

# Simulation of Blackhole Attack in WSN Cluster Topology

By

**Ovejite Saha**

ID: CSE2001019268

**Md Jewel Rana**

ID: CSE2001019117

**Md. Rajon Miah**

ID: CSE2001019226

**Md. Alamin**

ID: CSE1803015002

Supervised by

**Mohammad Naderuzzaman**

Submitted in partial fulfillment of the requirements for the degree of Bachelor of Science  
in Computer Science and Engineering



**Department of Computer Science & Engineering  
Sonargaon University(SU)**

September, 2023

# Approval

The thesis titled “**Simulation of Blackhole Attack in WSN Cluster Topology**” has been submitted to the following respected members of the board of Examiners of the Department of Computer Science in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science on - by Ovejite Saha (CSE2001019268), Md Jewel Rana (CSE2001019117), Md. Rajon Miah (CSE2001019226) and Md. Alamin (CSE1803015002) has been accepted as satisfactory.

.....

**Mohammad Naderuzzaman**

Assistant Professor

Department of Computer Science & Engineering  
Sonargaon University (SU)

**Supervisor**

.....

(Examiner Name & Signature)

Examiner

Department of Computer Science & Engineering  
Sonargaon University (SU)

**Examiner 1**

.....

(Examiner Name & Signature)

Examiner

Department of Computer Science & Engineering  
Sonargaon University (SU)

**Examiner 2**

.....

(Examiner Name & Signature)

Examiner

Department of Computer Science & Engineering  
Sonargaon University (SU)

**Examiner 3**

# Declaration

We, hereby, declare that the thesis work presented in this report is the outcome of the investigation performed by us under the supervision of **Mohammad Naderuzzaman**, Department of Computer Science and Engineering, Sonargaon University (SU), Dhaka, Bangladesh. We reaffirm that no part of this thesis has been or is being submitted elsewhere for the award of any degree or diploma.

Countersigned

Signature

.....  
**(Mohammad Naderuzzaman)**  
**Supervisor**

.....  
(Ovejite Saha)  
ID: CSE2001019268

.....  
(Md Jewel Rana)  
ID: CSE2001019117

.....  
(Md. Rajon Miah)  
ID: CSE2001019226

.....  
(Md. Alamin)  
ID: CSE1803015002

# Abstract

Wireless Sensor Networks (WSNs) have sensor nodes that sense and extract information from the surrounding environment, locally processing information and then wirelessly transmitting it to the sink.

Data sinks are a fundamental component of data storage, and they play a critical role in ensuring that data is accessible, secure, and reliable. Data sinks work by receiving data from one or more data sources and storing that data in a format that is optimized for retrieval and analysis. Depending on the type of data sink.

Wireless multimedia sensor networks (WMSNs) could be present. As multimedia data is larger than scalar data, that's why we need Wireless Multimedia Sensor Networks (WMSNs). In terms of efficient use of energy, throughput, and reduced end-to-end delay, Multi-path routing is used to discover multi-path during route discovery from source to sink.

In blackhole attack, the attacker drops packets selectively, or all control and data packets that are routed through him. Therefore, any packet routed through this intermediate malicious node will suffer from partial or total data loss. Since the data sink attack is detected only after the black hole attack, we used the black hole attack in this case.

Considering the point in this thesis are going to implement a Simulation of a Black-hole Attack in WSN. We are showing a simple scenario of attacking if wireless security has some weak points. Cluster Topology is an experiment with the "NS-2" simulator and discloses enhanced results for multimedia data, Index Terms WMSNs, multimedia data, end-to-end delay, Black hole attack, Cluster topology, NS-2, and multi-path routing. In the simulation, we can understand how a malicious node affects of node and how to drop packets. This is just a simple copy of on process that happened in real life. Some nodes are affected by a malicious node which is an attacker that blocks, drops, sends, and receives packets.

We suggest to ensure better security and encryption to prevent this type of case. Overall, we are emphasizing there is a possibility of attacking by hackers with another signal. This attack can be protected by high-level security and a special firewall system, which can control the network as much as possible.

# Acknowledgement

At the very beginning, we would like to express our deepest gratitude to the Almighty for giving us the ability and strength to finish the task successfully within the scheduled time. We would like to thank our supervisor **Mohammad Naderuzzaman** for his help and supervision.

We also would like to thank **Bulbul Ahamed**, Associate Professor & Head, Department of Computer Science and Engineering, Sonargaon University (SU) whose hearted and valuable support with best concern and direction acted as necessary recourse to carry out our project.

We want to convey our special gratitude to Brig. Gen. (Retd) **Prof. Habibur Rahman Kamal**, ndc, psc, Dean, Faculty of Science and Engineering for his kind concern and precious suggestions.

We are also thankful to all our faculty Teachers.

We are also happy to thank **Dr. T S Pradeep Kumar**, Professor in Computer Science and Engineering at VIT Chennai for his guideline. At last, we want to give thanks to the full **Overleaf teams** for making a collaborative cloud-based LaTeX editor used for writing, editing, and publishing scientific documents.

# List of Abbreviations

<b>Acronym</b>	<b>Description</b>
ACK	Acknowledgement
AODV	Ad-Hoc on Demand Routing Vector
ARAN	Authenticate Routing for Ad-Hoc Networks
CM	Control Module
CHs	Cluster-Head
CREP	Route Confirmation Reply
DOS	Denial of Service
DSR	Distance Source Routing
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Message Authentication Code
MANET	Mobile Ad-Hoc Network
NS-2	Network Simulator-2
Nam	Network Animator
PDA	Personal Device Assistance
RREQ	Route Request
RREP	Route Reply
SAODV	Secure Ad-hoc On-Demand Distance Vector Routing
TCP	Transmission Control Protocol
TC	Topology Control
TCL	Tool Command Language
TR	TomeRaider EBook Format
TORA	Temporally Ordered Routing Algorithm
GRP	Geographic Routing Protocol
WSN	Wireless Sensor Networks
WMSN <sub>s</sub>	Wireless multimedia sensor networks
WPAN	Wireless Personal Area Network
Wi-Fi	Wireless Fidelity

# Contents

<b>List of Figures</b>	<b>VIII</b>
<b>List of Tables</b>	<b>X</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.2 Characteristics of WSN . . . . .	1
1.2.1 Computing capacities . . . . .	2
1.2.2 Power of the battery . . . . .	2
1.2.3 Capacity . . . . .	2
1.2.4 Wireless network sensor reliability . . . . .	3
1.2.5 Wireless network application . . . . .	3
1.2.6 Importance of application . . . . .	4
1.3 Threats in WSN . . . . .	4
1.3.1 Black hole . . . . .	4
1.3.2 HELLO Flood Attack . . . . .	5
1.3.3 Jamming . . . . .	5
1.3.4 Blackmail Attack . . . . .	5
1.3.5 Wormhole Attack . . . . .	6
1.3.6 Sybil attack . . . . .	6
1.3.7 Tampering attack . . . . .	6
1.3.8 Selective Forwarding Attack . . . . .	7
1.4 AODV Routing Protocol . . . . .	7
1.5 Problem Statement . . . . .	8
1.6 Motivation . . . . .	8
1.7 Objectives . . . . .	8
1.8 Cluster Topology . . . . .	8
1.9 Working Process . . . . .	9
<b>2 OVERVIEW OF Attacks in WSN</b>	<b>10</b>
2.1 Black hole attack . . . . .	10
2.1.1 Introduction . . . . .	10
2.1.2 External Black hole attack . . . . .	10
2.1.3 Attacking process . . . . .	12
<b>3 Simulation</b>	<b>13</b>
3.1 Simulation Setup . . . . .	13
3.2 Simulation Details . . . . .	13

3.3	Creating Cluster topology . . . . .	14
3.4	Implementing Black Hole Attack . . . . .	14
3.5	Simulation File . . . . .	14
3.6	Simulation Without Attacker . . . . .	15
3.6.1	Normal Position of Nodes . . . . .	15
3.6.2	Packet Sending . . . . .	15
3.6.3	Status Without Attacker . . . . .	15
3.7	Simulation With Attacker . . . . .	16
3.7.1	Normal Position of Nodes . . . . .	16
3.7.2	Packet Sending . . . . .	16
3.7.3	Block Or Drop By Attacker . . . . .	17
3.7.4	Status With Attacker . . . . .	17
<b>4</b>	<b>Analysis</b>	<b>19</b>
4.1	Result Analysis . . . . .	19
4.2	Analysis Methods . . . . .	19
4.2.1	Average throughput . . . . .	19
4.2.2	Instantaneous throughput . . . . .	21
4.2.3	Average Delay . . . . .	21
4.2.4	Instantaneous delay . . . . .	22
4.2.5	Average goodput . . . . .	22
4.2.6	Instantaneous goodput . . . . .	23
4.2.7	Average jitter . . . . .	23
4.2.8	Instantaneous jitter . . . . .	24
4.2.9	Average Residual Energy . . . . .	24
4.2.10	Residual Energy for particular node . . . . .	24
4.2.11	Packet Delivery Ratio . . . . .	25
4.2.12	Normalised Routing Load . . . . .	25
<b>5</b>	<b>Discussion</b>	<b>26</b>
5.1	Graph of Instantaneous throughput . . . . .	26
5.2	Graph of Instantaneous delay . . . . .	27
5.3	Graph of Instantaneous goodput . . . . .	27
5.4	Graph of Instantaneous jitter . . . . .	28
<b>6</b>	<b>Discussions</b>	<b>29</b>
<b>7</b>	<b>Conclusion</b>	<b>31</b>



# List of Figures

1.1	WSN Scenario . . . . .	2
1.2	Blackhole Attack . . . . .	5
1.3	HELLO Flood Attack . . . . .	5
1.4	Jamming Attack . . . . .	5
1.5	Blackmail Attack . . . . .	6
1.6	Wormhole Attack . . . . .	6
1.7	Sybil attack . . . . .	6
1.8	Tampering attack . . . . .	7
1.9	Selective Forwarding Attack . . . . .	7
2.1	Blackhole Attack In WSN . . . . .	10
2.2	Black hole attack specification . . . . .	11
3.1	Creating Cluster topology . . . . .	14
3.2	Normal Position of Nodes Without Attacker . . . . .	15
3.3	Packet Sending Without Attacker . . . . .	16
3.4	Status Without Attacker . . . . .	16
3.5	Normal Position of Nodes With Attacker . . . . .	16
3.6	Packet Sending Block By Attacker . . . . .	17
3.7	Data Blocking By Attacker . . . . .	17
3.8	Status With Attacker . . . . .	18
4.1	Result Analysis . . . . .	19
4.2	Analysis of Average throughput . . . . .	20
4.3	Analysis of Instantaneous throughput . . . . .	21
4.4	Analysis of Average Delay . . . . .	21
4.5	Analysis of Instantaneous delay . . . . .	22
4.6	Analysis of Average goodput . . . . .	22
4.7	Analysis of Instantaneous goodput . . . . .	23
4.8	Analysis of Average jitter . . . . .	23
4.9	Analysis of Instantaneous jitter . . . . .	24
4.10	Analysis of Average Residual Energy . . . . .	24
4.11	Analysis of Residual Energy for particular node . . . . .	25
4.12	Analysis of Packet Delivery Ratio . . . . .	25
4.13	Analysis of Normalised Routing Load . . . . .	25
5.1	Graph of Instantaneous throughput . . . . .	26
5.2	Graph of Instantaneous delay . . . . .	27
5.3	Graph of Instantaneous goodput . . . . .	27

5.4 Graph of Instantaneous jitter . . . . . 28

# List of Tables

3.1	Simulation Setup. . . . .	13
3.2	Simulation Details. . . . .	14
3.3	Simulation Files Types . . . . .	15
4.1	Analysis Methods . . . . .	20

# Chapter 1

## Introduction

### 1.1 Background

A wireless sensor network can be defined as communicating information gathered from an area monitored through wireless links. The network of wireless sensors communicates data through multiple nodes and a gateway[1] These nodes are interconnected to other networks like Wi-Fi. WSN is made up of base stations and node numbers. They use networks to track sound, noise, temperature, and the mutual transfer of data to primary places across the network. physical and environmental conditions are monitored. Often sensitive data are transmitted through unsecured means to the target node. Therefore, denial-of-the-assail will quickly add WSN. Service attacks (DoS) together cause a loss of information and high energy consumption. WSNs are widely available independent sensors in physical or environmental terms and can communicate their data in collaboration via the network. In various applications, a wireless sensor network is used for military activities to track your enemy's movement, for instance. A safe pulse track device was also used for fire prevention and detection. It is a part of our everyday lives slowly and steadily. The US has identified a high-level research project age. Wireless sensor networks consist of a large number of sensor nodes. Wireless communication interacts with each other. Normally a sensor node has five components: detection, memory, processor, transceiver, and battery. As such, their resources (usually battery life, memory decrease, and capacity for processing) are reduced. Due to the braking power of communication, wireless sensor nodes can only communicate directly with some nearby neighbors. So, the nodes must work together to accomplish their tasks: feeling, reporting processing, computing, routing, localization, security, etc. Therefore, WSN is, by nature, a collaborative network.[2]

### 1.2 Characteristics of WSN

A network of wireless sensors includes a significant but small part including a sensor node. Efficiency, scalability, transparency, reliability, and versatility are the characteristics of an excellent wireless sensor network. Such features can be very useful for wireless sensor networks, and if left unnoticed or approved, this can result in preliminary results A biased network therefore can not apply. The wireless network comprises mobile communications, wireless LAN, Ethernet, ad hoc networks, etc.[3] A sensor network, which is similar to an Ad hoc system, has several features, including mobility, battery limit, and switching

characteristics.[4] WSN and certain distinct features relative to these wireless networks.

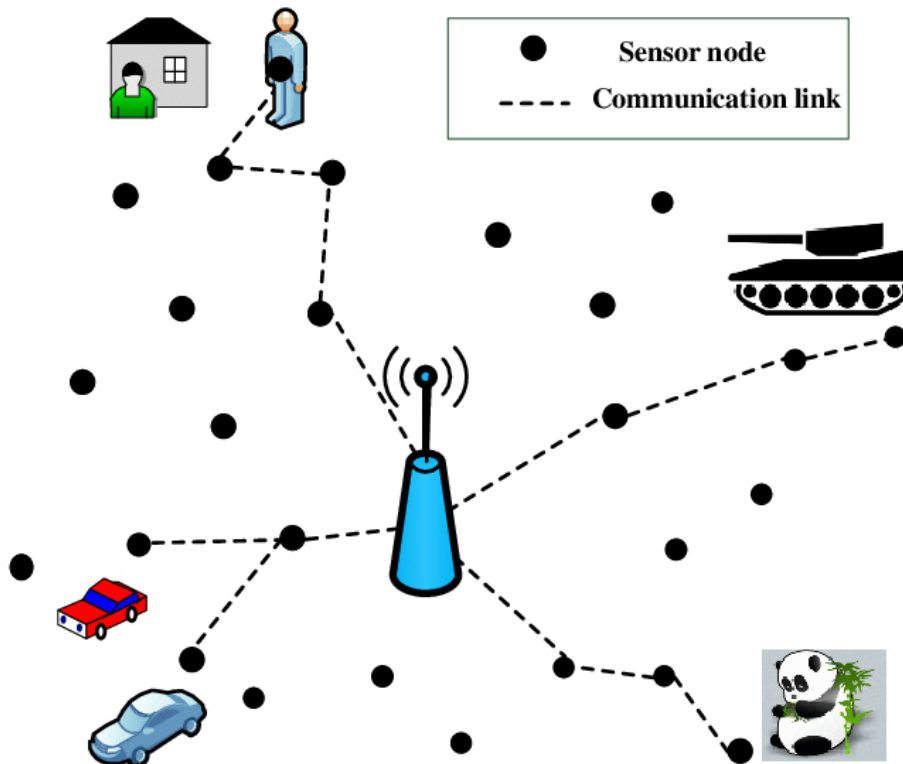


Figure 1.1: WSN Scenario.

The features of the WSN are

### 1.2.1 Computing capacities

The space for the system and the sensor memory are very limited due to the cost, size, and consumption of batteries.

### 1.2.2 Power of the battery

Sensor nodes are often canceled and decreased due to exhaustion. To retain battery power beforehand, protocols and algorithms must be considered for communications

### 1.2.3 Capacity

The Sensor network's transmission bandwidth is narrow and variable, with a distance between a few tens and a few hundred meters. Because the sensor is easily influenced by natural environmental impacts such as mountains, buildings, floods, precipitation and lighting, ground barriers, and temperature. It is hard to run WSN smoothly for that reason. It means the strong, non-partisan, stable WSN software and hardware, a research focal point for the future.[5]

#### 1.2.4 Wireless network sensor reliability

Any network that is the basic requirement needs to be reliable. In a state of constant network structure transition, you expect reliable data transmission. For ad hoc wireless networks, there is often an inverse relation between scalability and reliability.[6] The explanation is that it becomes harder to maintain stability as the number of nodes in the network increases. Data transmission efficiency is placed on the network when highly scalable and built into a bigger network than was originally intended, and the point of departure will appear earlier. Mobility is the ability of networks to handle mobile nodes and through data paths. In order for the wireless sensor network to handle mobility, it is necessary to do the design. The design of a large-scale and mobile wireless sensor network is thus harder.[7]

#### 1.2.5 Wireless network application

In modern society, WSN is used all over the place. It has been applied successfully in various domains including political, ordinary, economic, health, and industrial applications. Even though the number of wireless sensor implementations is high, there's no exact "mote" standard. The word mote means a small frame, but there can be no utter isolation. Regardless of the exact platform category, known applications may be categorized under certain headings: military applications, environmental monitoring, industrial or human-centric applications, and robotics applications.

**Some of the requirements are listed below:[8]**

**Military applications:** The idea of wireless networks with sensors is closely linked to military applications. Nonetheless, whether bases were designed for military or air defense purposes, or whether they were invented separately and used for military purposes, is very difficult to say with certainty. The area of interest in military applications includes general information collection, enemy monitoring, surveillance of the battlefield, and classification. For example, classification algorithms use seismic and acoustic signal detection input data.

**Environmental monitoring:** Various environmental monitoring criteria exist, including wind speed calculation and path parameters. Show contours of WSN applications of the environmental monitoring program. Many of them slowly change behaviors that allow you to effectively sample them during their reaction for about one to five minutes. But interesting in such a situation was the Rock wheel phenomenon, which has taken a long time to find. Real-time environmental surveillance examples of system applications using WSNs are required for the following technical requirements.

**Forest monitoring:** The forest's importance and its significance for the soil play a key role in human life and an unparalleled role in sustaining the biogeochemical cycle of the environment. Reforestation due to urbanization is of extreme social significance. Furthermore, forest surveillance is required. WSNs are normally used in the above range in order to maintain protection. In view of the expected climate change, monitoring of the microclimate in the forest is increasingly important. Intensive surveillance of forestry ecosystems can contribute to the detailed knowledge of the physical, chemical, and biological status of the soil in the root systems of trees.

**WSN in medicine:** WSN uses the most advanced medical system in healthcare to improve wellness applications. As an example of real-time applications for health monitoring, WSN is used to monitor diseases such as heart attacks. In a hospital environment, scientists have researched an in-house sensor and found it significant. The patients receiving admission to the Emergency Unit of John Hopkins Hospital, USA, were examined at blood oxygen levels and heart rate. The authors have collected statistics on the RF network links, tree trucking activity, and its reality within the network.

**Industrial uses:** In an industrial application this is very useful. Such sensors also track, regulate and process data such as sound, vibration, temperature, and viscosities. These sensors are used. Data or information sent to the control system management is gathered by sensors. They also play a key role when the business process is implemented.[9] A better routing algorithm provides a robust, user-friendly system, and cost-effective devices which are extremely useful for business purposes. The WSN uses the building's decision-aid systems to avoid different real-world problems. More and more are also used in agriculture to overcome the decision support system

## 1.2.6 Importance of application

WSN is a consolidated data collection, a multi-hop communication, and a multi-to-one model of traffic. The WSN is special and very reliant on applications from conventional networks. The primary purpose is to collect environmental knowledge. Different network implementations of sensors manage various physical signals; one network of sensors cannot be routing protocols on the other. One of the most important issues in the WSN is the importance of applications.[10]

## 1.3 Threats in WSN

There are two kinds of attacks in WSN. They are passive and active attacks.

Passive assault is restricted to the listening and review of information exchanged. These attacks (sufficient to have the right receiver) can be easier to perform and are hard to detect. Since there is no impact on the information shared by the attacker. By analyzing information routings and preparing an active attack, the attacker may want to know the confidential information or the significant nodes in the network (cluster head node).[11]

An attacker tries to remove or edit messages sent on the networks during successful attacks. He may also replay old messages or inject his own traffic to interrupt the network's operation or cause a service denial. We may quote from the most well-known active attacks.[12]

### 1.3.1 Black hole

A node falsifies routing information in order to force data to move through later, and the only function is to migrate anything and create a sink or a black hole on your network

Selective transmission: as mentioned above, the router is a Node. Malicious nodes may fail to transmit and simply drop those messages during selective forwarding attacks.[13]

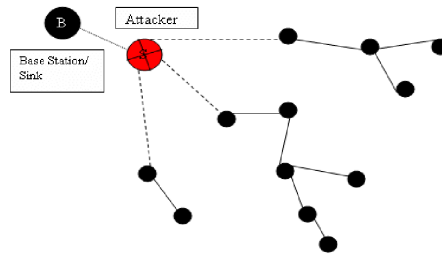


Figure 1.2: Blackhole Attack

### 1.3.2 HELLO Flood Attack

Most routing protocols use the "HELLO" packet to find nearby nodes, thereby creating a network topology. The best attack for an attacker is to send a cascade of such messages to the network and block the exchange of other messages.

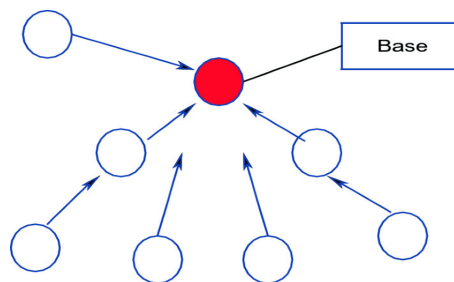


Figure 1.3: HELLO Flood Attack

### 1.3.3 Jamming

A well-known WiFi attack is to interrupt the radio channel by sending useless frequency band information. This sporadic or persistent jamming can be temporary.

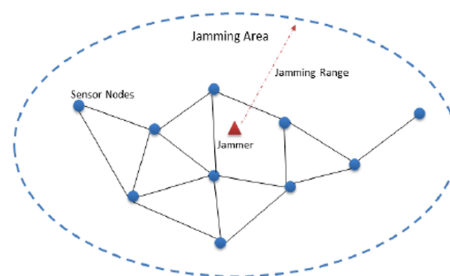


Figure 1.4: Jamming Attack

### 1.3.4 Blackmail Attack

A malicious node declares an additional legitimate node that excludes the latter from the network. If the malicious node attacks a large number of nodes, the activity of the



network can be interrupted. Extent. to use all the energy resources of the victim's node by pressuring them to measure or to excessively collect or transmit data.



Figure 1.5: Blackmail Attack

### 1.3.5 Wormhole Attack

Attackers here at different points of a network are strategically placed. You will receive and replay messages in various parts through a tunnel.

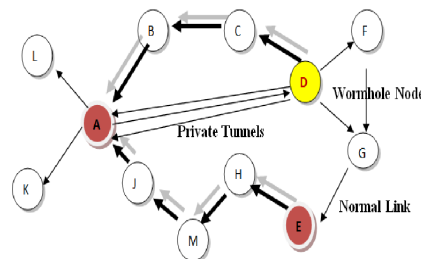


Figure 1.6: Wormhole Attack

### 1.3.6 Sybil attack

A Sybil attack basically occurs in the network layer. This attack occurs in multiple locations at a time when geographical routing protocols are appearing. A malicious node is upholding its multiple identities in this network.

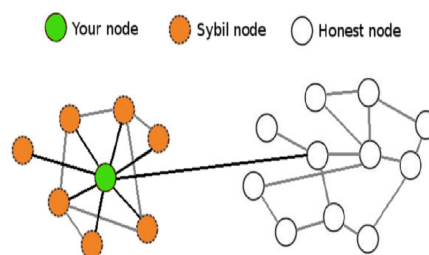


Figure 1.7: Sybil attack

### 1.3.7 Tampering attack

A tampering attack works in a whole network system. This attack easily damages a sensor node and its other node as a result the whole network is not working properly. In other words, it replaces the whole node and the whole part of its hardware service easily.

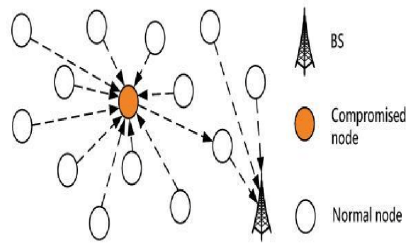


Figure 1.8: Tampering attack

### 1.3.8 Selective Forwarding Attack

This Selective and forwarding attack also occurs in the network layer. In this attack, the sensor networks some nodes want to forward the received message but some mentioned node easily replaces the whole node and part of its hardware services nation. However, some nodes easily start their connection from one route to another.

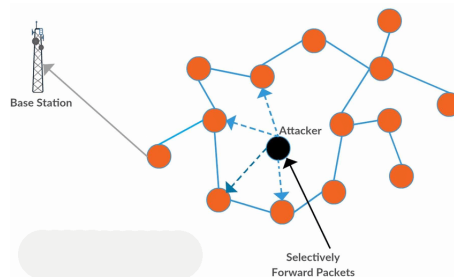


Figure 1.9: Selective Forwarding Attack

## 1.4 AODV Routing Protocol

Routing: Routing is information exchange from one network station to another and a set of rules or norms is used for the exchange of data between two devices. Routing: The usual limitations of these networks are protected by these protocols, including high power consumption, high error rate, and limited bandwidth. The protocols of routing are defined as:-(a) constructive (b) on-demand oriented (reactive) (c) protocols with a hybrid feature. The Ad-hoc On-demand Distance Vector (AODV) is a wireless and mobile ad hoc network routing protocol. Its protocol offers routes for both unicast and multicast routing on request. Nokia Research Center, the University of California, and Santa Barbara together developed the AODV protocol in 1991, as well as the University of Cincinnati. [14]

Only when requests are made for source nodes can the AODV protocol build routes between nodes. Consequently, AODV is considered an according algorithm and does not create extra connection traffic. The routes are kept as long as the sources need them. They are also trees that connect members of the multicast group. To ensure travel freshness, AODV uses sequence numbers. In addition to various mobile nodes, they are self-initiating and loop-free. Nets are not connected in AODV until links have been formed. Network nodes needing ties send a connection order. The other AODV nodes forward the message and record the link node. Therefore, they create several temporary

routes to the requested node. A node that receives these messages and has a path to a desired node sends a reverse message to the requested node via temporary routes. The application node uses the path with the least number of hops in other nodes. The entries not used in routing tables will be recycled after a period of time. If a connection fails, the routing mistake is returned and repeated. The routing error happens again.

## **1.5 Problem Statement**

Previously the works done on WSNs focused mainly on different security threats and attacks such as DoS, DDoS, Impersonation, Wormhole, Jellyfish, and Black Hole attacks. Among these attacks Black Hole attack involved in WSNs is evaluated based on reactive routing protocol like Ad-Hoc On-Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupts the performance of WSNs. Very little attention has been given to the fact to study the impact of Black Hole attacks in WSNs using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols under the attack, as well as the impacts of the attacks on the WSNs. This thesis analyzes Black Hole attacks in WSNs using AODV and OLSR which are reactive and proactive respectively in nature.

## **1.6 Motivation**

Wireless sensor networks (WSNs) are a new alternative in many fields to solve specific problems and are a demanding research field for the automation of embedded systems, impacting many applications. The efficient design of a network of wireless sensors has become a leading area of research in recent years. A sensor is a system that addresses and senses certain types of inputs under physical and environmental conditions, such as pressure, heat, and light. The sensor output is normally an electrical signal transmitted for further processing to a processor. But it has some threats. As I mentioned above there are a lot of attacks in WSN. The black hole is one of the popular attacks in WSN. Black hole attack affects network performance. WSN is a popular network and the application of this network is at the highest level so it has to be attack-free and perform at its best. As we want to keep it attacked we need to know the difference in the performance of the network with attack and without attack. We choose cluster topology to analyze the performance.

## **1.7 Objectives**

Our main objective is to analyze the performance of the WSN cluster topology which is attacked by the black hole. So we need to implement a black hole attack in cluster-based WSN. To analyze the performance we need to find results with some performance matrices.

## **1.8 Cluster Topology**

Introduction: A network of Wi-Fi sensors is made up of many wireless nodes. The topology control in WSNs is a way of identifying connections between nodes so that interference can be minimized, energy saved and network length extended. One is the

topology of classes to be regulated in the WSN. Clustering is one of the widely investigated solutions for the extensive flat sensor network and the efficiency of network operation

## **1.9 Working Process**

The network's two-layer cluster node approach breaks layers into two layers. The nodes in the same layer form a cluster in the first layer. There are many nodes in the second layer of the cluster. A cluster-head (CHs) node is used by each group to effectively spread the task between the cluster nodes. There remains a gateway node also. Through this process, the network becomes efficient because of energy saving less packet drop.

# Chapter 2

## OVERVIEW OF Attacks in WSN

### 2.1 Black hole attack

#### 2.1.1 Introduction

In WSN there are a lot of attacks. Among them, the black hole attack is one of the famous attacks and is easy to execute. A packet drop attack or black hole attack is a form of denial-of-service attack that discards packets from the router that is supposed to relay. This usually happens because several factors influence a router.[15]

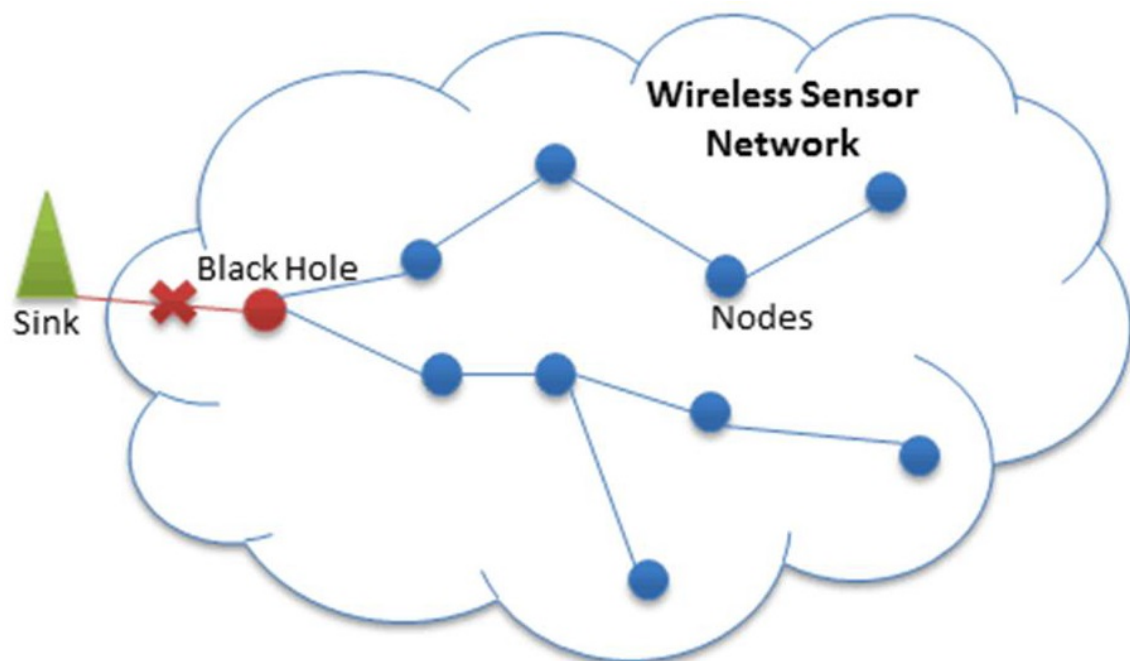


Figure 2.1: Blackhole Attack In WSN

#### 2.1.2 External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic creating congestion in the network or disrupting the entire network. The external attack can become a kind of internal attack when it takes control of an internal malicious node

and controls it to attack other nodes in MANET. External black hole attacks can be summarized in the following points

1. Malicious node detects the active route and notes the destination address.
2. A malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. The hop count value is set to the lowest value and the sequence number is set to the highest value.
3. The malicious node sends RREP to the nearest available node which belongs to the active route. This can also be sent directly to the data source node if the route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of the source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belongs in the route.

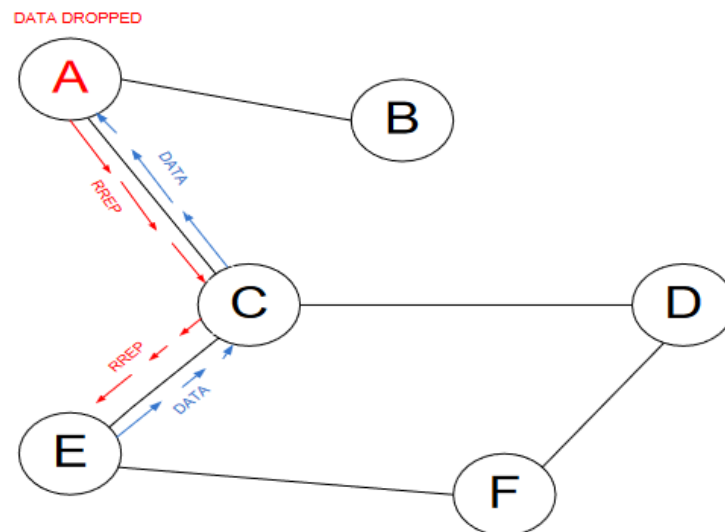


Figure 2.2: Black hole attack specification

In AODV black hole attack the malicious node “A” first detects the active route in between the sender “E” and destination node “D”. The malicious node “A” then sends the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way, data will arrive at the malicious node. These data will then be dropped. In this way, the sender and destination node will be in no position to communicate in a state of black hole attack.

### **2.1.3 Attacking process**

One of the potential WSN attacks is a Black hole attack. In a black hole attack, a malicious node sends the RREP message as the shortest path to the target node, and then the receiving node sends a data packet b to the malicious node in the network. Finally, the malicious Node drops the entire data packet instead of sending it to the destination node. As a result, the throughput gets low and the end-to-end delay gets high.[16]

# Chapter 3

## Simulation

### 3.1 Simulation Setup

To do the simulation, we used Network Simulator-2(NS-2.35). It runs frequently on Ubuntu. We used NAM animator so that we could see simulations. NS-2 simulator is used for implementing cluster topology and Blackhole attacks.[17]

Parameter	Value
Operating System	Ubuntu 20.04
Operating System Type	Linux
Simulation Software	NS-2.35
Network Animator	NAM 1.15
Graph	xgraph
Editor	gcc-4.8 g++-4.8
Code File	.tcl

Table 3.1: Simulation Setup.

### 3.2 Simulation Details

We used the AODV protocol. To implement this we run a .tcl file. After running the .tcl file we got .nam and .tr files. We get different kinds of values from the .tr file, which is a trace file. We use 17 nodes in this simulation and the area size is 500\*500. We giving a details table for simulation below



Parameter	Value
Protocol	AODV
Simulation Area	500*500
Packet Size	1500 kb
Simulation Time	25 sec
Number of Nodes	17
Traffic Generation	UDP

Table 3.2: Simulation Details.

### 3.3 Creating Cluster topology

We created cluster topology. We create four groups of four nodes. Node no 3 is the source and 5,15 is the main node. Node no 4,6,9,16 are supporting node to help with file transferring and node no 12 is the destination node.

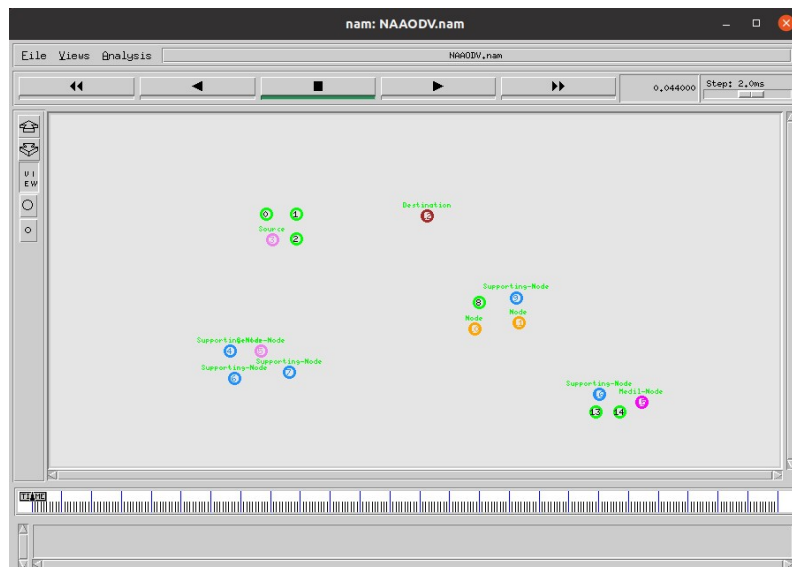


Figure 3.1: Creating Cluster topology

### 3.4 Implementing Black Hole Attack

After creating the cluster topology we implemented a black hole attack. In this simulation we show a black hole attack by two TCL files, one is without an attacker and another is with the attacker.

### 3.5 Simulation File

We complete the simulation with two types of files. Both files are prepared with proper source code. The source code is written in "C" language. During simulation, files are run in Network Simulator but on the back side C program completes the whole process. We make two TCL files one is without an attacker and another with the attacker. Without

the attacker file named NAAODV.tcl and with the attacker file named AODV.tcl. After completing the simulation each file made two files. With attacker files are AODV.nam & AODV.tr without attacker files are NAAODV.nam & NAAODV.tr. A simulation file table is given for understanding file types.

Types of Simulation	File Name
With Attacker Main file	AODV.tcl
With Attacker AniMator file	AODV.nam
With Attacker Trace file	AODV.tr
Without Attacker Main file	NAAODV.tcl
Without Attacker AniMator file	NAAODV.nam
Without Attacker Trace file	NAAODV.tr

Table 3.3: Simulation Files Types

## 3.6 Simulation Without Attacker

### 3.6.1 Normal Position of Nodes

In the figure, nodes are standing side by side. There are 17 nodes. Node 3 is the source node and node 12 is the destination node.

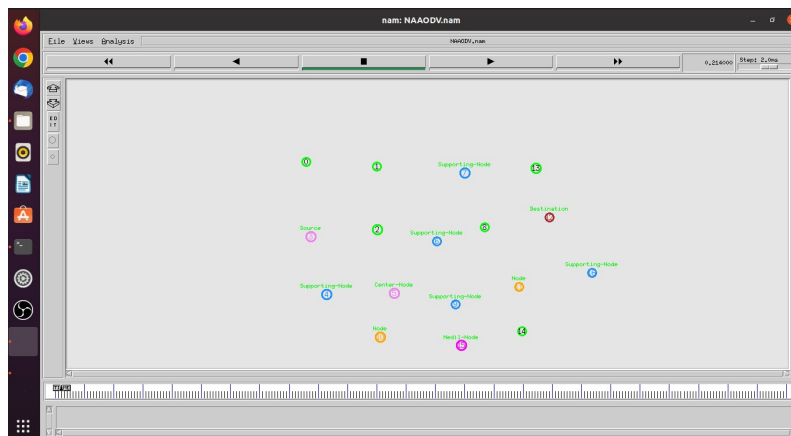


Figure 3.2: Normal Position of Nodes Without Attacker

### 3.6.2 Packet Sending

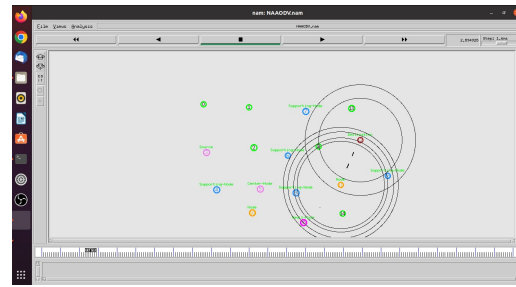
So the transferring route is from 3 to 4,5,6,7,9,10,15,16 to 12. There is no block or packet drop. Send and replay is ok.

### 3.6.3 Status Without Attacker

In the status figure, there is no error or packet drop in transferring data or packets.



(a) From Source



(b) To Destination

Figure 3.3: Packet Sending Without Attacker

```

ovejite@fireonbd:~/Desktop/AODV File$ ns NAAODV.tcl
num_nodes is set 17
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
  
```

Figure 3.4: Status Without Attacker

### 3.7 Simulation With Attacker

#### 3.7.1 Normal Position of Nodes

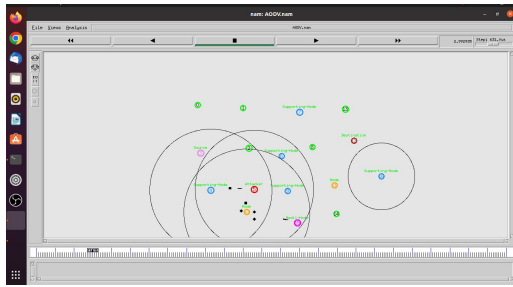
In the figure, nodes are sitting side by side. There are 17 nodes. Node 3 is the source node and node 12 is the destination node. Previously node 5 was a normal and transferring node but now we make it an attacker node. After node 5 is attacker node declined there is some change of route.[18]



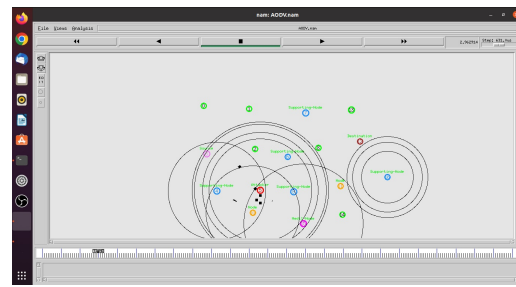
Figure 3.5: Normal Position of Nodes With Attacker

#### 3.7.2 Packet Sending

In the previous, the transferring route is from 3 to 4,5,6,7,9,10,15,16 to 12. There is no block or packet drop. Send and replay is ok. But when we make node 5 an attacker then route forwarder node 5 changes and node 4 is assigned as a forwarder. Node 5 blocks all packets that trying to bypass node 5. Here is a fugue of packet sending...



(a) Packet Drop



(b) Packet Drop and Destination change

Figure 3.6: Packet Sending Block By Attacker

### 3.7.3 Block Or Drop By Attacker

As declared node 5 is an attacker node so node 5 block and drop the packet. In the figure, we can see the node 5 block and drooping packer during data transfer.

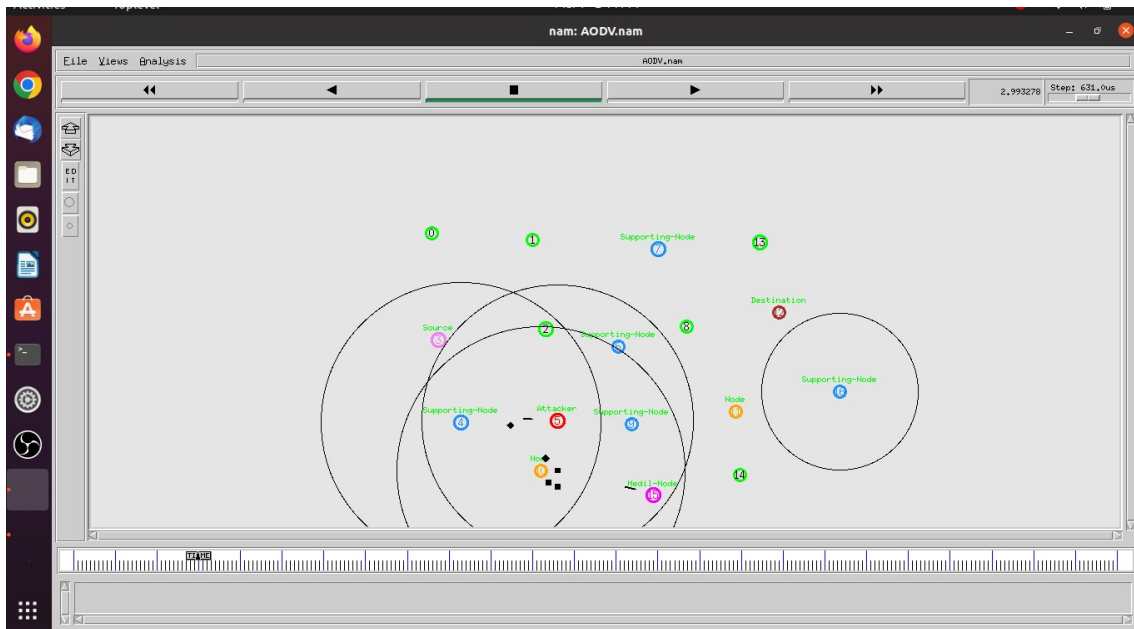


Figure 3.7: Data Blocking By Attacker

### 3.7.4 Status With Attacker

The status figure shows an error and packet drop in transferring data or packets. Node number 5 drop packer in data transferring time.

```
Starting a new one...
ovejite@fireonbd:~/Desktop/AODV File$ ns AODV.tcl
num_nodes is set 17
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
Packets dropped by node number5 is 0
Packets dropped by node number5 is 1
Packets dropped by node number5 is 2
Packets dropped by node number5 is 3
Packets dropped by node number5 is 4
Packets dropped by node number5 is 5
Packets dropped by node number5 is 6
Packets dropped by node number5 is 7
Packets dropped by node number5 is 8
Packets dropped by node number5 is 9
Packets dropped by node number5 is 10
Packets dropped by node number5 is 11
Packets dropped by node number5 is 12
Packets dropped by node number5 is 13
Packets dropped by node number5 is 14
ovejite@fireonbd:~/Desktop/AODV File$ Missing required flag -x in: W -t 25.0
```

Figure 3.8: Status With Attacker

# Chapter 4

## Analysis

### 4.1 Result Analysis

After completing the simulation let's analyze the output result file which is NAAODV.tr & AODV.tr file. We will analyze 12 different options. NAAODV.tr & AODV.tr both files will be checked by this analysis, and the output result of both will be given by screenshots.[19]

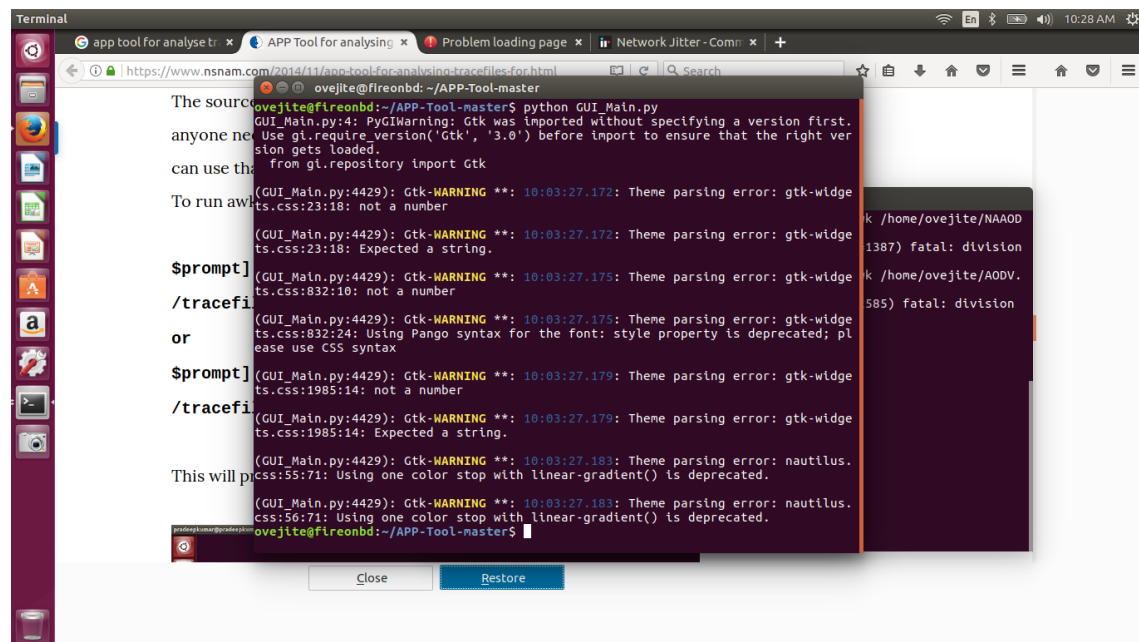


Figure 4.1: Result Analysis

### 4.2 Analysis Methods

Let's analyze NAAODV.tr & AODV.tr file with proper image. We will analyze the result in 12 methods. A table of methods is given below

#### 4.2.1 Average throughput

Using throughput to measure network speed is good for troubleshooting because it can root out the exact cause of a slow network and alert administrators to problems specifically

Method Number	Name of Methods
01	Average throughput
02	Instantaneous throughput
03	Average Delay
04	Instantaneous delay
05	Average goodput
06	Instantaneous goodput
07	Average jitter
08	Instantaneous jitter
09	Average Residual Energy
10	Residual Energy for a particular node
11	Packet Delivery Ratio
12	Normalised Routing Load

Table 4.1: Analysis Methods

in regard to packet loss. Packet loss, and latency are all related to slow throughput speed.[20]

```

NAODV-Average throughput
~/Desktop/File
--Average throughput--
    startTime: 1
    stopTime: 22
    receivedPkts: 524
    avgTput[kbps]: 162.1
-----|

```

(a) Average throughput Without Attacker

```

AODV-Average throughput
~/Desktop/File
--Average throughput--
    startTime: 1
    stopTime: 23
    receivedPkts: 27
    avgTput[kbps]: 9.47541
-----|

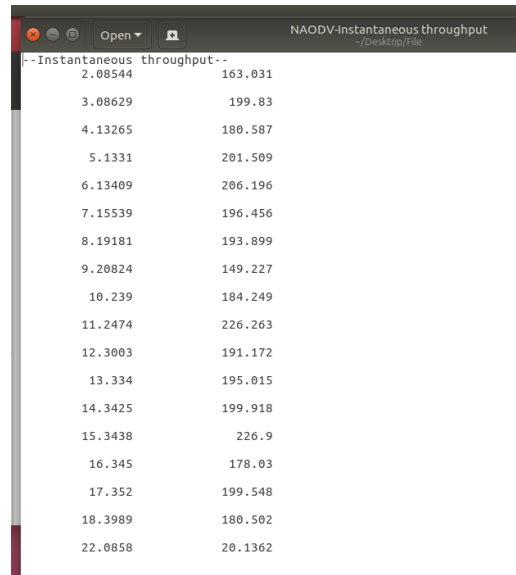
```

(b) Average throughput With Attacker

Figure 4.2: Analysis of Average throughput

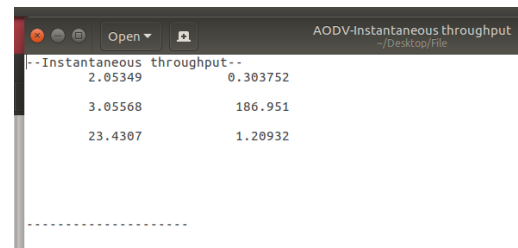
## 4.2.2 Instantaneous throughput

The number of bits per second actually transmitted through a network is the network throughput. the number seconds used for the measurement is significant: if the measurement is taken over a very short time interval, we are measuring the instantaneous throughput.



```
NAODV-Instantaneous throughput
~/Desktop/File
|--Instantaneous throughput--
2.08544      163.031
3.08629      199.83
4.13265      180.587
5.1331       201.509
6.13409      206.196
7.15539      196.456
8.19181      193.899
9.20824      149.227
10.239       184.249
11.2474      226.263
12.3003      191.172
13.334       195.015
14.3425      199.918
15.3438      226.9
16.345       178.03
17.352       199.548
18.3989      180.502
22.0858      20.1362
```

(a) Instantaneous throughput Without Attacker



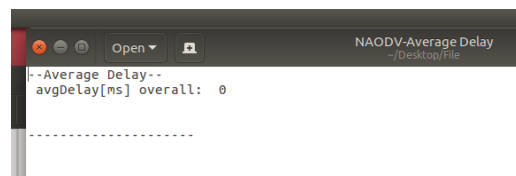
```
AODV-Instantaneous throughput
~/Desktop/File
|--Instantaneous throughput--
2.05349      0.303752
3.05568      186.951
23.4307      1.20932
```

(b) Instantaneous throughput With Attacker

Figure 4.3: Analysis of Instantaneous throughput

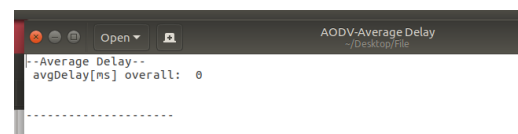
## 4.2.3 Average Delay

The average delay any given packet is likely to experience is given by the formula. The average rate at which packets are arriving to be serviced. This formula can be used when no packets are dropped from the queue.[21]



```
NAODV-Average Delay
~/Desktop/File
|--Average Delay--
avgDelay[ms] overall: 0
```

(a) Average Delay Without Attacker



```
AODV-Average Delay
~/Desktop/File
|--Average Delay--
avgDelay[ms] overall: 0
```

(b) Average Delay With Attacker

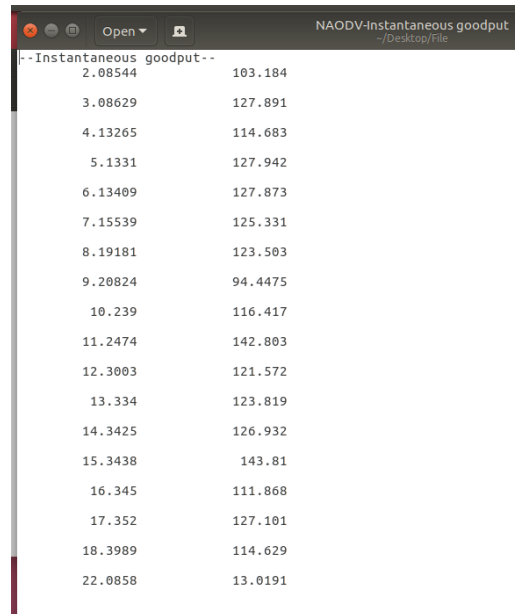
Figure 4.4: Analysis of Average Delay





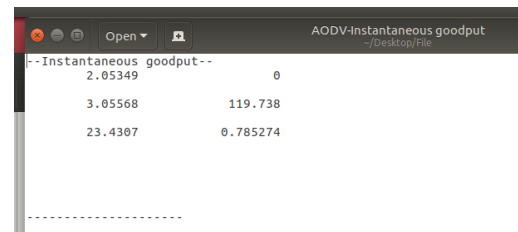
## 4.2.6 Instantaneous goodput

The goodput is a ratio between the delivered amount of information and the total delivery time. This delivery time includes Inter-packet time gaps caused by packet generation processing time instantly.



```
NAODV-Instantaneous goodput
~/Desktop/File
|--Instantaneous goodput--
2.08544      103.184
3.08629      127.891
4.13265      114.683
5.1331       127.942
6.13409      127.873
7.15539      125.331
8.19181      123.503
9.20824      94.4475
10.239       116.417
11.2474      142.803
12.3003      121.572
13.334       123.819
14.3425      126.932
15.3438      143.81
16.345       111.868
17.352       127.101
18.3989      114.629
22.0858      13.0191
```

(a) Instantaneous goodput Without Attacker



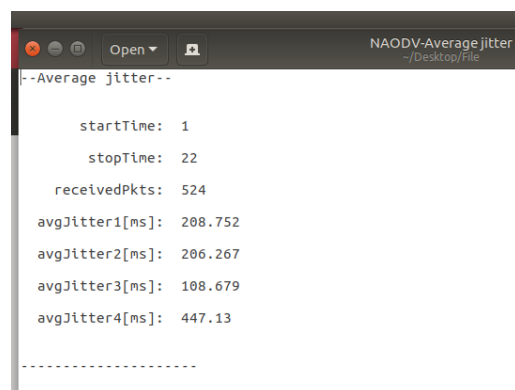
```
AODV-Instantaneous goodput
~/Desktop/File
|--Instantaneous goodput--
2.05349      0
3.05568      119.738
23.4307      0.785274
```

(b) Instantaneous goodput With Attacker

Figure 4.7: Analysis of Instantaneous goodput

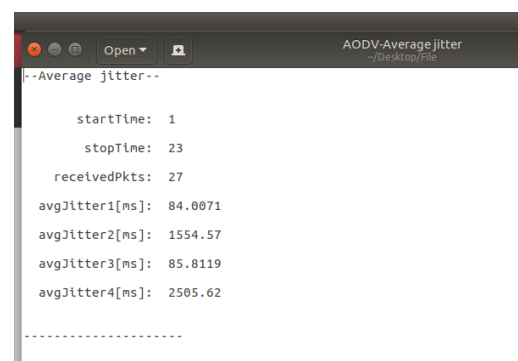
## 4.2.7 Average jitter

Jitter is the variation in the time delay between when a signal is transmitted and when it's received over a network connection, measuring the variability in ping. This is often caused by a network error, poor hardware performance and not implementing packet prioritization.



```
NAODV-Average jitter
~/Desktop/File
|--Average jitter--
  startTime: 1
  stopTime: 22
  receivedPkts: 524
  avgJitter1[ms]: 208.752
  avgJitter2[ms]: 206.267
  avgJitter3[ms]: 108.679
  avgJitter4[ms]: 447.13
```

(a) Average jitter Without Attacker



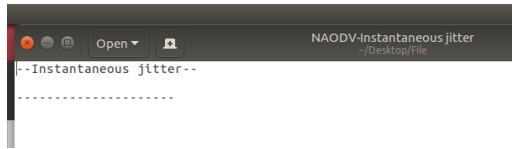
```
AODV-Average jitter
~/Desktop/File
|--Average jitter--
  startTime: 1
  stopTime: 23
  receivedPkts: 27
  avgJitter1[ms]: 84.0071
  avgJitter2[ms]: 1554.57
  avgJitter3[ms]: 85.8119
  avgJitter4[ms]: 2505.62
```

(b) Average jitter With Attacker

Figure 4.8: Analysis of Average jitter

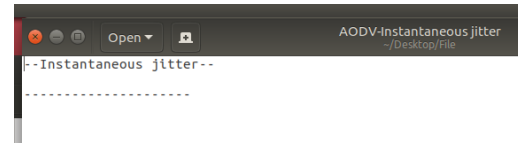
### 4.2.8 Instantaneous jitter

Information is transported from your computer in data packets across the internet. They are usually sent at regular intervals and take a set amount of time. Jitter is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and sometimes route changes.



```
NAODV-Instantaneous jitter
~/Desktop/File
--Instantaneous jitter--
-----
```

(a) Instantaneous jitter Without Attacker



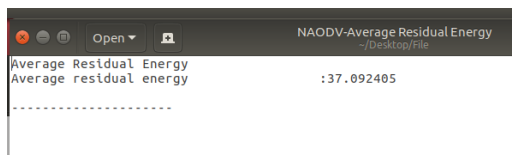
```
AODV-Instantaneous jitter
~/Desktop/File
--Instantaneous jitter--
-----
```

(b) Instantaneous jitter With Attacker

Figure 4.9: Analysis of Instantaneous jitter

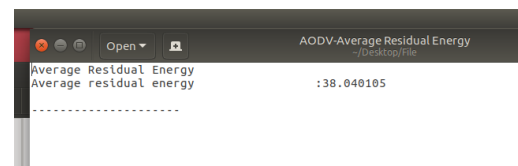
### 4.2.9 Average Residual Energy

In wireless sensor networks (WSNs), energy-constrained sensor nodes are always deployed in hazardous and inaccessible environments, making energy management a key problem for network design. The mechanism of RNTA (redundant node transmission agents) lacks an updating mechanism for the redundant nodes, causing an unbalanced energy distribution among them.



```
NAODV-Average Residual Energy
~/Desktop/File
Average Residual Energy
Average residual energy      :37.092405
-----
```

(a) Average Residual Energy Without Attacker



```
AODV-Average Residual Energy
~/Desktop/File
Average Residual Energy
Average residual energy      :38.040105
-----
```

(b) Average Residual Energy With Attacker

Figure 4.10: Analysis of Average Residual Energy

### 4.2.10 Residual Energy for particular node

A node loses a particular amount of energy for every packet transmitted and every packet received. As a result, the value of inertial energy in a node gets decreased. The current value of energy in a node after receiving or transmitting routing packets is the residual energy.

```

NAODV-Residual Energy for particular node
Residual Energy for particular node
Residual energy of node 3 is : 34.460066
-----

```

(a) Energy for particular node Without Attacker

```

AODV-Residual Energy for particular node
Residual Energy for particular node
Residual energy of node 5 is : 35.805751
-----

```

(b) Energy for particular node With Attacker

Figure 4.11: Analysis of Residual Energy for particular node

### 4.2.11 Packet Delivery Ratio

The packet delivery ratio (PDR) can be measured as the ratio of the number of packets delivered in total to the total number of packets sent from the source node to the destination node in the network. It is desired that a maximum number of data packets has to be reached the destination.[22]

```

NAODV-Packet Delivery Ratio
Packet Delivery Ratio
GeneratedPackets = 403
ReceivedPackets = 524
Packet Delivery Ratio = 130.025
Total Dropped Packets = 0
-----

```

(a) Packet Delivery Ratio Without Attacker

```

AODV-Packet Delivery Ratio
Packet Delivery Ratio
GeneratedPackets = 759
ReceivedPackets = 27
Packet Delivery Ratio = 3.55731
Total Dropped Packets = 0
-----

```

(b) Packet Delivery Ratio With Attacker

Figure 4.12: Analysis of Packet Delivery Ratio

### 4.2.12 Normalised Routing Load

The normalized routing load (NRL) it is the ratio of all routing control packets sent by all nodes to the number of received data packets at the destination nodes.[23]

```

NAODV-Normalised Routing Load
Normalised Routing Load
awk: /home/ovejite/APP-Tool-master/Final/nrm_rt_ld.awk:16: (FILENAME=/home/ovejite/NAODV.tr
FNR=167798) fatal: dlviston by zero attempted
-----

```

(a) Normalised Routing Load Without Attacker

```

AODV-Normalised Routing Load
Normalised Routing Load
awk: /home/ovejite/APP-Tool-master/Final/nrm_rt_ld.awk:16: (FILENAME=/home/ovejite/AODV.tr
FNR=14546) fatal: dlviston by zero attempted
-----

```

(b) Normalised Routing Load With Attacker

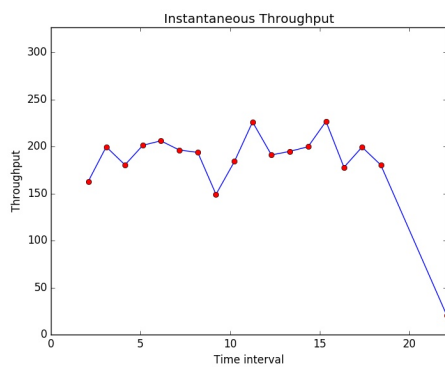
Figure 4.13: Analysis of Normalised Routing Load

# Chapter 5

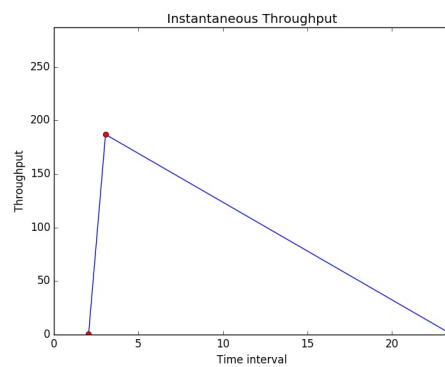
## Discussion

Before discussion let's see some analysis graph

### 5.1 Graph of Instantaneous throughput



(a) Instantaneous throughput graph without Attacker



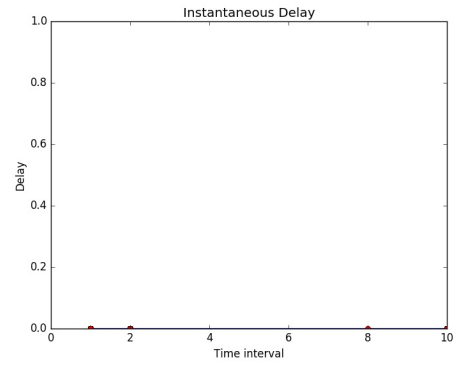
(b) Instantaneous throughput graph With Attacker

Figure 5.1: Graph of Instantaneous throughput

## 5.2 Graph of Instantaneous delay



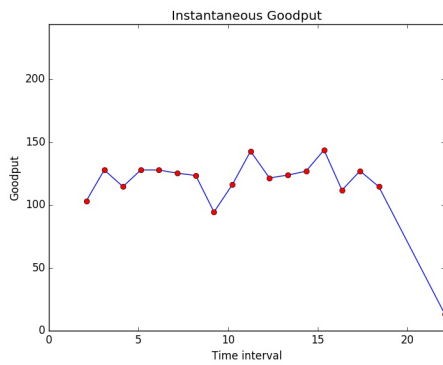
(a) Instantaneous delay graph Without Attacker



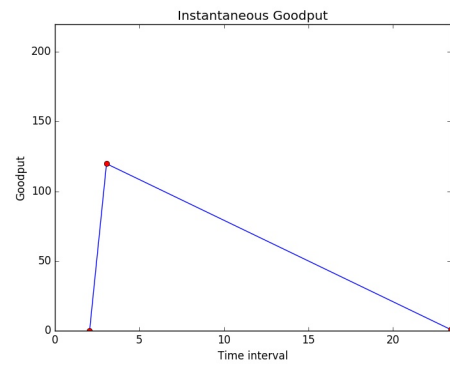
(b) Instantaneous delay graph With Attacker

Figure 5.2: Graph of Instantaneous delay

## 5.3 Graph of Instantaneous goodput



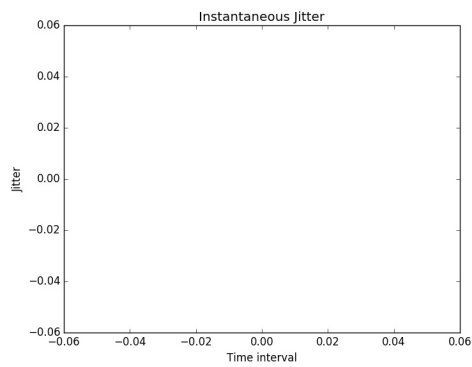
(a) Instantaneous goodput graph Without Attacker



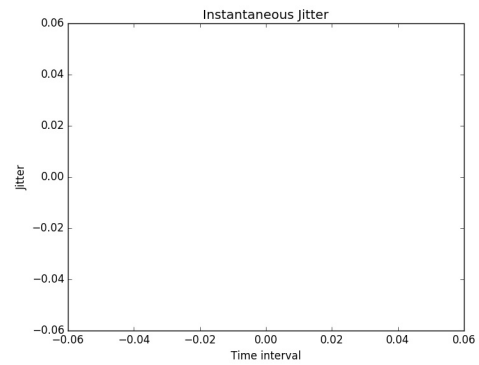
(b) Instantaneous goodput graph With Attacker

Figure 5.3: Graph of Instantaneous goodput

## 5.4 Graph of Instantaneous jitter



(a) Instantaneous jitter graph Without Attacker



(b) Instantaneous jitter graph With Attacker

Figure 5.4: Graph of Instantaneous jitter

After showing all the graphs we can decide when attackers attack nodes then package loss, energy waste, and make a lot of delays happen. The network jitter rate is always low on the wireless network so in the jitter graph nothing to show.

# Chapter 6

## Discussions

Our goal was to determine the protocol that has a low vulnerability for black hole attacks taking AODV routing protocols. Three performance parameters delay, throughput, and network load are taken. Our aim was to study the effect of black holes on AODV by analyzing how much the performance of a network has been compromised.

Considering the delay of a whole network in mind the performance in the presence of a single black hole node is analyzed. Similarly, performance parameters i.e. throughput and network load show to the extent that network performance has been affected by the presence of a black hole node.

As in the Black Hole attack, there is no need for RREQs and RREPs. So in the presence of a malicious node (attack scenario), the delay has been reduced. This is because when the sender node sends its RREQ, the malicious node is ready, and that node lies in between the path of the sender and the receiver actually receives the request earlier than the destination. So the malicious node sends its RREP to the sender node before the reception of RREQ from the actual receiver. Hence the malicious node establishes a direct link with the sender node. Now all the data sent through this malicious node never reaches the actual receiver causing the black hole effect. Also when both protocols are compared with each other in order to find the effect of the attack on both protocols AODV shows more delay. For throughput considering the low traffic (low load) of WSN, in the presence of a malicious node is comparatively low in comparison to ADOV because of its fewer routing forwarding and routing traffic. The malicious node discards the data rather than forwarding it to the destination, thus affecting and manipulating the throughput. The throughput in the case of AODV with the presence of a malicious node is comparatively higher than WMSNs. This is because of the packets discarded by the malicious node. The malicious node immediately sends its route reply and the data is sent to the malicious node which discards all the data. The network throughput is much lower.

In the case of network load, at high speeds, the routing protocols take much more time to adjust and afterward send traffic to the new routes. In case of a higher number of nodes, AODV reacts more quickly as compared to WMSNs, i.e. high network load for WMSNs which made the difference in network load much wider. As the node begins to pause and restarts its mobility after the starting period has more stability makes the network load more pronounced.

The black hole node discards the data which is routed to it. This means that the consequence of a black hole attack is packet loss of almost all the data sent from source to destination. After analyzing the vulnerability of both protocols i.e. AODV and WMSNs in terms of low network traffic and high network traffic, results show that AODV is more affected by the black hole node. This level of delay affected is about 2 to 5 percent while in WMSNs



is about 5 to 10 percent. The delay of AODV in normal networks is much higher than the delay in black hole attack which has been explained in our results chapter 6. The throughput of AODV is affected twice as compared to WMSNs. In the case of network load, however, there is effect on AODV by the malicious node is less as compared to WMSNs.

# Chapter 7

## Conclusion

We defined it before that wireless multimedia sensor networks (WMSNs) could be present. As multimedia data is larger than scalar data, that's why we need Wireless Multimedia Sensor Networks (WMSNs). Since the data sink attack is detected only after the black hole attack, we used the black hole attack to find that type of sink.[24]

From the above Result analysis, it can be seen that the performance of the network was affected greatly by the Black Hole Attack. Among the different positions of the attacker, it has been found that the performance of the network becomes worse when the attacker takes the position in the middle of the network.[25]

To prevent this type of attack on wireless mesh networks must be sure to use a better quality network device and security system. Otherwise, it's not possible to prevent it.[26]It must be noted, that not only a Black Hole attack but also another attack will happen there. Our main target is understanding the type of protocol used, data type, and node type with positions.

This research will help to detect protocol types, data sink types, and the black hole attack in WSN prospective researchers. Therefore, much research needs to be done on how to mitigate the attacks in this popular topology of WSN.

At last, we can tell that, every node which has some signal that can be hacked. So no device or node is safe from hackers, it is only reduced by using a high-level network firewall device, security patch, and protection system. Our advice is, it's better to prevent hacking from trying to stop hacking.

# References

- [1] J. Vacca. *Network and System Security*. Elsevier Science, 2013. ISBN: 9780124166950.
- [2] Chethana R. M. Balaraju G. Suhas G. K. *Detection of Black Hole Attacks in Wireless Sensor Networks*. 120 High Road, East Finchley, London, N2 9ED, United Kingdom: LAP LAMBERT Academic Publishing, 2018.
- [3] Karishma Chugh, L Aboubaker, and Jonathan Loo. “Case study of a black hole attack on LoWPAN-RPL”. In: *Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012)*. Vol. 7. 2012, pp. 157–162.
- [4] Ila Kaushik and Nikhil Sharma. “Black hole attack and its security measure in wireless sensors networks”. In: *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario’s* (2020), pp. 401–416.
- [5] G Umashankar and P Jayaram. “A study on black hole attack in wireless sensor networks”. In: *International Journal of Advance Computing Technique and Applications (IJACTA) 5.1* (2017).
- [6] H. Al-Mutairi, H. Alqarni, and A. Alshehri. *Detecting Black Hole Attacks in Ad Hoc Networks: Security, Algorithm and Simulation in Vanet*. Lap Lambert Academic Publishing GmbH KG, 2015. ISBN: 9783659787294.
- [7] Y. Xiao, X. Shen, and D.Z. Du. *Wireless Network Security*. Signals and Communication Technology. Springer US, 2007. ISBN: 9780387331126.
- [8] C.W. Badenhop. *A Black Hole Attack Model for Reactive Ad-hoc Protocols*. Air Force Institute of Technology, 2012.
- [9] R. Shree and R.P. Pandey. *Security Advancement in ZRP Based Wireless Networks*. Lap Lambert Academic Publishing GmbH KG, 2014. ISBN: 9783659500411.
- [10] Rajesh Kumar Dhanaraj et al. “Black-Hole Attack Mitigation in Medical Sensor Networks Using the Enhanced Gravitational Search Algorithm.” In: *Int. J. Uncertain. Fuzziness Knowl. Based Syst.* 29.Suppl-2 (2021), pp. 297–315.
- [11] Mohammad Wazid et al. “Detection and prevention mechanism for blackhole attack in wireless sensor network”. In: *2013 International Conference on Communication and Signal Processing*. IEEE. 2013, pp. 576–581.
- [12] P.K. Singh et al. *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario’s*. Advances in Intelligent Systems and Computing. Springer International Publishing, 2020. ISBN: 9783030403058.
- [13] Deepak Sharma. *Black Hole Attack in Manet*. 94, Sector 6 Dwarka, Block RZ, Dwarka, New Delhi, Delhi 110075, India: Educreation Publishing, 2019.

- [14] Oluwatobi Ayodeji Akanbi Elahe Fazeldehkordi I.S. Dr. Amiri. *A Study of Black Hole Attack Solutions: On AODV Routing Protocol in MANET*. 800 Hingham St Rockland, Massachusetts 02370, US: Syngress, 2015.
- [15] A John Clement Sunder and A Shanmugam. “Jensen–Shannon divergence based independent component analysis to detect and prevent black hole attacks in healthcare WSN”. In: *Wireless Personal Communications* 107 (2019), pp. 1607–1623.
- [16] F. Poulsen. *The Black Hole in Isaiah: A Study of Exile as a Literary Theme*. Forschungen zum Alten Testament. Mohr Siebeck, 2019. ISBN: 9783161568626.
- [17] T.S.P. Kumar and M. Alamelu. *Modelling and Simulation of Fast Moving Ad-Hoc Networks (FANETs and VANETs)*. Advances in wireless technologies and telecommunication (AWTT) book series. IGI Global, 2022. ISBN: 9781668436103.
- [18] V.V. Das et al. *Information Processing and Management: International Conference on Recent Trends in Business Administration and Information Processing, BAIP 2010, Trivandrum, Kerala, India, March 26-27, 2010. Proceedings*. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2010. ISBN: 9783642122149.
- [19] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park. “Black hole attack in mobile ad hoc networks”. In: *Proceedings of the 42nd annual Southeast regional conference*. 2004, pp. 96–97.
- [20] R.A. Hamamreh. *Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks*. IntechOpen, 2018.
- [21] A. P and V. PALANISAMY. *Impact of Black Hole Attack on Multicast in Ad Hoc Network*. Lap Lambert Academic Publishing GmbH KG, 2011. ISBN: 9783844313758.
- [22] Mohammad Wazid et al. “Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network”. In: *2013 International Conference on Communication and Signal Processing*. 2013, pp. 576–581. DOI: 10.1109/icccsp.2013.6577120.
- [23] Umashankar Ghugar and Jayaram Pradhan. “A study on black hole attack in wireless sensor networks”. In: *IJACTA* 5.1 (2017), pp. 001–003.
- [24] Mehdi Medadian, Mohammad Hossein Yektaie, and Amir Masoud Rahmani. “Combat with Black hole attack in AODV routing protocol in MANET”. In: *2009 First Asian Himalayas International Conference on Internet*. IEEE. 2009, pp. 1–5.
- [25] K. Munjal, S. Verma, and N. Munjal. *Cooperative Black Hole Attack Detection by Modifying Aodv*. Lap Lambert Academic Publishing GmbH KG, 2012. ISBN: 9783659227202.
- [26] Jaydip Sen. “Security and privacy issues in wireless mesh networks: A survey”. In: *Wireless networks and security: issues, challenges and research trends* (2013), pp. 189–272.