DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

A PROJECT REPORT

Submitted by

MD FAHEEM M N	- 113022106059
ZUHAIL AKTHAR S	- 113022106060
CHANDRU P	- 113022106016

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING
IN
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA
ENGINEERING COLLEGE
AVADI, CHENNAI-600062

ANNA UNIVERSITY: CHENNAI 600 025
JUNE 2024

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report **" DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK "** is the bonafide work of **FAHEEM M N**(113022106059),**MOHAMED ZUHAIL S**(113022106060), **CHANDRU P**(113022106016) who carried out the project work under my supervision.

SIGNATURE

Dr. S. HEMAJOTHI Ph.D.,

HEAD OF THE DEPARTMENT

Professor

Department of ECE
VEL TECH HIGH TECH
DR.RANGARAJAN DR. SAKUNTHALA
ENGINEERING COLLEGE
CHENNAI-600062

SIGNATURE

Dr.K.STELLA Ph.D.,

SUPERVISOR

Assistant Professor

Department of ECE
VEL TECH HIGH TECH
DR.RANGARAJAN DR. SAKUNTHALA
ENGINEERING COLLEGE
CHENNAI-600062

Submitted for the viva-voce held oN at VELTECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE

.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We wish to express our sincere thanks to the people who extended their help during the course of our project work.

We are greatly and profoundly thankful to our honorable Chairman **Col. Prof. Dr. Vel. R.Rangarajan, B.E., (Mechanical), B.E., (Electrical), M.S., (Automobile),D.Sc.,** and our Vice Chairman **Dr. Sakunthala Rangarajan, MBBS.,** Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering college, for facilitating us with this opportunity.

We are greatly thankful to our Chairperson and Managing Trustee **Mrs. Mahalakshmi Kishore Kumar B.E.,** and to our Vice President **Mr. K.V.D. Kishore Kumar, B.E, M.B.A(U.S.A).,** Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering college.
We also record our sincere thanks to our honorable Principal
Dr. E. Kamalanaban Ph.D We also greatly thankful to our dean Academics & Dean-SoCE **Dr. V.R Ravi Ph.D.,** for their valuable suggestions.

We also record our sincere thanks to our honorable Head of the Department,
Dr.S. Hemajothi Ph.D., Professor, for her constant support and encouragement.

We would like to extend our sincere thanks to our supervisor **Dr K.Stella Ph.D., Assistant Professor** Department of Electronics and communication, Vel Tech HighTech Dr. Rangarajan Dr. Sakunthala Engineering college for their constant technical support, valuable suggestions which enabled us to complete our project successfully.

Further the acknowledgement would be incomplete if we would not mention a word of thanks to our most beloved **PARENTS** whose continuous support and encouragement all the way through the course has led us to pursue the degree and confidently complete the project.

ABSTRACT

In this paper , we study the detection and prevention of black hole attack in wireless sensors network . Wireless sensor network is a Device which has a combination of device called sensor nodes and gate ways , software. These WSN nodes are capacity to transmit the data to other nodes . It plays an important role in the many applications like Military, health-care monitoring , traffic monitoring, industrial monitoring, agriculture monitoring etc...WSN (wireless sensor network) is quite vulnerable to many security concession attacks as worm hole , message replay or tampering , identity spoofing and black hole attack. Black hole attack is attack when the hacker attack the node to become the malicious node to give the false information to the receiver. The WSN sensor node has two types generic nodes and gateway nodes.These WSN nodes has only limited Transmission range and limited processing speed, with low battery and storage Capacity in IoET (internet of Everything). Today so many network are use in many areas like industrial, health care and commercial. When black is detected the intermediary capture and re program set of nodes to block the packets and create false messages instead of forwarding a true information towards the station.Here our paper are focus to detect and prevent a black hole attack inWireless sensor network. Also elaborate security against the black Hole attack. Also proposed the trust based mechanism for detect the Black hole attack . simulation result are used in NS-2 simulator by evaluated in term of packets . By preventing wireless network fromMalicious nodes by analiyse through an NS-2 simulator and step to reduces the effect of attack from the network. black hole attack in wireless sensor networks occurs when a malicious node falsely claims to have the optimal path to a destination, attracting all data traffic and dropping it, effectively creating a "black hole" where data disappears.When the source selects the path including the attacker node, the traffic starts passing through the adversary node and this node starts dropping the packets selectively or in whole. Black hole region is the entry point to a large number of harmful attacks.The wireless sensor network architecture is built with nodes that are used to observe the surroundings like temperature, humidity, pressure, position, vibration, sound, etc. These nodes can be used in various real-time applications to perform various tasks like smart detecting, a discovery of neighbor nodes, data processing and storage, data collection, target tracking, monitor and controlling, synchronization, node localization, and effective routing between the base station and nodes.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURE NO. TITLE PAGENO.

LIST OF SYMBOLS AND ABBREVIATIONS

WSN	-	Wireless Sensor Network
RIPEMD	-	RACE Integrity Primitives Evaluation Message Digest
MAC	-	Message Authentication Code
PDR	-	Packet Delivery Ratio
AODV	-	Ad-hoc On-demand Distance Vector
DSR	-	Dynamic Source routing
DARPA	-	Defense Advanced Research Projects Agency
VINT	-	Virtual Inter Network Testbed
AOMDV	-	Ad hoc On demand Multipath Distance Vector
NS-2	-	Network Simulator Version 2
OTC L	-	Object-oriented Tool Command Language
NAM	-	Network AniMator
RREP	-	Route Reply

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Wireless Sensor Network (WSN)
infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions. Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data.

Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components. These components are integrated on a single or multiple boards, and packaged in a few cubic inches.In many applications, wireless sensor networks often operate in hostile and unattended environments. Therefore, there is strong need for protecting sensing data and sensing reading from various attacks like sinkhole attack, blackhole attack, etc. The proposed approach provides a solution to meet sinkhole attack. The algorithm's main aim is to detect sinkhole attack and provide security against it in wireless sensor networks and improve the network's reliability.

1.2 ARCHITECTURE OF WSN

The architecture of a wireless sensor network (WSN) consists of a base station, clusters, and sensor nodes. The base station can communicate with computers at other locations, such as an end- user terminal connected through the internet.Currently, WSN is the most standard services employed in commercial and industrial applications, because of its technical development in a processor, communication, and low-power usage of embedded computing devices.

The wireless sensor network architecture is built with nodes that are used to observe the surroundings like temperature, humidity, pressure, position, vibration, sound, etc. These nodes can be used in various real-time applications to perform various tasks like smart detecting, a discovery of neighbor nodes, data processing and storage, data collection, target tracking, monitor and controlling, synchronization, node localization, and effective routing between the base station and nodes.

1.2.1 **BASE STATION**:~

A base station contains the antennas and other equipment needed to connect wireless communications devices to the network. It also acts as a gateway to other networks through the internet

1.2.2 **CLUSTERED NETWORK ARCHITECTURE**:~

Clustered network architecture is a two-tier hierarchy clustering architecture. It uses a distributed algorithm to organize sensor nodes into groups called clusters.

1.2.3 **SENSOR NODES**:~

Sensor nodes in a wireless sensor network (WSN) measure environmental parameters and transmit the data to a network gateway. The gateway then aggregates, stores, and processes the data.

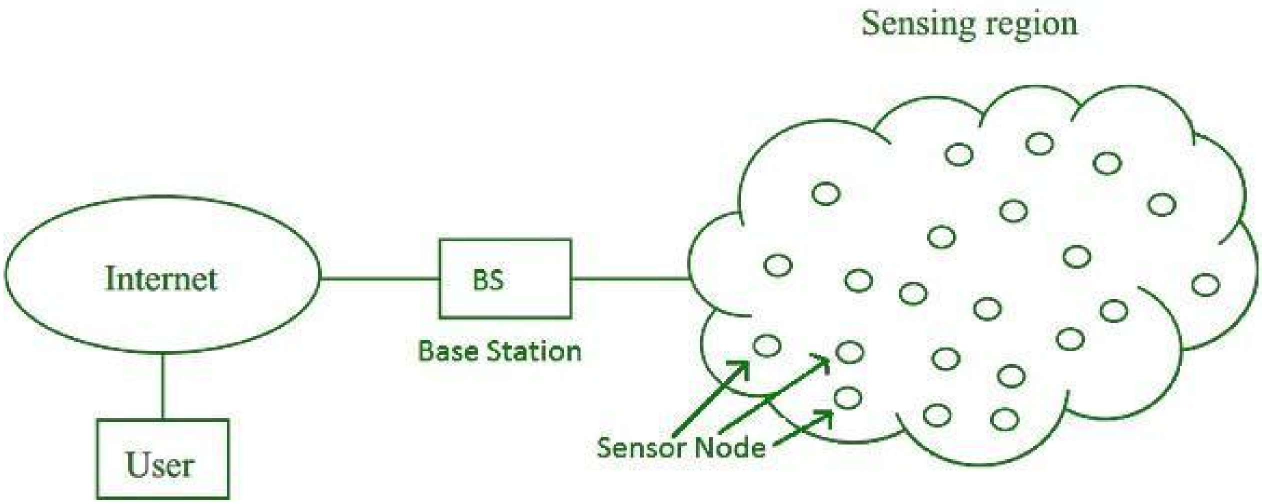


FIGURE 1.1

1.3 CHARACTERISTICS OF WSN

A wireless sensor network (WSN) is a platform that connects many distributed sensors. WSNs have several characteristics, including:

- Power consumption: WSNs have limitations on how much power sensor nodes can consume.
- Node failures: WSNs can handle node failures.
- Node mobility: WSNs have mobile nodes.
- Node heterogeneity: WSNs have heterogeneous and homogeneous nodes.
- Large-scale deployment: WSNs can be deployed on a large scale.
- Environmental conditions: WSNs can survive harsh environmental conditions.
- Ease of use: WSNs are easy to use.
- Power efficiency: WSNs are power efficient.
- Scalability: WSNs are flexible and scalable, allowing for easy deployment and reconfiguration of sensor nodes.
- Responsiveness: WSNs are responsive.
- Reliability: WSNs are reliable.
- Localization: WSNs use localization to identify the location of sensor nodes.
- Quality of service: WSNs provide high accuracy in data delivered to central control.
- Security: WSNs have limited security, as nodes can be intercepted, jammed, and seized.
- ROBUST OPERATIONS - Since the sensor nodes are deployed in hostile environments, they have certain capability of fault and error tolerance. Therefore, it is necessary to develop ability of sensor nodes in terms of self-test, self-calibrate and self-repair.

One of the major concerns of wireless sensor network is security. There are quite prone to unauthorized access, attacks, and unintentional damage of the information inside of the sensor node. The next section mainly focuses on sinkhole attack.

1.4 WSN SECURITY THREATS :~

There are various threats in wireless sensor networks as it includes packages which that contains important and secured files. The informations are not only to be stolen but can also be manipulating the information of the particular file.

There are several acctacks which includes:~

- DENIAL OF SERVICE
- SELECTIVE FORWARDING
- MANIPULATING ROUTING INFORMATION
- SINKHOLE ATTACKS
- WORMHOLE ATTACKS
- BLACKHOLE ATTACKS

1.4 .1 DENIAL OF SERVICE ATTACK:~

A denial-of-service (DoS) attack is a cyberattack on devices, information systems, or other network resources that prevents legitimate users from accessing expected services and resources. This is usually accomplished by flooding the targeted host or network with traffic until the target can't respond or crashes.

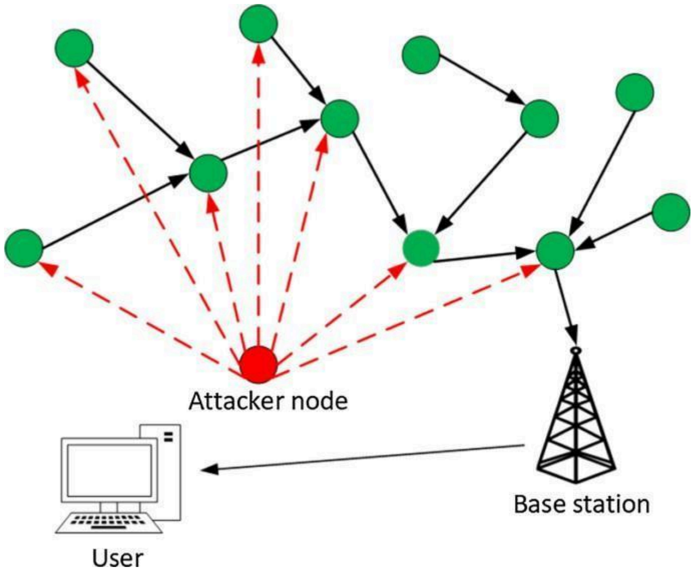


FIGURE 1.4

1.4.2 SELECTIVE FORWARDING ATTACK

The malicious nodes are created by the attacker and forwards only selected messages as shown in Figure.1.4. It is also called as black hole attackwhich drops all packets it receives. The defence against these attacks is by using multiple paths to forward the data.

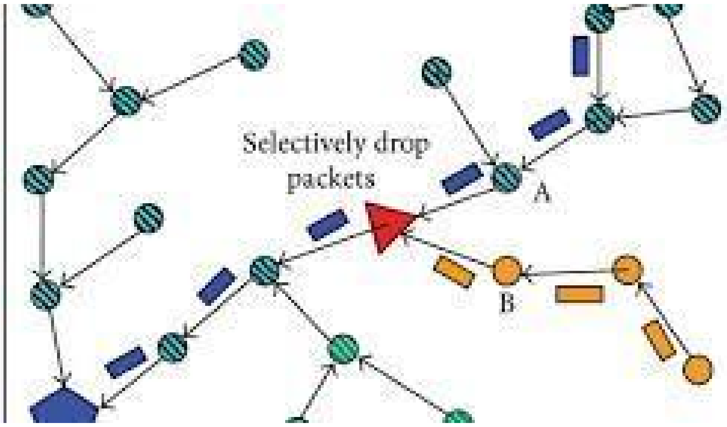


Figure 1.4.2 Selective forwarding attack

1.4.3 MANIPULATING ROUTING INFORMATION:~

This attack targets the routing information between two sensor nodes. It can be launched through spoofing or replaying the routing information. This can be done by adversaries who have the capability of creating routing loops, attracting or repelling network traffic, and extending or shortening source routes.

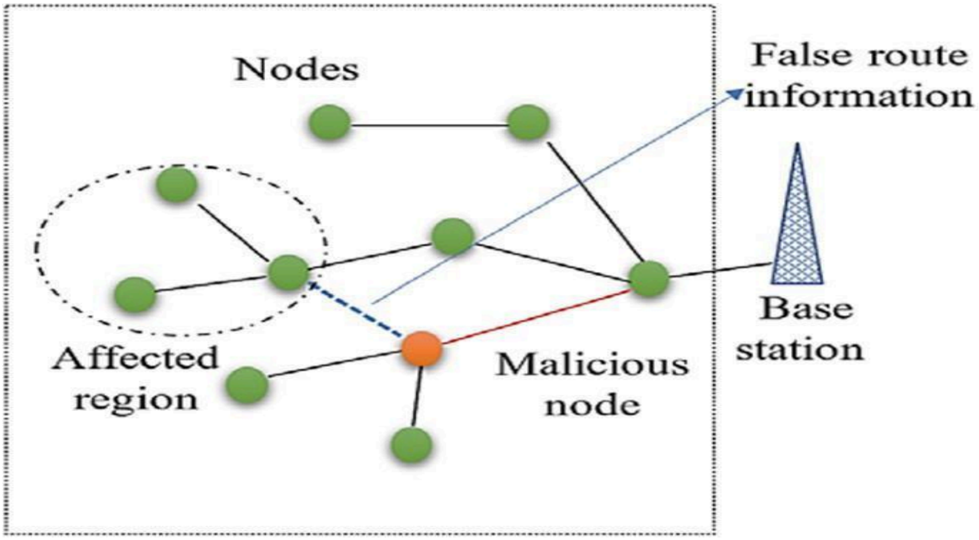


FIGURE 1.4.3

1.4.4 SINK HOLE ATTACKS:~

Sinkhole attacks are carried out by either hacking a node in the network or introducing a fabricated node in the network.The malicious node promotes itself as the shortest path to the base station and tries to guide the traffic from other nodes towards itself

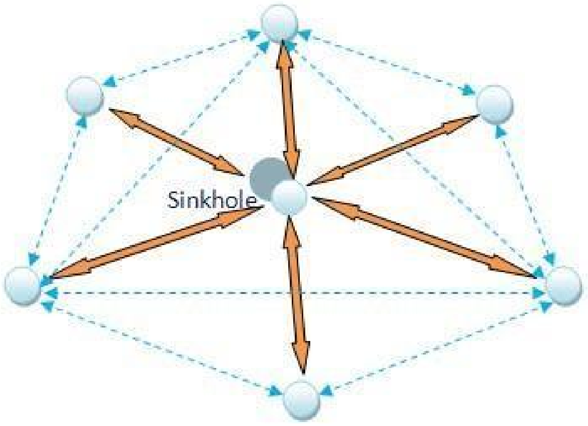


FIGURE 1.4.4

1.4.5 WARM HOLE ATTACKS:~

A wormhole attack is a popular and severe attack that involves two or more malicious nodes. The attack involves tunneling a data packet from one malicious node to another, and then broadcasting the data packets

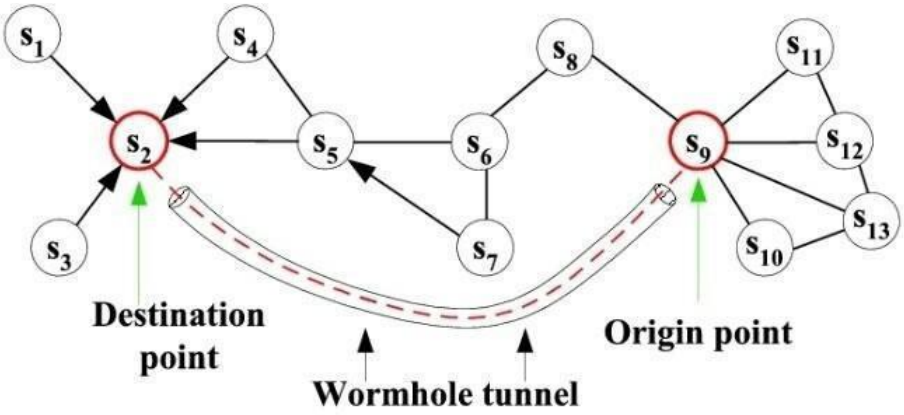


FIGURE 1.4.

1.4.6 BLACK HOLE ATTACK:~

A black hole attack in wireless sensor networks occurs when a malicious node falsely claims to have the optimal path to a destination, attracting all data traffic and dropping it, effectively creating a "black hole" where data disappears.
When the source selects the path including the attacker node, the traffic starts passing through the adversary node and this node starts dropping the packets selectively or in whole. Black hole region is the entry point to a large number of harmful attacks.

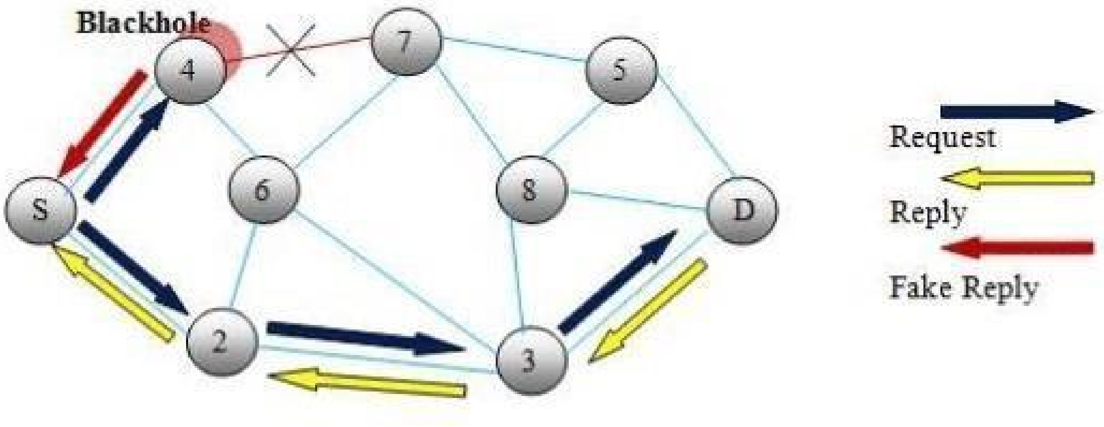
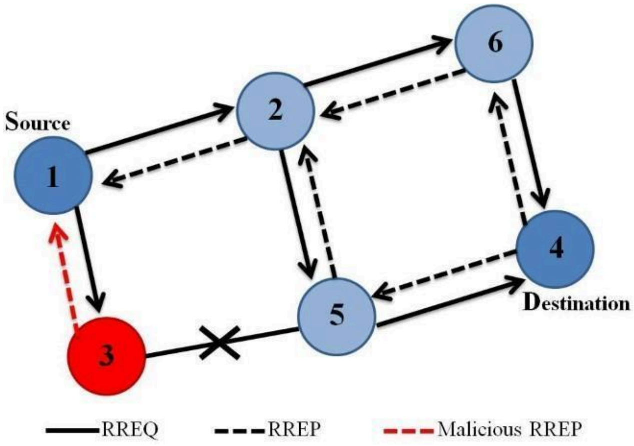


FIGURE 1.4.6

In this above figure node “s” reprecents the host and node “D” represents the destination.As we can see clrealy that the source node is passing a request to the neighbouring node(2) it gives the message as a reply, when the source node passes the request to its another respective node(4) which is a malicious one it passes a fake reply as a result, which ends up giving false information to the destination.
FIGURE 1.4.5



CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

Ruslan Dautov[2019],Gill R Tsour[2019] has proposed,A wireless body area network (WBAN) involves small sensors placed in or around the human body for various applications, including fitness monitoring and medical diagnosis. These sensors face hardware limitations like limited memory and power. The importance of medical WBANs is reflected in the dedicated U.S. FCC bandwidth and IEEE 802.15.6 standard.

Dawei Liu[2017],Yuedong Xu[2017]and xing huang[2017]
The author discusses the increasing importance of wireless localization, driven by the widespread use of wireless networks and smart sensors. However, security concerns, such as terrorist fraud and location spoofing, have emerged, particularly disrupting systems reliant on accurate localization like smart grids and traffic control. The paragraph introduces various localization methods, emphasizing distance-based approaches widely used in industrial wireless sensor networks (WSN). It highlights challenges, such as errors caused by non-line-of-sight (NLOS) conditions and location spoofing. The author raises a critical question: how can we detect location spoofing in situations where obstacles obstruct direct radio paths (NLOS conditions)? This question, despite its significance, hasn't been adequately addressed.

Lei shi[2020],qingchen liu[2020],jinliang shao[2020]and yuhua cheng[2020] has proposed Localizing sensor nodes in wireless sensor networks is a significant challenge. While centralized methods work well for some networks, like in agriculture or traffic monitoring, they're impractical for large networks due to complexity and reliability issues. In 2009, Khan et al. introduced DILOC, a distributed iterative localization algorithm based on barycentric coordinates. It uses anchors with known locations and relative distance measurements to find sensor locations. Despite its success, security concerns, especially denial-of-service (DoS) attacks, raised issues.

2.2 RELATED WORKS

OHIDA RUFAI AHUTU[2020] AND HOSAM EL-OCLA[2020] the author discusses A wireless sensor network consists of small, low-power sensor nodes deployed to monitor physical or environmental conditions, often relying on batteries for energy. While these networks are versatile, their lack of infrastructure makes them vulnerable to security threats, such as the Wormhole Attack, where an attacker creates a tunnel between distant locations to manipulate communications without disrupting the network structure.

To address this, the article proposes the MAC Centralized Routing Protocol (MCRP) for 802.15.4 wireless sensor networks. MCRP takes a centralized approach, using a high-energy Base Station (BS) to calculate routes, monitor the network, and perform energy-intensive tasks only when necessary. The protocol efficiently detects Wormhole Attacks through consensus by analyzing time delays between sensor nodes and the BS, helping identify potential threats and improve overall network scalability in terms of energy consumption, delay, throughput, and frame delivery ratio compared to other protocols.

PATEL BHOOMIKA[2016] AND PATEL ASHISH[2016] has described A Wireless Sensor Network (WSN) is a bunch of closely placed sensor nodes that keep an eye on different things. Thanks to advancements in technology, these nodes are now smaller, cheaper, and use less power. Each sensor node has its own resources like energy, wireless communication, and Micro Electro Mechanical Systems (MEMS). WSNs are used in various areas like military activities, environmental monitoring, healthcare, industrial processes, and urban surveillance.

After deployment, these sensor nodes automatically create a wireless communication network. There are two main types of nodes: generic sensors, which have limited resources but can detect various things, and gateway nodes, which have higher capabilities to send information from generic nodes to a server or end-user. They act like wireless access points or bridges.

OPEYEMIJOSANAIYE,ATTAHIRUS.ALFA,GERHARD P.HANCKE[2018] has described In the network layer, some sensors may get compromised and mess with the routes, controlling how information flows. This poses a threat to the network's integrity. The paper is organized into sections discussing attacks, related work, the proposed system, simulation results, and conclusions.

SARITA AGARWAL , MANIK LAL DAS , JAVIER LOPEZ[2018] these author says In practical applications like battlefield surveillance and forest fire detection using wireless sensor networks (WSNs), nodes are densely and randomly
deployed in hazardous conditions to monitor events collaboratively.
However, the wireless communication and unattended deployment make the network susceptible to node capture attacks, where a sensor node is physically obtained, reprogrammed, and redeployed for malicious purposes. Detecting such attacks remains challenging due to potential false reports from non-captured malicious nodes and the limitations of existing detection protocols. The challenge lies in developing effective protocols for detecting and preventing node capture attacks in WSNs, considering the resource constraints of sensor nodes and the risk of malicious collaboration among network nodes.

SHOUKAT ALI , DR MUAZZAM A KHAN , JAWAD AHMAD [2018] The author discusses Black Hole (BH) attacks in wireless sensor networks (WSNs), where malicious nodes advertise false paths to attract traffic but drop the packets instead of forwarding them, causing a denial-of-service (DoS) effect. These attacks significantly degrade network performance, impacting throughput, end-to-end delay, and energy consumption of nodes. The limited resources in WSNs make them vulnerable to such security threats. The paper explores the challenges posed by BH attacks, emphasizing their classification into single and collaborative attacks, which are harder to detect and more detrimental to network performance. The author also outlines the process of a BH attack, where a malicious node absorbs packets instead of forwarding, leading to adverse consequences for the network. The paper concludes by highlighting the need for new solutions to effectively address and mitigate BH attacks in WSNs.

DHARA BUCH[2014] The author discusses differentiating attacks based on the efficiency of the attacker's device, categorizing them into Mote class with limited power and laptop class with greater power. Another classification is insider and outsider attacks, where insiders are authorized participants turned malicious, posing a more challenging threat. The focus then shifts to Denial of Service (DoS) attacks, aiming to make a system or resource unavailable to legitimate users. Various types of DoS attacks are outlined, causing network slowdown, unavailability of websites, increased spam emails, and packet loss or delay. The classification of DoS attacks includes physical layer attacks like jamming, where excessive packets disrupt communication paths, particularly affecting sensor nodes with limited resources. The paper concludes by emphasizing the significance of understanding and defending against these attacks at different network layers.

MANDEEP KUMAR AND JAHID ALI[2021] This research focuses on enhancing energy-aware routing and detecting black hole attacks in Wireless Sensor Networks (WSN) using a deep-stacked autoencoder. The proposed approach involves energy-aware routing based on parameters like energy, distance, and delay, followed by black hole attack detection at the WSN base station using a pre-processed data-driven method with a Deep stacked autoencoder trained by the TaylorSFO algorithm. The study compares and contrasts with classical attack detection techniques, highlighting their strengths and limitations in preventing black hole attacks in WSN.

MISS. PRACHI S. MOON MR. PIYUSH K. INGOLE[2015] This research addresses security concerns in Wireless Sensor Networks (WSN), focusing on detecting Gray Hole attacks and implementing an Enhanced Adaptive Acknowledgment (EAACK) scheme. Gray Hole attacks occur when nodes falsely claim to forward data but disrupt communication, impacting the Ad-hoc On-demand Distance Vector (AODV) routing protocol. The EAACK scheme combines energy-aware routing and attack detection, employing an acknowledgment mechanism to identify malicious nodes. Additionally, the study introduces a hybrid mechanism involving Cellular Automata-based Security Algorithm (CAWS) for key management and secure communication. The hybrid approach enhances security by integrating two-phase algorithms to manage keys and ensure secure data transmission.

The paper emphasizes the importance of security in WSN due to unique sensor node characteristics. The hybrid mechanism incorporates Cellular Automata for key distribution and communication security, along with Modern Encryption Standard (MES-1) techniques for cryptographic protection. MES-1, featuring Double Jumping Symmetric Algorithm (DJSA) and Tree Top Jumping Symmetric Algorithm (TTJSA), provides robust encryption for data integrity. By combining these cryptographic methods and key management strategies, the proposed hybrid mechanism aims to fortify WSN against various security threats, ensuring secure and reliable data transmission from source to destination.

MADHU SHARMA[2016] delves into the critical role of routing protocols within Wireless Sensor Networks (WSN) and their importance in establishing communication routes between nodes. Specifically, the Ad-hoc On-demand Distance Vector (AODV) protocol is highlighted for its ability to dynamically discover and maintain routes as needed, thereby reducing bandwidth requirements. Despite these advancements, the paper underscores persistent security challenges in WSN, with a particular focus on the Wormhole attack. This malicious tactic involves creating a covert channel between nodes to selectively replay data packets, potentially leading to disruptions in communication and compromising the overall integrity of the network. The broader context extends the security concerns to Mobile Ad-hoc Networks (MANET), emphasizing the need for dynamic confidentiality approaches and addressing vulnerabilities in routing processes susceptible to various attacks.

SHARMA ASHISH JAIN , SHWETA SHAH[2016] part of the paper emphasizes the broader security landscape in MANET, shedding light on energy utilization and resource consumption as major challenges. Traditional security mechanisms are deemed impractical for the resource constraints of sensor nodes in WSN. The discussion centers on confidentiality and routing security, identifying insecure routing as a vulnerability that results in increased routing time, unnecessary energy consumption, and restricted access conditions during communication. The paper acknowledges the susceptibility of WSNs to a spectrum of attacks, including those targeting secrecy, authentication, denial-of-service, and service integrity. The Node Replication attack is specifically highlighted, illustrating the severe consequences of attackers capturing and replicating nodes to compromise network functionality. Lastly, the presence of various types of holes, such as coverage holes, routing holes, jamming holes, sink/black holes, and wormholes, contributes to the complexity of security challenges in wireless mobile networks.

CHAPTER 3

NETWORK SIMULATION(NS2) SOFTWARE

3.1 INTRODUCTION

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator 1, the foundation which NS is based on. Since 1995 the Defense Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual Inter Network Testbed (VINT) project.Currently the National Science Foundation (NSF) has joined the ride in development.

Last but not the least, the group of Researchers and developers in the community are constantly working to keep NS2 strong and versatile. In addition, it also provides substantial support for different protocols over wired and wireless networks. It provides high modular platform for wired and wireless simulations supporting different network elements,protocols, traffic and routing types. In general, WSNs use NS2 as a base for security evaluation and provides complete description of simulation and software program needed for implementing the network.

3.2 FEATURES OF NS2

1.It is a discrete event simulator for networking research.

2.It provides substantial support to simulate bunch of protocols like TCP,FTP, UDP, https and DSR.

3.It simulates wired and wireless network.

4.It is primarily UNIX based.

5.Uses TCL as its scripting language.
6.Otcl: Object oriented support.
7.Tclcl: C++ and otcl linkage.
8.Discrete event scheduler.
9.Cheap- Does not require costly equipment
10. Complex scenarios can be easily tested.
11. Results can be obtained quickly - more ideas can be tested in lesser time.
12. They also allow the designers of the system to study trouble at numerous abstraction levels.

3.3BASIC ARCHITECTURE OF NS2

The basic architecture of NS2. NS2 provides users with executable command ns which take on input argument, the name of a Tcl simulation scripting file.

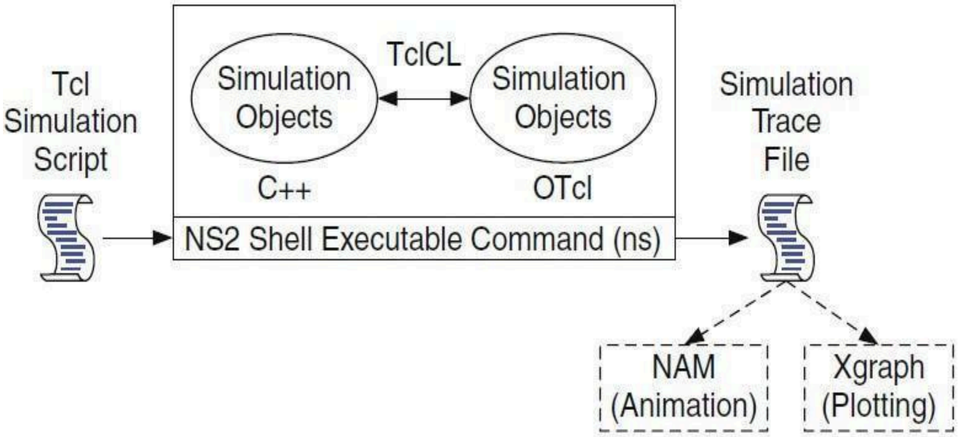


Figure 3.3 Architecture of NS2

Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend).

The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle (e.g., n as a Node handle) is just a string (e.g., _o10) in the OTcl domain, and does not contains any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++ object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts with users and other OTcl objects. It may define its own procedures and variables to facilitate the interaction.

The member procedures and variables in the OTcl domain are called instance procedures (instprocs) and instance variables (instvars), respectively.NS2 provides a large number of built-in C++ objects. It is advisable to use these C++ objects to set up a simulation using a Tcl simulation script.

However, advance users may find these objects insufficient. They need to develop their own C++ objects, and use a OTcl configuration interface to put together these objects. After simulation, NS2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used. To analyze a particular behaviour of the network, users can extract a relevant subset of text-based data and transform it to a more conceivable presentation. In these cases, iteration time (change the model and re-run) is more important. Thus, ns meets both of these needs with two
languages, C++ and OTcl.

3.4 INSTALLATION OF NS2

Step 1: Install the basic libraries like

```
$] sudo apt install build-essential autoconf automake libxmu-dev Step 2:
```

Install gcc-4.8 and g++-4.8

Open the file using sudo mode

```
$] sudo nano /etc/apt/sources.list Include the
```

following line

```
deb http://in.archive.ubuntu.com/ubuntu bionic main universe
```

```
$] sudo apt update
```

```
$] sudo apt install gcc-4.8 g++-4.8
```

Step 3: Unzip the ns2 packages to home folder

```
$] tar zxvf ns-allinone-2.35.tar.gz
```

$] cd ns-allinone-2.35/ns-2.35 Modify the

following make files.

~ns-2.35/Makefile.in Change

@CC@ to gcc-4.8 Change

@CXX@ to g++-4.8

~nam-1.15/Makefile.in

~xgraph-12.2/Makefile.in

~otcl-1.14/Makefile.in Change in

all places @CC@ to gcc-4.8

@CPP@ or @CXX@ to g++-4.8 Open the

file: ~ns-2.35/linkstate/ls.h

Change at the Line no 137: void eraseAll( ) { erase(baseMap::begin( ),

baseMap::end( )); } to
this void eraseAll( ) { this->erase(baseMap::begin( ), baseMap::end( )); } Step 4:

Open a new terminal

$] cd ns-allinone-2.35/

$] . /install

Step 5 - Set the PATH Open a

new Terminal,

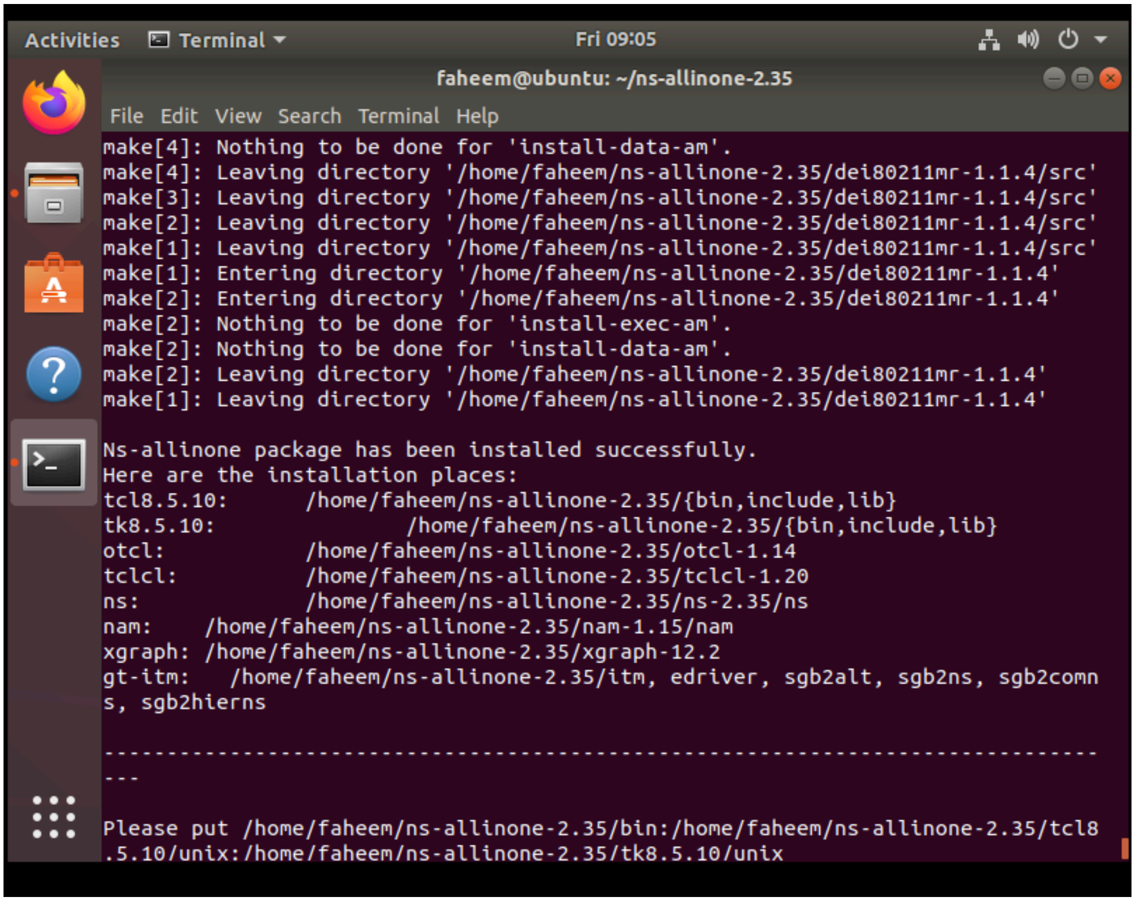
$] gedit .bashrc

Paste the following lines

Export PATH=$PATH:/home/<yourusername>/ns-allinone-2.35/bin:/home/<yourusername>/ns-allinone-2.35/tcl8.5.10/unix:/home/<yourusername>/ns-allinone-2.35/tk8.5.10/unix export LD_LIBRARY_PATH=/home/<your user name>/ns-allinone-2.35/otcl-1.14:/home/<yourusername>/ns-allinone- 2.35/lib

Logout and Login back or $] source .bashrc

Upon successful installation, we obtain $ symbol at command prompt


Activities
Terminal
Fri 09:05
faheem@ubuntu: ~/ns-allinone-2.35
File Edit View Search Terminal Help

```
make[4]: Nothing to be done for 'install-data-am'.
make[4]: Leaving directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4/src'
make[3]: Leaving directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4/src'
make[2]: Leaving directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4/src'
make[1]: Leaving directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4/src'
make[1]: Entering directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4'
make[2]: Entering directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4'
make[1]: Leaving directory '/home/faheem/ns-allinone-2.35/dei80211mr-1.1.4'

Ns-allinone package has been installed successfully.
Here are the installation places:
tcl8.5.10:      /home/faheem/ns-allinone-2.35/{bin,include,lib}
tk8.5.10:               /home/faheem/ns-allinone-2.35/{bin,include,lib}
otcl:           /home/faheem/ns-allinone-2.35/otcl-1.14
tclcl:          /home/faheem/ns-allinone-2.35/tclcl-1.20
ns:             /home/faheem/ns-allinone-2.35/ns-2.35/ns
nam:    /home/faheem/ns-allinone-2.35/nam-1.15/nam
xgraph: /home/faheem/ns-allinone-2.35/xgraph-12.2
gt-itm:   /home/faheem/ns-allinone-2.35/itm, edriver, sgb2alt, sgb2ns, sgb2comn
s, sgb2hierns

-------------------------------------------------------------------------------
---

Please put /home/faheem/ns-allinone-2.35/bin:/home/faheem/ns-allinone-2.35/tcl8
.5.10/unix:/home/faheem/ns-allinone-2.35/tk8.5.10/unix
```

FIGURE 3.4

CHAPTER-4
AODV ROUTING PROTOCOLS

4.1 INTRODUCTION:~

AODV (Ad-hoc On-demand Distance Vector) is a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures and packet losses.

AODV is an on-demand algorithm, meaning that it builds routes between nodes only as desired by source nodes.It maintains these routes as long as they are needed by the sources.The figure 4.1 explains the aodv(Ad hoc On-Demand Distance Vector) process as the source uses the rreq(route request) on its neighbouring node to confirm the behaviours of that specific node. The corresponding node will give rrep(route reply)as a respond.This process continious untill the source reaches its destination.

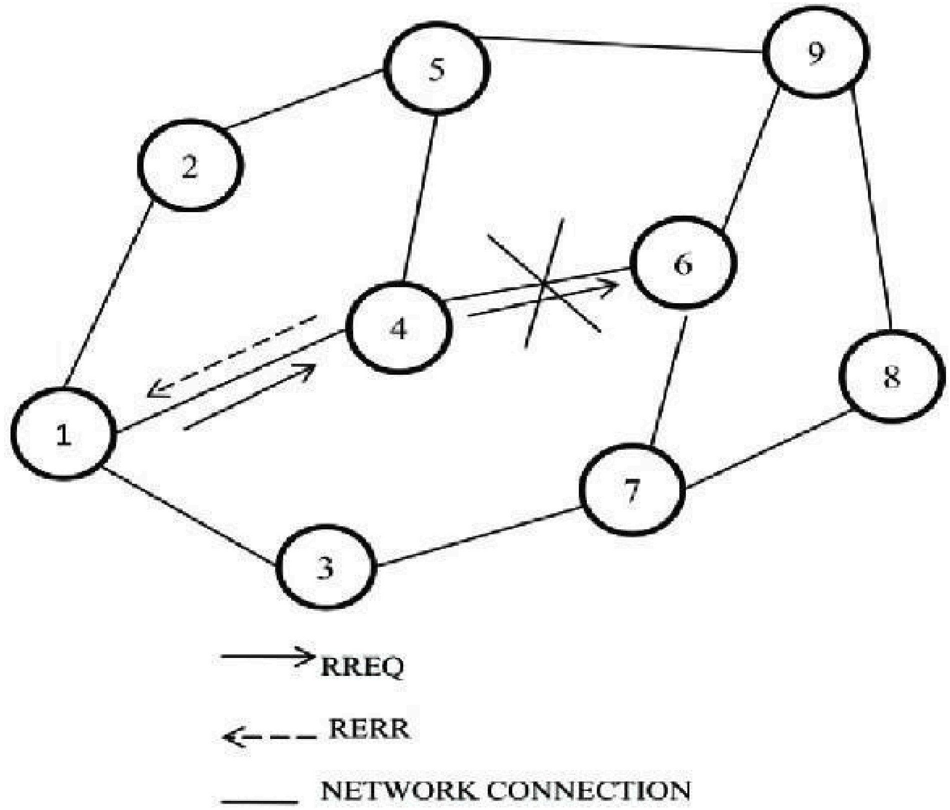


figure 4.1

4.2 Types of routing in AODV :~

There are three types of routing in ad hoc on demand vector,they are:~

1. RREP
2. RREQ
3. REER

4.2.1 RREP:~

In the context of Wireless Sensor Networks (WSN), RREP typically stands for Route Reply, which is a control message used in the Ad Hoc On-Demand Distance Vector (AODV) routing protocol. When a node in a WSN needs to send a packet to a destination node and does not have a route to it, it initiates a Route Discovery process.

4.2.2 RREQ:~

In the context of Wireless Sensor Networks (WSN), RREQ typically stands for Route Request, and it is associated with the Ad Hoc On-Demand Distance Vector (AODV) routing protocol.When a node in a WSN needs to send a packet to a destination node and does not have a route to it, it initiates a Route Discovery process.The RREQ continues to be propagated through the network until it reaches the destination node or a node with a valid route to the destination.

4.2.2REER:~

AODV typically has less overhead as a reactive protocol (less route maintenance messages) than proactive. In the event of the connection interruption that the path no longer functions, i.e. messages cannot be sent, a RERR message is sent through a node detecting the link interruption. The message is re-cast by other nodes. The RERR message shows the unattainable destination. Message receiving nodes inactivates the route.

CHAPTER 5

DETECTION OF BLACKHOLE ATTACK

5.1 INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a critical technology, enabling efficient monitoring and data collection in various domains, from environmental sensing to healthcare. However, within the realm of WSNs, a lurking threat known as the "Black Hole" has become a significant concern. Similar to its cosmic counterpart, the Black Hole in WSNs represents a malicious entity capable of disrupting communication and compromising the integrity of the network.

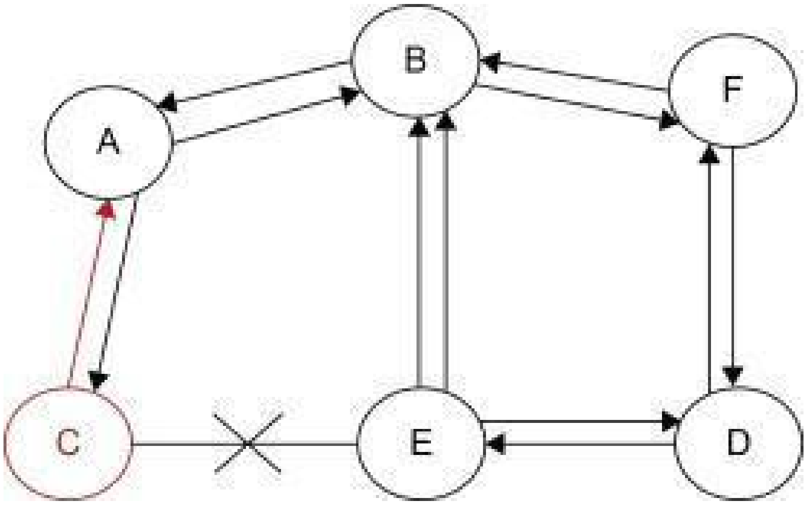


FIGURE 5.1

As Wireless Sensor Networks continue to play a pivotal role in modern technological applications, addressing security threats such as the Black Hole attack is paramount. The collaborative efforts of researchers, developers, and policymakers are essential to fortify WSNs against these malicious entities.

Here are some commonly used methods for detecting black hole attacks in WSNs:

5.2.1 WATCHDOG MECHANISM:

In a Watchdog-based approach, each node monitors the behavior of its neighbors.Nodes (watchdogs) check if their neighboring nodes are forwarding the data packets they claim to receive.If a node is detected as a potential black hole, it can be isolated, and alternative paths can be explored.

5.2.2 NEIGHBOR MONITORING:

Nodes continuously monitor the behavior of their neighbors.
If a node notices that a neighbor consistently claims to have the shortest path to the sink but fails to forward packets, it raises an alarm.Collaborative monitoring among nodes enhances the accuracy of detection.

5.2.3 ENERGY CONSUMPTION MONITORING:

Black hole nodes may exhibit abnormal energy consumption patterns since they may be actively participating in dropping packets.By monitoring the energy consumption of neighboring nodes, anomalies can be detected, and nodes with suspicious behavior can be isolated.

5.2.4 TRUST-BASED APPROACHES:

Establishing trust relationships among nodes can be effective. Nodes maintain a trust level for each of their neighbors based on their past behavior.Suspicious nodes with low trust levels can be avoided, reducing the chances of falling victim to black hole attacks.

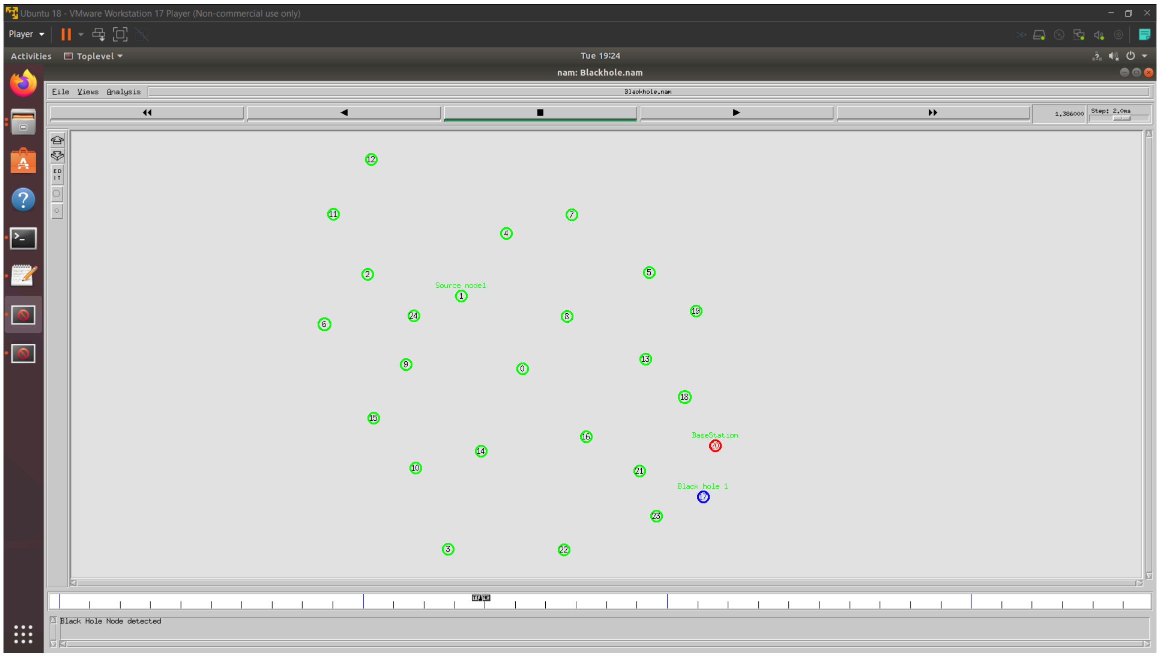
CHAPTER 6

RESULTS AND DISCUSSION

The performance of the black hole attack was analysed by using NS2 simulation software. Node 1 as a source node and node 20 as a black node. The black hole node is represented by red colour. The hash value was calculated by using RIPEMD algorithm which is stored in each sensor node.

When a new node advertises to provide a shorter route to the base station, it is necessary to find if the new advertising node is a trustable node or a malicious node. The sink hole node is identified by comparing the hash value which are stored in the data base and the present value. The black hole node is represented by blue colour. The simulation output of detection of black hole attack is shown in fig.6.1.

.



```
Black Hole Node detected
```

Figure.6.1

CHAPTER 7

CONCLUSION

In conclusion, the mini-project focused on the detection and prevention of black holes in Wireless Sensor Networks (WSNs) using the Ad- hoc On-Demand Distance Vector (AODV) routing protocol. The primary objective was to enhance the security and reliability of WSNs by addressing the potential threat of black hole attacks.
Through the implementation of AODV, we aimed to create a robust and dynamic routing mechanism that could adapt to the changing network conditions and detect anomalous behavior indicative of a black hole.

The methodology involved integrating additional security mechanisms within the AODV protocol to identify and prevent malicious nodes from disrupting the network.

The project demonstrated that by leveraging the inherent capabilities of AODV and incorporating security measures, it is possible to enhance the WSN's resilience against black hole attacks. The proposed solution not only detected the presence of black holes promptly but also mitigated the impact by dynamically rerouting traffic through secure paths.

Furthermore, the evaluation of the implemented solution revealed promising results in terms of detection accuracy and prevention effectiveness. The approach proved to be scalable and efficient, ensuring minimal overhead on the network while maintaining reliable communication.

In future work, further optimization and fine-tuning of the proposed solution could be explored to improve its performance under various network scenarios. Additionally, extending the study to consider other types of attacks and integrating more advanced security mechanisms could contribute to a comprehensive and holistic approach to WSN security.

CHAPTER 8

REFERENCES

[1]Ruslan Dautov and Gill R Tsouri[2019] Effects of Passive Negative Correlation Attack on Sensors Utilizing Physical key Extraction in Indoor Wireless Body Area Networks

[2]DAWEI LIU, MEMBER,YUEDONG XU, AND XIN HUANG[2017] Identification of Location Spoofing in Wireless Sensor Networks in Non-Line-of-Sight Conditions

[3]OHIDA RUFAI AHUTU AND HOSAM EL-OCLA[2020] Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks

[4]LEI SHI, QINGCHEN LIU, JINLIANG SHAO, AND YUHUA CHENG[2020] Distributed
Localization in Wireless Sensor Networks Under Denial-of-Service Attacks

[5]OPEYEMI OSANAIYE, ATTAHIRU S. ALFA GERHARD P. HANCKE[2018] Denial of Service
(DoS) Defence for Resource Availability in Wireless Sensor Networks

[6]PATEL BHOOMIKA D,PATEL ASHISH D[2016] A Trust Based Solution for Detection of Network Layer Attacks in Sensor Networks

[7]DR. MUAZZAM A KHAN, JAWAD AHMAD, ASAD W. MALIK, AND ANIS UR REHMAN[2018] Detection and Prevention of Black Hole Attacks in IOT & WSN

[8]SARITA AGRAWAL , MANIK LAL AND JAVIER LOPEZ[2017] Detection of Node Capture Attack in Wireless Sensor Networks

[9]WATEEN A. ALIADY AND SAAD A. AL-AHMADI[2019] Energy Preserving Secure Measure Against Wormhole Attack in Wireless

[10]DHARA BUCH,D. C. JINWALA[2010] Denial of Service Attacks in Wireless Sensor Networks

[11]MANDEEP KUMAR AND JAHID ALI[2022] Taylor Sailfish Optimizer-Based Deep Stacked Auto Encoder for Blackhole Attack Detection in Wireless Sensor Network

[12]MISS. PRACHI S. MOON MR. PIYUSH K. INGOLE[2015] An Overview on: Intrusion
Detection System with Secure Hybrid Mechanism in Wireless Sensor Network

[13]ASHISH JAIN MADHU SHARMA[2016] Wormhole Attack in Mobile Ad-hoc Networks

[14]Karthiga Devi, S. Balamurali and M. Venkatesulu, "Based on NeighborDensity EstimationTechnique to Improve theQuality of Service and todetect and Prevent the Sinkhole Attack in Wireless Sensor Network

[15]Abdulmalik Danmallam Bello, Dr. O. S. Lamba, 2020, How to Detect andMitigate Sinkhole Attack in Wireless Sensor Network International Journalof Engineering Research & Technology (IJERT) Volume 09, Issue 05

[16]Semagn Shifere et al. Department of Computer Science Woldia University, Ethiopia ,Volume 6, Issue 2, February – 2021 International Journal of Innovative Science and Research Technology ISSN No:-2456-2165.

[17]Dhivya M et al. vol.2, 2021, Detection and Prevention of Sinkhole Attack inWireless Sensor Network using Armstrong 16-digit Key Identity and GANNetwork

[18]Sihem Aissaoui & Sofiane Boukli, Sinkhole attack detection based on SVM in wireless sensor network, international journal of wireless networks and broadcast technologies,IGI Global, vol. 10(2), pages 16-31, July.

[19]Sumit Pundir et al. [2020] designed efficient sinkhole attack detectionmechanism in egde based IoT deployment

[20]Neha Singh, Kamakshi Rautela [2016], International Journal of Engineering and Computer Science ISSN: 2319 – 7242, Volume 5, pp. no. 17544-m