lightweight mixed secure technique	The simulation results confirmed that the investigated technique provided consistency and resistance.	The response of WSN (Wireless Sensor Network) was the major limitation of this technique in an attack was detected.
Mojtaba Jamshidi, et.al	2020	A three-stage methodology	The simulation results depicted that the presented methodology was applicable for detecting the replicated nodes and mitigating the false detection probability 0.005% below.	The presented methodology had a slight delay to recognize the replicated nodes due to which the malicious nodes attained an opportunity for performing the operations in the network.

Conclusion

Wireless Sensor Network can be described as a self-organized and infrastructure less wireless network of sensor nodes. These sensor nodes perform the monitoring of physical or environmental conditions such as humidity, sound, vibration etc. The sensor nodes collectively forward their data via the network to a base station or sink. At base station, the observing and analysis of data can be done. A sink or base station acts as a link between users and the network. It is possible to extract necessary information from the network by inserting queries and collecting outcomes from the base station. The various schemes are analysed which increase security of the network. In future, novel scheme will be designed to increase security of wireless sensor networks.

References

[1] M. N. I. Khan and M. S. Islam, "A New Scheme to Detect and Prevent Node Replication Attacks for Wireless Sensor Networks," 2019 International Conference on Computer Communication and Informatics (ICCCI), 2019, pp. 1-5

[2] B. Shimpi and S. Shrivastava, "A modified algorithm and protocol for Replication attack and prevention for Wireless sensor Networks," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016, pp. 1-5

[3] Y. -S. Ho, R. -L. Ma, C. -E. Sung, I. -C. Tsai, L. -W. Kang and C. -M. Yu, "Deterministic detection of node replication attacks in sensor networks," 2015 IEEE International Conference on Consumer Electronics - Taiwan, 2015, pp. 468-469,

[4] H. Kaur and S. Saxena, "A review on node replication attack identification schemes in WSN," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1-8

[5] M. Qabulio, Y. A. Malkani and A. Keerio, "Securing mobile Wireless Sensor Networks (WSNs) against Clone Node Attack," 2015 Conference on Information Assurance and Cyber Security (CIACS), 2015, pp. 50-55

[6] M. Numan et al., "A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 65450-65461, 2020

[7] C. -M. Yu, C. -S. Lu and S. -Y. Kuo, "Compressed Sensing-Based Clone Identification in Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 3071-3084, April 2016

[8] T. P. Rani and C. Jayakumar, “Unique identity and localization based replica node detection in hierarchical wireless sensor networks”, Computers & Electrical Engineering, vol. 7, no. 4, pp. 239-244, Nov. 2017

[9] P. Abinaya and C. Geetha, "Dynamic detection of node replication attacks using X-RED in wireless sensor networks," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-4

[10] S. Roy and M. J. Nene, "Prevention of node replication in Wireless Sensor Network using Received Signal Strength Indicator, Link Quality Indicator and Packet Sequence Number," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 2016, pp. 1-8

[11] W. Z. Khan, M. S. Hossain and M. Atiquzzaman, “A cost analysis framework for claimer reporter witness based clone detection schemes in WSNs”, Journal of Network and Computer Applications, vol. 2, no. 9, pp. 261-267, March 2016

[12] P. P. Devi and B. Jaison, “Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms”, Computer Communications, vol. 1, no. 18, pp. 967-975, 1 Feb. 2020

[13] U. Iqbal and A. H. Mir, “Secure and practical access control mechanism for WSN with node privacy”, Journal of King Saud University - Computer and Information Sciences, vol. 15, no. 7, pp. 1013-1021, 26 May 2020

[14] K. Farah and L. Nabila, "The MCD Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," 2014 International Conference on Advanced Networking Distributed Systems and Applications, 2014, pp. 58-63

[15] L. Yang, C. Ding and M. Wu, "Location Similarity Based Replica Node Detection for Sensor Networks," 2016 9th International Symposium on Computational Intelligence and Design (ISCID), 2016, pp. 56-59

[16] L. Sujihelen and C. Senthilsingh, "Detect the replica node in Mobile Wireless Sensor Networks," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 265-267

[17] L. Sujihelen, M. Satyanarayana and C. Senthilsingh, "Replica Node Detection in Distributed Wireless Sensor Networks," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 704-707

[18] W. Z. Khan, M. Y. Aalsalem, N. M. Saad, Y. Xaing and T. H. Luan, "Detecting replicated nodes in Wireless Sensor Networks using random walks and network division," 2014 IEEE Wireless Communications and Networking Conference (WCNC), 2014, pp. 2623-2628

[19] G. Cheng, S. Guo, Y. Yang and F. Wang, "Replication attack detection with monitor nodes in clustered wireless sensor networks," 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), 2015, pp. 1-8

[20] M. M. Singh, A. Singh and J. K. Mandal, "Preventing node replication attack in static Wireless Sensor Netwroks," Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, 2014, pp. 1-5

[21] A. Rani and S. Kumar, "A low complexity security algorithm for wireless sensor networks," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1-5

[22] S. Anitha, P. Jayanthi, and V. Chandrasekaran, “An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks”, Measurement, vol. 5, no. 12, pp. 8022-8030, 2020

[23] L. S. Sindhuja, "Security of Healthcare Monitoring System using EHIP-HOP method," 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), 2018, pp. 199-204

[24] P. Sherubha, P. Amudhavalli and S. P. Sasirekha, "Clone Attack Detection using Random Forest and Multi Objective Cuckoo Search Classification," 2019 International Conference on Communication and Signal Processing (ICCSP), 2019, pp. 0450-0454

[25] L. Li et al., "A Secure Random Key Distribution Scheme Against Node Replication Attacks in Industrial Wireless Sensor Systems," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2091-2101, March 2020

[26] M. Buragohain and N. Sarma, "PKSN: A pairing based key management scheme for heterogeneous sensor network," 2018 10th International Conference on Communication Systems & Networks (COMSNETS), 2018, pp. 198-205

[27] M. Perez-Jiménez, B. Bordel, A. Migliorini and R. Alcarria, "An Automatic Key Generator based on Physical Functions for Resource Constrained Nodes in Future Wireless Sensor Networks," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-6

[28] V. -T. Nguyen, V. -H. Bui, T. -T. Nguyen and T. -M. Hoang, "A Novel Watermarking Scheme to against Fake Node Identification Attacks in WSNs," 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), 2018, pp. 1-5

[29] T. Hoang, V. Bui, N. Vu and D. Hoang, "A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks," 2020 International Conference on Information Networking (ICOIN), 2020, pp. 649-653

[30] M. Jamshidi, S. S. A. Poor and M. R. Meybodi, “A simple, lightweight, and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information”, Ad Hoc Networks, vol. 4, no. 23, pp. 415-427, 29 Jan. 2020

Approach for Isolation of Sinkhole Attack In Wireless Sensor Networks

Abstract: **Maintaining security and energy consumption of wireless sensor networks is a bit difficult due to non-availability of any central controller. They are also self-configuring in nature. Such types of networks are susceptible to several types of attacks. In this paper, we focus on one such attack called sink hole attack in which the malicious nodes spoof identification of base station and act like base station. The sensor nodes start transmitting data to malicious node instead of base station. This paper proposes a new technique to identify and eliminate such malicious nodes using identity verification to provide a secure environment for communication in the network. Proposed technique is implemented in NS2 and extensive simulations are performed to obtain the results. Results indicate the superiority of the proposed approach over existing approaches in terms of (packet loss, energy consumption, delay and throughput).**

Keywords: ***Wireless Sensor Networks, Sink Hole Attack, Spoofing, Malicious nodes, NS2.***

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of numerous sensing devices to gather the information about the surrounding environment of a specific region. The sensing devices which are otherwise known as nodes are very small in size and also incur least cost. Initially, these networks were only deployed within the military regions in which keeping a track on the activities of opponents was very important. Each of their movements was tracked and the important information was used by authorities to take appropriate actions [1]. There are several such applications in which it is very difficult to monitor the activities or mobility going on in such wide regions. Thus, the deployment of WSNs is very helpful in such applications. Today, there are large numbers of applications in which WSN's have been deployed. Mainly the applications of WSN are large and hostile due to which certain constraints also arise for them [2]. WSNs are deployed within regions that are not suitable as well as do not require any infrastructure. The deployment of around hundreds to thousands of sensor nodes is to accomplish the required task [3]. Since the WSNs are heterogeneous is nature, it is important to study the manner in which it is possible to deploy them in several regions. There are several types of operations performed by the sensor nodes deployed within WSNs. In order to gather the information from certain regions, it is important to ensure that the network is distributed all across it. For performing the overall analysis, it is important to monitor the areas in cooperative manner such that all the relevant data is collected [3].

WSN consists of two important components within it which are aggregation and base station. From the sensors present around the regions, the information is collected and forwarded to other nodes such that it can be passed on to authorities. The base station is known as the device towards which all the collected data is passed on. The base station is responsible to transfer the information further. WSNs are known to be very different from other networks since they have highly unique properties from others. The possibility of attacks to enter these networks is also high [4]. The vulnerability and susceptibility of these networks to other security attacks is very high since they include broadcasting communication. The entrance of attacks is higher in the networks since they are deployed in higher and dangerous regions. Several attacks can occur at various layers of the network since all these layers work in different manner and perform different functions. Several routing protocols are included here in which the security mechanisms are not provided. Therefore, it is very easy for the attackers to breach the security of networks. Collision attack occurs when the channel arbitration faces neighbor-to-neighbor communication within the link layer. There will be disruption of complete packet in case when collisions occur in any region of the deployed network. Therefore, there is a need to retransmit the packet since single bit error is caused. In the networks, packets are forwarded using multiple hops at high speeds due the creation of a low-latency link. This results in causing a wormhole attack in the network [5]. This attack is known to be a severe threat for any routing protocol available in the networks. It is very difficult to detect or prevent such attack. An attack uses a malicious node to create an influence on the network's traffic. Thus, numerous entities are created in the network which results in causing Sybil attack. An ID is generated in case when any fake additions are made or the duplicates of already available legitimate identities are created. DoS completely interrupt the efficiency of networks here. The physical disruption of network components is seen here when this attack occurs [6]. Further, this attack also results in destroying the wireless transmission. This attack generates noise, collision or interference at the receiver's end. The attacker has certain targets to be focused on amongst which few are the infrastructure of network, the server application as well as the network access. The victim node transmits the extra un-required data in DoS attack.

II. LITERATURE REVIEW

Li et al. proposed AWDV-hop that is a secure mechanism, using which the above mentioned issues can be minimized easily and also the effects of the wormhole attack [7]. They created the neighbor node relationship list (NNRL) by utilizing the broadcast flooding used by the first algorithm. The outcomes were achieved by simulating the proposed technique. Shukla et al. proposed to overcome this major issue by introducing an optimal solution called as TESRP [8]. Even though the attack is not prevented from occurring here, this is known as the best trust based protocol available. The sequence number is used with the trust algorithm to provide

secure scenario within the networks. Sharma et al. presented the wireless sensor network in the scenario that provides communication by linking nodes amongst themselves [10]. To make sure that the rink is minimized, comparative analysis was made amongst the techniques that were designed earlier and the new designed approach. Modirkhazeni et al. designed a new distributed network discovery mechanism which can be applied easily [11]. The outcomes achieved after conducting experiments clearly depict that the new designed approach is highly secure and keeps the attacks away from private data transmissions. Bhagat et al. presented the widespread application of this technology. A wormhole type of attack also results in degrading the overall performance of network due to which solutions are present by applying which it is easy to remove it [12]. A wormhole can be recognized using a powerful transmission as per their proposed approach.

III. RESEARCH METHODOLOGY

The different steps of proposed approach are explained below:

1. Network Deployments:- The WSN is the self configuring types of network in which sensors node sense the information and passes the information to base station. Such types of networks, various types of active attacks are possible in the network. Among all the type of attacks the sink hole attack is the attack which is difficult to detection and isolation from the network due to its unique properties.

2. Key Distribution of the Base station:- The novel approach is implemented in this research work for the detections of malicious node. In techniques of intrusion detection system, require extra software for the detection of malicious nodes which affect performance of technique for the detection of malicious nodes. The second technique which is popular for the detection of malicious nodes is the Delphi technique. This technique do not has any parameters of quality of service due to which we are not able to detect malicious nodes accurately. The technique which is proposed in this research work do not required any extra software and also includes the quality of service parameters for the detection of malicious nodes.

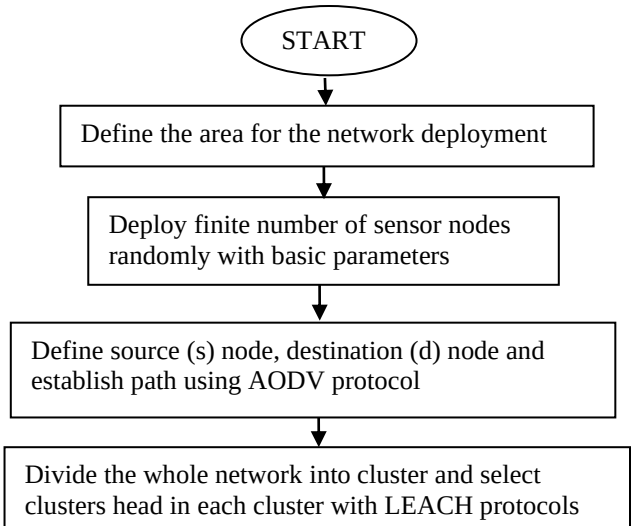
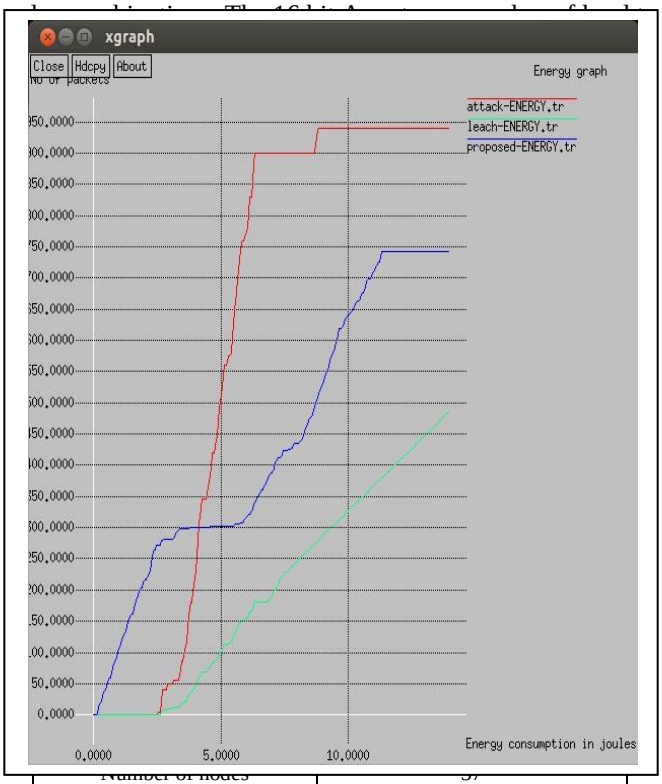


Fig. 1: Proposed Work Flow Methodology

In the proposed technique, as per figure 1, the sensor nodes are deployed in the finite area with the basic configuration. In the network, the source and destination nodes are defined randomly and also the path from source to destination is selected with AODV protocol. The AODV protocol is the reactive routing protocol; in which source node send the route request packets and nodes which are adjacent to destinations replies back with the routes replies packet. The paths from sources to destinations are selected on the basis of hop count and sequence number. In the communication, the malicious node spoof the identification of the base station and sensor nodes pass data to malicious node instead of base station. The

bases stations perform the task of node localization and key distribution. The base station distributes keys to all sensor nodes in the network and also defines the virtual keys. The sensor nodes when transmit the data to the base station, it will ask for the unique key of the base station. The base station calculates the key with Armstrong number.

3. Detection of Malicious node: - The original base station is able to provide its identification but the malicious node is not able to provide its identification. When the malicious node is not able to provide its identification, it is detected as the malicious node. The keys which are distributed in the network, to generate such keys the concept of Armstrong number is applied in this work. The Armstrong number is the unique number 16 bits which is generated from the various



Number of nodes	50
Antenna Type	Omni-directional
Link layer	LL
Queue Type	Priority Queue
Area	800 * 800 meters

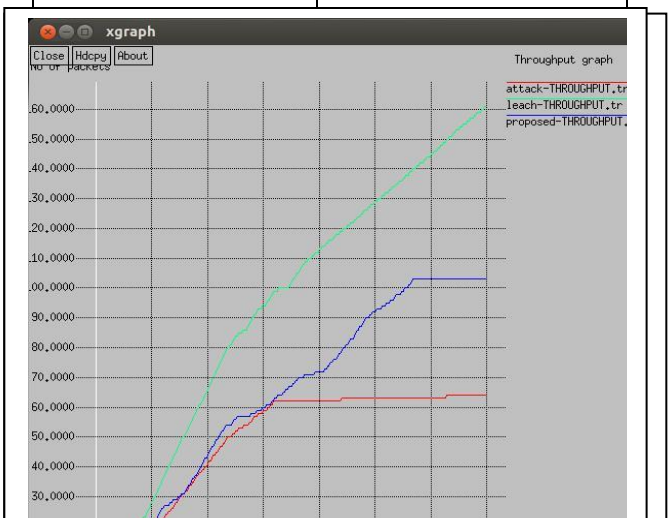


Fig.2: Packet Loss

In figure 2, the LEACH protocol shows the maxi effect and reduced packet loss in the network after the isolation of the sinkhole attack.

Fig. 3: Energy Comparison

Fig.3: Energy Consumption

Figure 3 shows that the energy consumption of the scneario that includes attack is the highest. The implementation of proposed protocol in the network reduces the amount of energy being consumed here.

Fig. 4: Throughput Comparisons

Figure 4 compares three scenarios which are the proposed, attack and existing genuine scenario and it has been analyzed that the network throughput is increased by steady rate after the isolation of the attack.

TABLE 2: Table of Comparison

Parameter	**Attack Scenario**	**LEACH Scenario**	**Proposed Scenario**
Packet loss	130 packets	60 packets	30 packets
Energy Consumption	950 Joules	750 Joules	400 Joules
Throughput	60 packets	110 packets	160 packets

V. CONCLUSION AND FUTURE SCOPE

In this work, it is concluded that the LEACH protocol is most effective technique used to reduce energy consumption of the wireless sensor networks. it is the network. The small sizes of sensor nodes are responsible for the reduced life time of these sensor nodes. The sinkhole attack is one of the active types of attack which reduces the LEACH protocol's performance. The technique of mutual authentication has been proposed in this thesis work, which detects and isolates the sinkhole attack. The outcomes achieved show that there is minimum packet loss and energy consumption rate achieved when the proposed approach is implemented. Thus, the proposed technique helps in reduction of energy consumption, increment in the throughput and reduces the delay time.

In future, a structure can be designed in for the reduction of power utilization of the network with the help of information collection. This future approach is based on the proposed LEACH protocol which is a multi-hierarchal protocol.

REFERENCES

[1] Xun Li, Guangjie Han, Aihua Qian, Lei Shu, Joel Rodrigues, "Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks", In *21st International Conference on Software, Telecommunications and Computer Networks-(SoftCOM 2013),* pp. 1-5. IEEE, 2013.

[2] James Harbin, Dr Paul Mitchell, "Reputation Routing To Avoid Sybil Attacks In Wireless Sensor Networks Using Distributed Beamforming", In *8th International Symposium on Wireless Communication Systems, Aachen*, pp. 276-280, 2011.

[3] BinZeng, Benyue Chen, "SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless Sensor Network", In *International Conference on Computer and Communication Technologies in Agriculture Engineering*, pp. 357-360, 2010.

[4] Shanshan Chen, Geng Yang, Shengshou Chen, "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks", In *International Conference on Communications and Mobile Computing*, pp. 142-146, 2010.

[5] Ren Xiu –li, Yang Wei, "Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network", In *5th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-5, 2009.

[6] Annie Mathew and J.Sebstian Terence, "A Survey on Various Detection Techniques of Sinkhole Attacks in WSN", In *International Conference on Communication and Signal Processing*, pp. 1115-1119, 2017.

[7] Jianpo Li, Dong Wang, Yanjiao Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network", *Institution of Engineering and Technology (IET) Wireless Sensor System*, Vol. 8 Issue 2, pp. 68-75, 2018.

[8] RanuShukla, Rekha Jain, P. D. Vyavahare, "Combating against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network", In *Proceeding International conference on Recent Innovations is Signal Processing and Embedded Systems*, pp. 555-561, 2017.

[9] Bharat Bhushan, Dr. G. Sahoo, "Detection and Defense Mechanisms against Wormhole Attacks in Wireless Sensor Networks", In *3rd International Conference on Advances in Computing, Communication & Automation (ICACCA*), pp. 1-5, 2017.

[10] Mayank Kumar Sharma, Brijendra Kumar Joshi, "A Mitigation Technique for High Transmission Power based Wormhole Attack in Wireless Sensor Networks", In *International Conference on ICT in Business Industry & Government (ICTBIG),* pp. 1-6, 2016.

[11] Ali Modirkhazeni, Saeedeh Aghamahmood, Arsalan Modirkhazeni, Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", In *7th International Conference on Networked Computing*, pp. 1-7, 2016.

[12] Swati Bhagat, Trishna Panse, "A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network", In *International Conference on ICT in Business Industry & Government (ICTBIG),* pp. 1-6, 2016.

Ajaz_FinalReport

by Turnitin Report

Submission date: 22-July-2022 12:20PM (UTC+0530)

Submission ID: 4647535617

File name: Ajaz_FinalReport.docx (1.4MB)

Word count: 16,847

Report_Ajaz

ORIGINALITY REPORT

9%	3%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Guru Nanak Dev Engineering College Student Paper	1%
2	Submitted to Thapar University, Patiala Student Paper	1%
3	Kamini Joshi, Sandeep Singh Kang. "Improved LEACH protocol using cache nodes for wireless sensor network", International Journal of Engineering & Technology, 2018 Publication	1%
4	airccse.org Internet Source	1%
5	Submitted to University of Bedfordshire Student Paper	1%
6	"Advanced Informatics for Computing Research", Springer Nature, 2019 Publication	1%
7	Saman Siavoshi, Yousef S. Kavian, Mehdi Tarhani, Hamid Sharif. "An energy-balanced	<1%