Air journal of Artificial Intelligence

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

INVESTIGATION OF BLACK HOLE ATTACKS IN WIRELESS SENSOR NETWORKS

Syed Muhammed Nouman Qadir

Lecturer (Pakistan Navy School of Logistics)

noman_qadir@yahoo.com

Keywords
Wireless sensor network
WSNs attack
Blackhole Attack
Performance-oriented attack
WSNs security
Active attack

Article History
Received: 10 October 2025
Accepted: 15 December 2025
Published: 31 December 2025

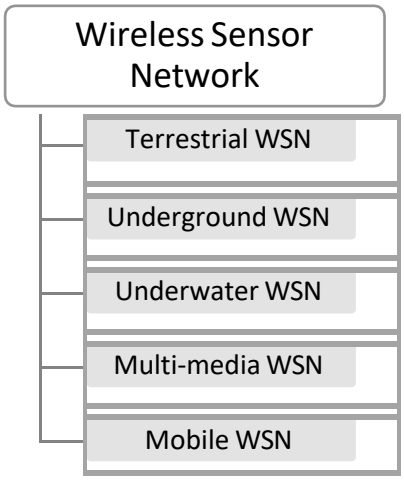
Corresponding Author: *
Syed Muhammad Nouman Qadir

Abstract
As sensor technologies advance, various types of sensors are widely deployed to form networks such as MANETs, WBANs, and VANETs–categories of Wireless Sensor Networks (WSNs). These sensors collect and transmit data to head nodes or base stations, often facing numerous security threats, both active and passive. This paper focuses on performance-oriented, layer-oriented, and goal-oriented attacks, analyzing their impact and exploring corresponding countermeasures. Special attention is given to the investigation, detection, and prevention of black hole attacks in WSNs.

INTRODUCTION

Wireless Sensor Network (WSN) is a network of different sensors that have different characteristics (sensing humidity, sensing temperature, and sensing fire, etc.) and limitations (low energy, low processing power, low coverage, and limited memory). WSN is a low-cost and effective solution which is why it is gaining popularity in communicating and turning your traditional environment into SMART Environments, but some challenges to designing in WSN will be defined in the next section. Due to the lack of infrastructure, limitations of resources, and Continuous changes in topology, Wireless sensor networks face security threats at every time. Both active and passive attacks are creating big trouble for WSN systems.

Figure 1: Types of WSN



1.1 Types of Wireless Sensor Networks

Wireless Sensor Networks can be categorized into five different types terrestrial WSN, Underwater

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

WSN, Underground WSN, multi-media WSN, and mobile WSN.

a) Terrestrial Wireless Sensor Network is denoted by TWSN, for the creation of TWSN you need a large number of inexpensive Sensor Node. A single TWSN might include hundreds to thousands of sensor nodes. This type of WSN can be built by two different strategies first one is pre-planned deployment in which you have to pre-plan deployment of a sensor node by a variety of options such as grid placement of sensor node, optimal placement of sensor nodes, 2-D and 3-D Placement of the model. On the other hand, there is an ad-hoc deployment of the sensor node in which the sensor node can be set up randomly in the target region/ area this type of deployment can be achieved by dropping the sensor node through a plane or helicopter because it is difficult to arrive that place where sensor node is required.

b) Underwater Wireless Sensor Network is denoted by UWSN, this type of network can be built to monitor underground situations in which possibility to place multiple sensor nodes underground, in a cave, or a mine. There is also the deployment of a Sensor node above ground to transmit information from the sensor node to the base station. This type of network requires expensive equipment the deployment of this network also increases the expense as compared to a terrestrial Wireless Sensor Network Also, UWSN requires expensive maintenance.

c) Underwater Wireless Sensor Network in which nodes are to be placed under the water, extremely few sensor nodes need to be set up in comparison to Terrestrial WSN and the cost of underwater sensor nodes is significantly higher, because underwater communication can be established by acoustic waves.

d) Mobile Wireless Sensor Network is denoted by MWSN, this type of sensor network in which several sensor nodes can move according to the requirements from one place to another place they also interact with the physical environments. MWSN Has all available that is available in a static node such as sensing capabilities, computing, and communication. MWSN has abilities to adjust its placement and arrangement inside the network under the specifications. Static WSN node can be used for static fixed routing and flooding and the other end in MWSN uses dynamic routing for transmitting packets from source to destination.

1.2 Characteristics of Sensor Node

There are Multiple characteristics of wireless sensor nodes are available some of them are described below.

a) Energy Efficient: Energy is the major resource for sensing nodes it must be utilized efficiently, recharging the node is impossible so your system must be as energy-efficient as possible.

b) Low Cost: A Wireless Sensor Network is the collection of multiple sensor nodes maybe a hundred or thousand so expensive node selections are increasing the WSN whole network cost, so it is better to choose the cheapest sensor node to reduce the overall cost of the network.

c) Distributed Sensing: In a Wireless Sensor Network there is a collection of different sensors so each node can send and keep data so distributed sensing provides a robust Network.

d) Wireless: In a Wireless sensor network, the sensor nodes need to be wireless since numerous applications necessitate collecting data without relying on the infrastructure of a physical medium like a cable. Thus, sensor nodes utilize wireless connectivity to communicate.

e) Multi-Hop: Due to the deployment of a large number of sensor nodes in WSN, one of the sensor nodes is required as the intermediate node to communicate with sink and base stations it must through a multi-hop route with the help of a routing path.

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

1.3. Challenges of Wireless Sensor Network

There are the following design challenges are available in different papers by different research scholars.

a) Scalable and Flexible Architecture: After creating WSNs there is flexibility to add further nodes as per requirement for generating more signals or removing dump nodes through WSNs.

b) Unreliable Communication: WSN is a network without medium means (wire) so it will broadcast the packets into the environments that is why the packet drop rate will be high so it is said that this is unreliable communication.

c) Fault Tolerance: The sensor has low energy so if any node not working properly then the routing protocol should automatically convert that responsibility to another node.

d) Limited Memory and Processing: Sensors having less memory and processing higher memory and processing capability are in higher demand in the market.

e) Heterogeneity Support Wireless sensor networks support different types of sensors so all of them are different protocols and WSNs all work together, therefore, it is also a big challenge for all.

f) Cost: The coverage area of wireless sensor networks is very low that's why we have to use multiple sensors for a single task which directly increases the cost of WSNs.

g) Data Aggregation: We use multiple sensors in the wireless sensor network so data transmission to the head node/ receiver may be redundant.

1. Related Work

In this paper [1] Author suggested a trust-based optimal reporting system is explained in this section, with particular attention paid to important components like the Group Member Nodes (GMNs) and Group Leader Nodes (GLNs), as well as the Trustor, Trustee, and Recommenders. It takes energy, selflessness, honesty, dishonesty, and similarity into account and uses both direct and indirect trust judgments. Lastly, we go over the Delta- Based Isolation Strategy, explain how it assesses if a particular trustee's trust value is declining, and examine the consequences for cost optimization and root node overhead reduction in trust management. In [10] researchers proposed a levels intrusion detection model (WSN-NSA) to detect the intrusion attack with the utilization of low memory consumption and computational time cost also the researchers successfully reduced the high detection accuracy.

In this paper [11] researchers achieved a high detection accuracy of 100% and no additional equipment is required, in this paper author Proposed an energy-preserving method to detect the wormhole attack in a wireless sensor network, and Mr. Al-Ahmadi's use of AODV routing protocol for simulating and analysing the result. This method is applied for all sensor nodes having two stages first one is to elect a path for transmission and the second stage is for protocol checking. This method is also efficient in terms of energy, throughput, PDR, and end-to-end delay.

In [12] researchers mainly focus on flooding and Greyhole attacks and proposed effective intrusion detection schemes Energy based on WSN. The author implemented lightweight energy prediction algorithms for observing the abnormality of the nodes' behaviour. By the author the prediction accuracy obtained is quite high therefore the detection accuracy is also achieved. This Scheme also increases the detection ratio and isolates the intruders from the network so it is energy efficient also their proposed scheme enhances the Network lifetime.

In this paper [13] Mr. Parmar Amisha introduces the new concept of self-protocol Trustiness (SPT) in which detecting a Blackhole intruder. In this paper author introduces a new mechanism called "Blackhole resisting mechanism (BRM)" and this mechanism BRM incorporates with any routing protocols that have reactive behaviour. This mechanism does not require the cryptographic technique therefore no power and computational requirements. Also, there is no need for additional packets generated so this mechanism is also efficient
from an overhead perspective. His Simulation result showed that BRM-AODV has the greatest improvements over the normal AODV and SAODV. In this paper

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

author [14] Sayed Mohammad Hossein Mirshahjafari especially focuses on a Hybrid Attack (combination of the sinkhole and CloneID attack) these attacks have a more negative/destructive impact on network performance. In this research, the author proposed detecting algorithms to detect the Sink-Clone attack. According to his observation True, the Positive Detection Rate is constantly increasing from time to time.

In this paper [15] Author works on passive attackers like (sniffers, Man-in-the-middle, and eavesdropping), especially in the military field, and proposes an algorithm called "LISA" with Steiner Minimal Tree (SMT) algorithm for providing security of data. This Algorithm provides both integrity and confidentiality to data by using the shortest routing path. In this research, the author achieved a successfully better result of almost 1:1.8 ratio and this result is continuously increased by increasing the number of nodes in terms of PDR, Energy Efficiency, and routing overhead.

In [16] Authors work on data authenticity and reliability of data delivery in IoT-based applications against DOS Attacks by designing an efficient scheme called SelGOR. According to the Author's literature, the existing authentication schemes found that they are failed to operate for opportunistic routing due to high computational cost or are un-serviceable in WSN. SelGOR holds a maximum Packet delivery Ratio with low computational cost and in low Wireless links.

In this paper [17] author works to detect the Sybil attack in IWSN and proposes the MKEM Scheme. Their simulation shows that the MKEM Scheme may detect malicious packets delivered by Sybil attackers, eliminating the necessity for a pre-labeled library of channel features for all sensor node SNs. MKEM Scheme also obtained great detection accuracy despite the presence of noise and interferences that are common in industrial contexts. MKEM system still assures detection accuracy when sensor nodes (SNs) adaptively adjust their transmission power or grow their number. In this paper, the author compares the MKEM Scheme with (PGDS, Simple K-Means, and Multi-kernel) and successfully received the highest accuracy by monitoring the Accuracy Parameter FNR (False-negative Rate) and FPR (False Positive Rate) and evaluating the result for Transmission power and Number of the sensor node.

In this paper [18] Author works for replication attacks because this attack is responsible for generating different types of attacks to reduce the performance of the network. According to this paper, the author recommended TBCND, when the cloned node communicates in the network TBCND detects this clone node. There are two phases to this TBCND technique the first phase is responsible for deploying the sensor node to create the network by using node-ID and this deployment is in the form of a special tree structure BST Node-id is the key of the BST First stage/ phase. After that, the second phase is responsible to detect the replication node and revoke the replica node from the network. In the paper, the author uses the NS-2 Simulator to evaluate the performance of the proposed method (TBCND) by four-parameter PDR, end-to-end delay, packet loss, and residual energy. In this observation, the author observes the result for three scenarios the network assault is generated by the first clone node while, second No attack in the network, and the third, and last is only the Clone node is present in the network and this clone node not generating the attack in the network. The author reduces the communicational cost and memory cost by comparing their result with RAWL, TRAWL, RAND, RM, LSM, and SDC methods therefore author declares the statements that the due to "proposed method the network is not affected by the cloned node".

2.1 Blackhole Mitigation Technique Other Scholar Technique

a) Fake Packets Acknowledgement: [2] In this method, the Author first creates a leader node and this leader node is responsible for identifying the Blackhole node. According to this method after generating a route request RREQ (route request) sets 20ms as expiration time. If the leader node receives RREP (Route Reply) within the pre-set intervals of time (20ms) then the leader node sends fake packets

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

and waits for the acknowledgment of fake packets if acknowledgment of fake packet is received then the original data is sent If acknowledgment of fake packets is not received leader node set some threshold value (10) for the comparison of packets Loss if Packet loss is greater than the threshold value (10) then the leader node broadcast a message to network that specific node ID is a malicious node and if RREP (route reply) is not received by a specified time (20ms) then the leader node resends the route request RREQ (route request).

b) MAC algorithm based: In this paper [3] Author "Proposed MAC algorithm based black hole attack avoidance technique", One cryptography method that is managed by a symmetric key is the MAC algorithm. Each function in this method can work with input data (messages) of varying sizes to produce output data with a predetermined length. Both the recipient and the authenticated sender share a secret key. This algorithm comes in three different varieties: block cipher-oriented MAC, stream cipher, and hash function. This algorithm's main benefit is data integrity. This algorithm's main concept is that the sender and the recipient will both produce MAC codes and compare them with one another using this shared secret key. The communication will not be accurately delivered if the sender's and recipient's MAC values do not match.

c) Two-Way Handshaking [4] In this research author uses two-way handshaking mechanisms. In this mechanism when the source node sends the RREQ (route request) Packets to the destination it will wait for RREQ_ACK to check whether it has a valid route or node. So every legitimate node firstly sends RREQ_ACK to the source node instead of the malicious node (Blackhole). Malicious nodes (Blackhole) are not aware of the actual mechanism of the algorithms therefore they directly send the RREP (route reply) packets to the sender node they do not send the RREQ_ACK (route request acknowledgment) Packets hence these RREP (route reply) Packets will help to sender to identifies and detect the malicious node (Blackhole) in the network.

d) Digital Signature [5] In this paper, the author uses a digital signature to identify the black hole in the network in which the author initially assigns a short signature to all nodes, if the digital signature is the routing update occurs otherwise routing updates are removed as well as inform to another node if they are not successfully verified the digital signature that node treated as black hole node. During the route discovery process, RREQ packets broadcast to all neighbor nodes, and this process continues until the destination is found. The RREQ packets header retains all records of the node visited by storing node ID into the header when the destination node receives this RREQ Packets it contains all node's IDs and the destination node unicast the reply against RREQ to every visiting node with adds its digital signature. When the receiving node validates the previous node's digital signature from its database, it considers the received packet to be authentic; if not, it considers the node to be an attacker node.

e) Timer Based [6] In this Paper Author proposed techniques consisting of Different steps to detect Blackhole nodes (Malicious nodes) in the Network. Firstly Source Node broadcasts a route request packet (RREQ) to its all neighbor in the network In the meantime source node starts a timer to check the timing of each route Reply Packet (RREP). Then the source node finds which node returns quickly in minimum time with an exceptionally high sequence number and puts this node into black list. Now this blacklist will be isolated from the network for isolating clustering technique used every node assigned rating and maximum trust value node will be selected as cluster head and the Cluster head will monitor all other network transmissions.

g) Baiting [7] in this Paper author proposed a technique to resist smart black-hole attacks. This technique depends on two phases first is Baiting and second one is non-neighbor Reply. In the first phase, each node is assigned a random bait timer (B second) when the node timer reaches B Second it broadcasts a randomly generated fake ID as a bath request. So, if any malicious (blackhole) node exists in the network it will respond to the randomly generated fake ID and claim that they have the best route into

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

their routing table to reach the destination that is mentioned in the randomly generated fake ID.
Now Source node receives the reply against fake packets it will immediately add this node to the black-hole list. The second phase is non-neighbor Reply in which each node has the ID of an adjacent node by sending a hello message broadcasting process. Whenever the source node receives a reply packet from the intermediate node, the source node checks the ID of the node with the shortest path if it is in the black-hole list then it discards the reply.

h) Cesar Cypher [8] In this Research Author slightly modifies the mechanism of AODV Protocols. The author adds the features of encryption and decryption in AODV protocols for detecting and reducing the effectiveness of malicious nodes (black holes). As we know there are a lot of cryptographic algorithm features available but in the research, the author implements the CESAR cipher with a pre-shared key of 3. As we study the working of CESAR cipher. CESAR cipher takes input in the form of plain text and then converts each character of plain text into ASCII value each ASCII value adding three means (65+3=38). Then each ASCII value is Converted into a Character. According to the author, every encryption and decryption can be implemented here if they use a symmetric key (Single key for encryption and the same key used for decryption). During the Route Discovery Process, the RREQ (route request) packets are firstly encrypted and then sent to the destination to find the route from source to destination. Every intermediate Node that is legitimate has the pre-shared key and that node can decrypt the RREQ (route request) Packets are also capable of sending Reply to the source Node through RREP (route reply). On the other hand, the Blackhole node cannot decrypt the RREQ (route request) Packets because it doesn't have the pre-shared key.

i) Algorithm-Based identification of Blackhole: In this paper [9] author suggests an algorithm for the authentication and identification of Black Hole nodes to protect the network's security and integrity and stop unwanted access. Malicious nodes can be effectively tracked by the algorithm, which also limits their network access.
The recommended algorithm for identifying Black Hole nodes is a crucial component in enhancing the network's security and integrity, aligning with the simulation scenario of entities being generated by nodes and our thorough investigation of IoT vulnerabilities reference. Thereafter, it systematically evaluates every node in the network by comparing it to the list of authentic nodes. A node is deemed possibly malicious and needs further investigation if there is any discrepancy in this comparison. As a watchful supervisor, the sink node routinely monitors the network's packet-forwarding activities to augment this monitoring. When the sink node finds nodes not fulfilling their forwarding duties, it quickly flags and removes them from the network.
Additionally, by dynamically altering the routing tables of nearby nodes and rerouting packets to avoid the identified malicious nodes, the strategy increases network resilience. The network receives a strong authentication mechanism that can quickly identify and neutralize Black Hole nodes by seamlessly integrating this technique, guaranteeing data integrity and safe transmission throughout the Internet of Things (IoT) network.

S. No.	Year	Their Work	Limitation	Our Solution	References
1.	2024	Proposed MAC algorithm based black hole attack avoidance technique.	Requires mathematical Calculation therefore it's require more computation resources.	We just assign node_ID therefore no additionally computational resources required	[3]

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

2.	2024	Proposed Trust-Based Optimized Reporting for Detection and Prevention of Black Hole Attacks in Low-Power and Lossy Green IoT Network	Multiple factors (energy, selflessness, honesty, dishonesty, similarity) and uses both direct and indirect trust judgments which can lead to increased processing requirements, especially in large networks	NO Trustor, Trustee, and Recommenders therefore our solution required less processing requirements	[1]
3.	2018	This technique depends on two phases first is Baiting and second one is non-neighbor Reply	This technique required the more time in baiting and the source node checks the ID of the node with the shortest path.	Our Techniques not require to check the Shortest path therefore comparatively less time required	[7]
4.	2024	Author suggests an algorithm for the authentication and identification of Black Hole nodes to protect the network's security and integrity and stop unwanted access	Continuously monitoring network activity, comparing nodes to an authentication list, and dynamically altering routing tables can introduce significant processing and memory overhead,	Our Proposed Solution not Continuously monitoring network activity, therefore no extra memory and processing requirements	[9]
5.	2021	The paper proposes a digital signature-based method to identify Black Hole nodes by assigning signatures to all nodes, verifying them during route discovery, and flagging nodes with invalid signatures as attackers.	Digital signature verification requires cryptographic operations, which may introduce processing delays, especially in resource-constrained networks like Wireless Sensor Networks (WSNs) and IoT devices.	Unlike some complex cryptographic or AI-based security mechanisms, the node_id verification method is lightweight and does not require intensive computations, making it suitable for resource-constrained WSNs.	[5]
6.	2015	The research enhances the AODV protocol by integrating encryption and decryption using the CESAR cipher with a pre-shared key to detect and prevent Black Hole attacks	The CESAR cipher is a basic substitution cipher that is highly vulnerable to brute force attacks, as there are only 25 possible shifts, making it easy for attackers to break the encryption.	NO cipher only the node_id verification method is lightweight and does not require intensive computations, making it suitable for resource-constrained WSN	[8]

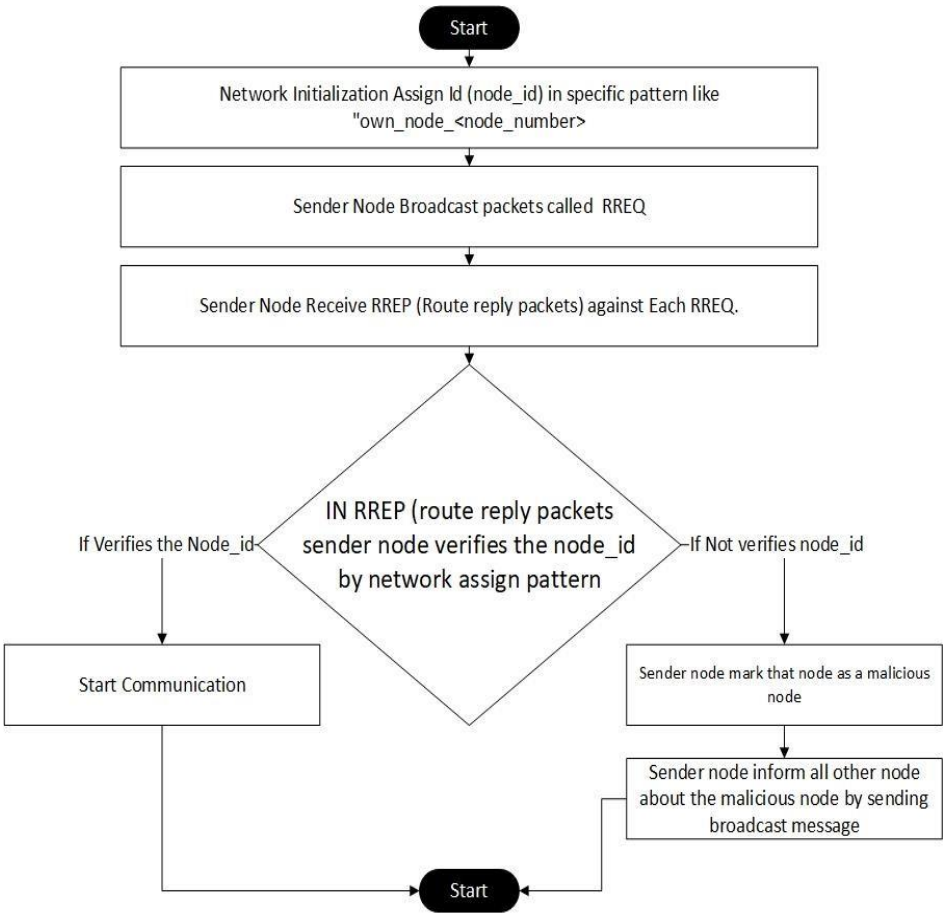
Proposed Blackhole Mitigation Techniques

In this study, we suggested a method for using the Node Identification Number, or node_id, to identify black hole nodes in WSNs wireless sensor networks. To do this, we defined a pattern that could be used to assign the node_id at any point during network establishment.

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

Node Number	Identification Number (Pattern)
1	own_node_1
2	own_node_2
3	own_node_3

Figure 2: Blackhole Mitigation Technique



After assigning a node identification number, the sender node broadcasts the RREQ Route Request packets and receives the RREP Route Reply Packets in response to each Route Request. Next, the sender node verifies the node identification number against the network's specific pattern. If the pattern is verified, the packets are accepted and communications begin. If the pattern is not verified, however, it indicates that some nodes outside of our network are sending the RREP packets, in which case our sender node will first reject the packets and broadcast a message to the network with the node_id identifying the malicious

node to alert all nodes of its presence. As a result, none of the network's nodes will react to the attacker.

Here are some positive aspects of the proposed method for identifying Black Hole nodes in Wireless Sensor Networks (WSNs) using **Node Identification Numbers (node_id):**

1. **Efficient Black Hole Node Detection** – The method quickly identifies malicious nodes by

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

verifying the node_id pattern, preventing unauthorized nodes from responding to Route Request (RREQ) packets.

2. **Early Prevention Mechanism** – Since the sender node verifies the node_id before communication begins, it stops Black Hole nodes from participating in the routing process, reducing potential security threats.
3. **Broadcast-Based Alert System** – Once a malicious node is detected, the sender node alerts the entire network, preventing other nodes from interacting with the attacker, which strengthens overall security.
4. **Low Computational Overhead** – Unlike some complex cryptographic or AI-based security mechanisms, the node_id verification method is lightweight and does not require intensive computations, making it suitable for resource-constrained WSNs.
5. **Minimal Energy Consumption** – The method does not rely on continuous monitoring or high-energy-consuming security mechanisms, helping to preserve the battery life of sensor nodes.
6. **Scalability and Flexibility** – The use of node_id patterns allows easy adaptation to different network sizes and configurations without requiring significant modifications.
7. **Fast Response to Attacks** – Since the sender node immediately rejects unverified packets and alerts the network, the system can respond to potential threats in real time, minimizing the impact of attacks.
8. **Enhanced Data Integrity and Security** – By ensuring that only authenticated nodes participate in communication, the method reduces the risk of data interception, manipulation, or loss due to malicious activities.

Limitation of Proposed Techniques

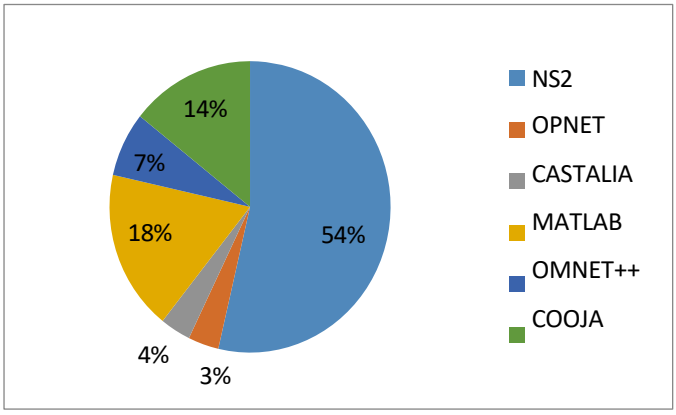
Our suggested technique has a drawback in that, should an attacker node intercept our packets and understand our network pattern, it will become a part of our network. However, because of time constraints, we can address this issue in the future.

2. Simulation

4.1 Selection of Simulator, Attack, and Network Performance Parameter

a) Reason for Selecting Network Simulator

Figure 3: Simulation Tools Comparison



For the Selection of the Simulator, I will analyze the 29 research scholars in the most recent year (from 2015 to 2024) and find that the maximum scholar Scholars who work for NS (Network Simulator) is approximately more than 50% of research scholars use NS (Network Simulator) that's why I am also selecting the NS (Network simulation) for simulating the Result.

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

b) Reason for selecting Blackhole

A blackhole attack is a dangerous attack and it affects for all over the network it drops the packets as welland generates false messages instead of sending correct/true Packets towards the base station in the wireless sensor network by capturing the node and reprogramed the set of the node in the network.

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

c) Reason for Network Performance Parameter

we found that the majority of scholars working on Resource Aggregation work on Routing Load/overhead only 3.4% work on Network Routing Load/ overhead, therefore, we selected this Parameter for my research Now we also select all parameters of Data Aggregation because when we analysed 29 research scholar in the most recent year (2015 to 2021) then I found Less working in Data Aggregation as compare to resource aggregation, therefore, we work for data aggregation we also found that every Research scholar works for Packets delivery and found 51.7% working on it, 41.4% working on End to End Delay and 31% works on Network Throughput and rest to this three-parameter I found that very fewer works done for remaining two-parameter such as

Fairness and jitter 0% and 6.9% respectively.

4.2 Simulation Setup

For performing the simulation, we need a Network simulator (NS-2.35) that works with both window and LINUX but this tool NS-2.35 works very smoothly and efficiently with LINUX-based operating systems, therefore, we use Ubuntu 18.2 (LINUX Distributer) furthermore tools are required that's description and version are mentioned in below table

Table 1: Hardware Configuration

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

4.3 Simulation Details

In this experiment, we standardized different parameters such as Routing protocol is AODV, Simulation area 1000mX1000m, and many more that are mentioned in the below table, this parameter is standardized in the .tcl file. When we compile this .tcl file in the NS-2.35 simulator we get two important files first one is in the .tr extension (trace file) and the second one is the. Nam extension (animator file), this .tr file is used by any .awk script (AWK is a scripting-based language that helps us to generate reports) to calculate different parameters such as (PDR, End to End Delay, throughput, network Routing load, and jitter).

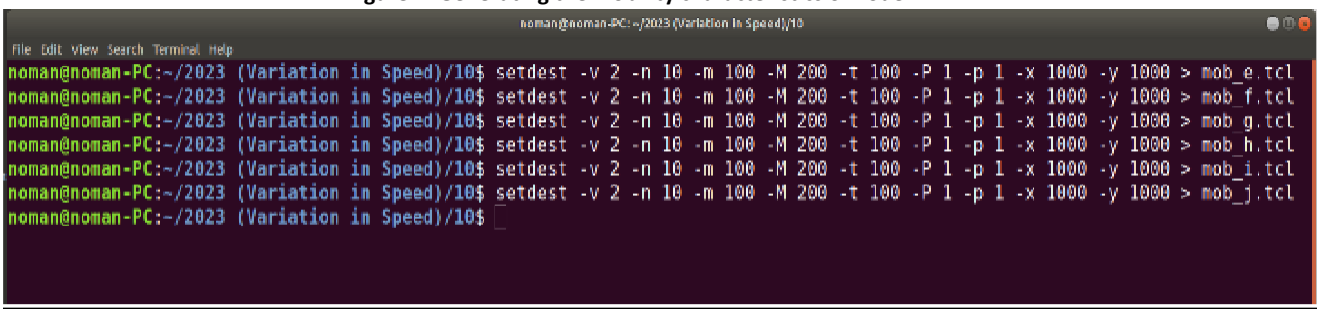
Table 2: Parameter Selection for Observations

Parameter	Details
Simulator	NS-2.35
Number of Nodes	10, 20, 50, 100, 200
Node Placement	Random
Number of Source Node	1
Number of Sink Node	1
Simulation Area	1000m X 1000m
Protocols	AODV
Traffic Type	CBR (constant bit rate)
Simulation Time	100 sec
Antenna Type	Omni Directional
Size of Packets	1500
MAC	802_11
interface queue type	Queue/ DropTail/ PriQueue

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

Connection Type	TCP
Application Used	FTP

Figure 4: Generating the mobility characteristics of node in



4.3 Node Mobility

To Enable the mobility characteristic of Node in WSN we need a setdest program setdest generates a file that contains the details of node movement using random waypoint algorithms. This program is automatically installed with the installation of NS-2.35, after the installation of NS-2.35 you can easily run this program. The saddest command may take some time to execute because it will generate a file and write some code in it and it depends upon the parameter that you pass to the command.

After creating the mobility file you can attach this mobility file with the .tcl script that you generate from NSG2 software. There are multiple switches of setdest command available some major are compiling in below mentioned.

Table 3: Setdest Command Switches

Switch	Description
-n	This switch is used to define the number of Nodes
-m	This switch is used for specifying the minimum node speed
-M	This switch is used for specifying the maximum Node Speed
-t	This switch is used to declare the timing/ duration of mobility
-x	This switch is used for defining simulation area in horizontal X-Axis
-y	This switch is used for defining simulation area in vertical Y-Axis
mob_a.tcl	It is the file name that is automatically created.

4.4 AWK Script

Manipulation of data and generation of reports is the core objective of any network and this task is accomplished with the help of any scripting language therefore in LINUX Architecture "Awk" is used. It is a scripting language and requires no compiling to allow users to use variable, athematic operations, logic, and text-based functions. Pattern matching and pattern processing are the most famous applications of Awk script.

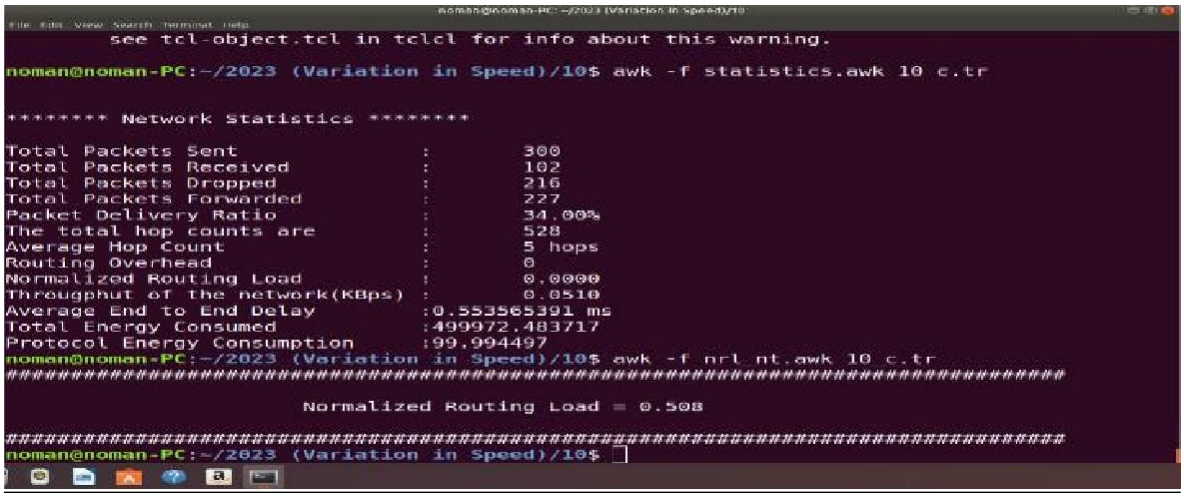
Awk Operations

1. Line-by-line file scanning.
2. Creating field by input splitting.
3. The input line compares with a specific pattern.
4. If compared successfully, perform actions.

Air journal of Artificial Intelligence

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

Figure 5: Awk Network Statistics observation



4.5 Creating topology

For observation, we create network topology of different sets of nodes in the form of a .tcl (Tool Command Language) script file with the help of the TCL script generator (NSG2) that is freely available on the internet but Java is the prerequisite for NSG2. It is a GUI GUI-based application that generates automatic both wire and wireless-based scenarios by providing a different set of parameters. From above mentioned script generator tool we generate 10 random samples of each topology.

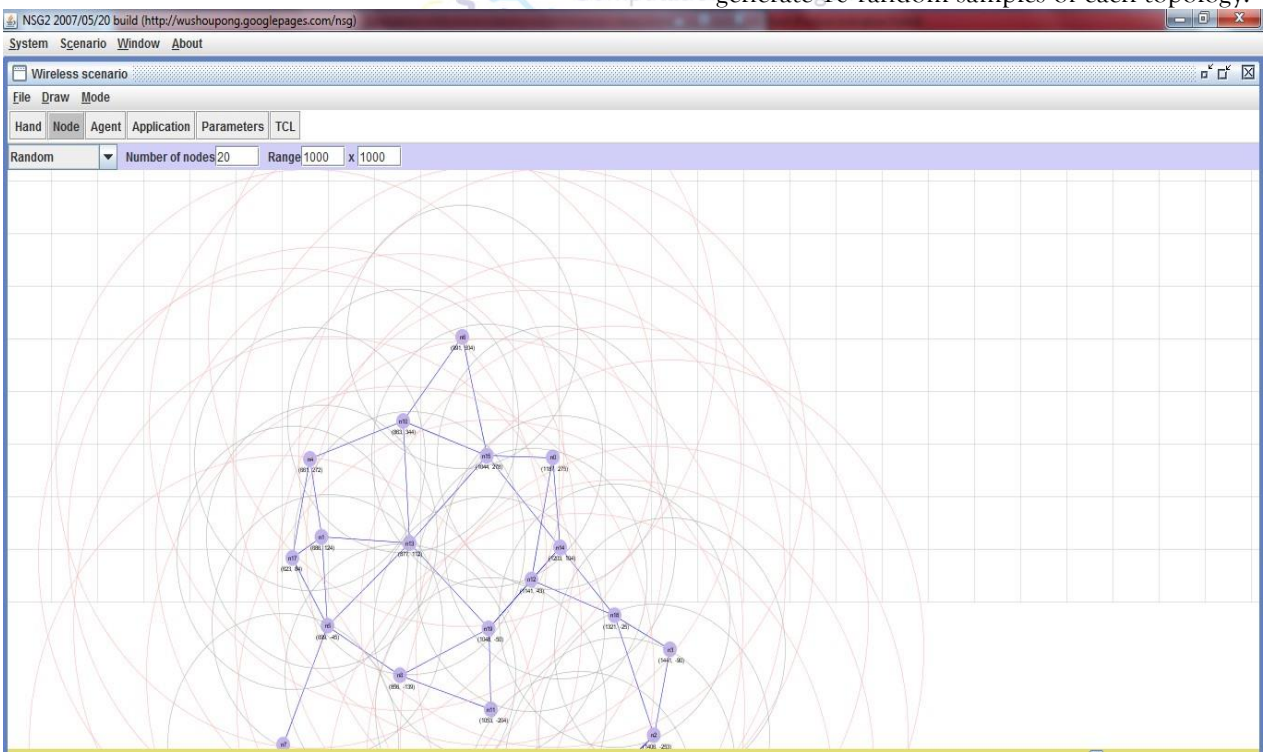


Figure 6: NS 2.35 Environment

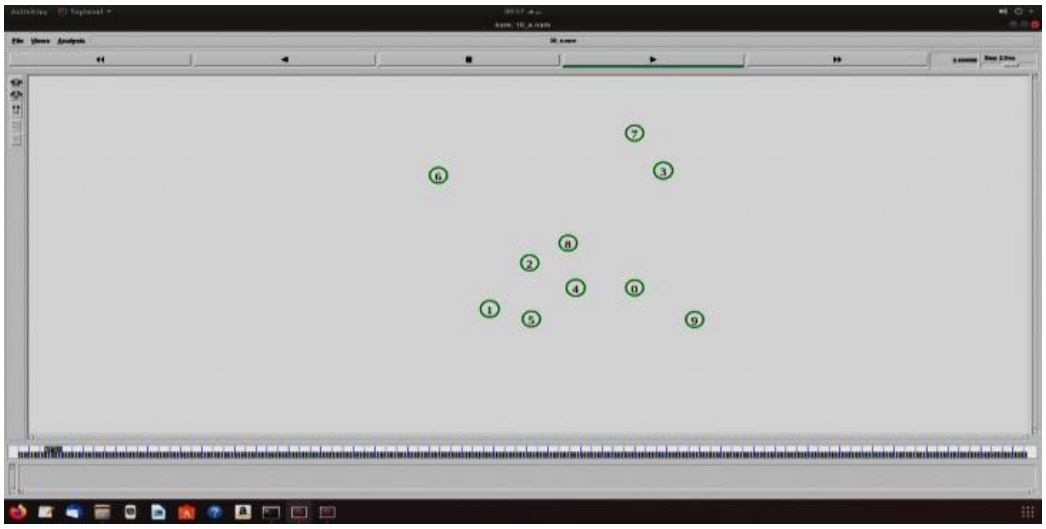
Air journal of Artificial Intelligence

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

By using a window-based machine we generate different sets of topologies with the help of the

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

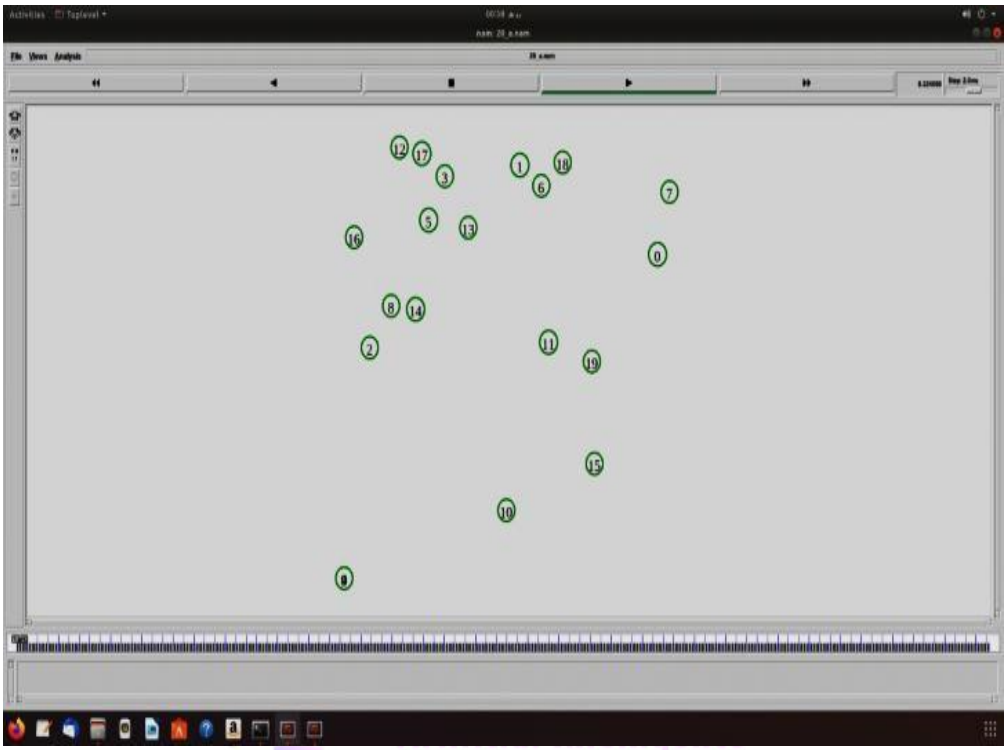
NSG2 Tool then we save our .tcl extension File and this .tcl file executes/runs in the NS2-2.35 simulator by the Following Commands.



a) Creating topology - 10 Node

Figure 7: 10 Nodes

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025



b) Creating topology - 20 Node

Figure 8: 20 Node topology

c) Creating topology - 50 Node

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

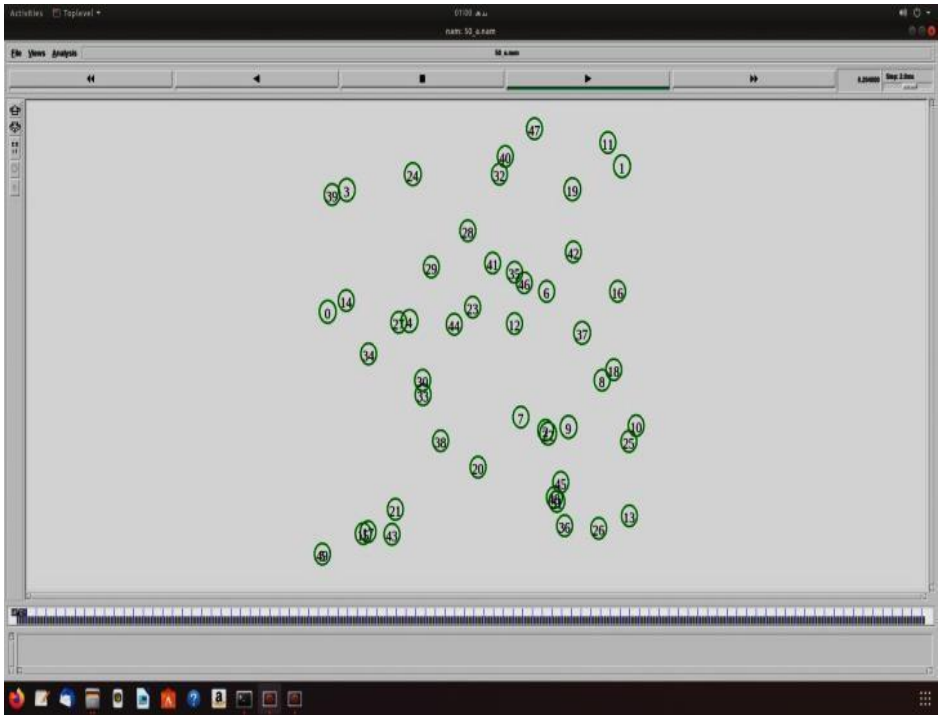


Figure 9: 50 Node topology

d) Creating topology - 100 Node

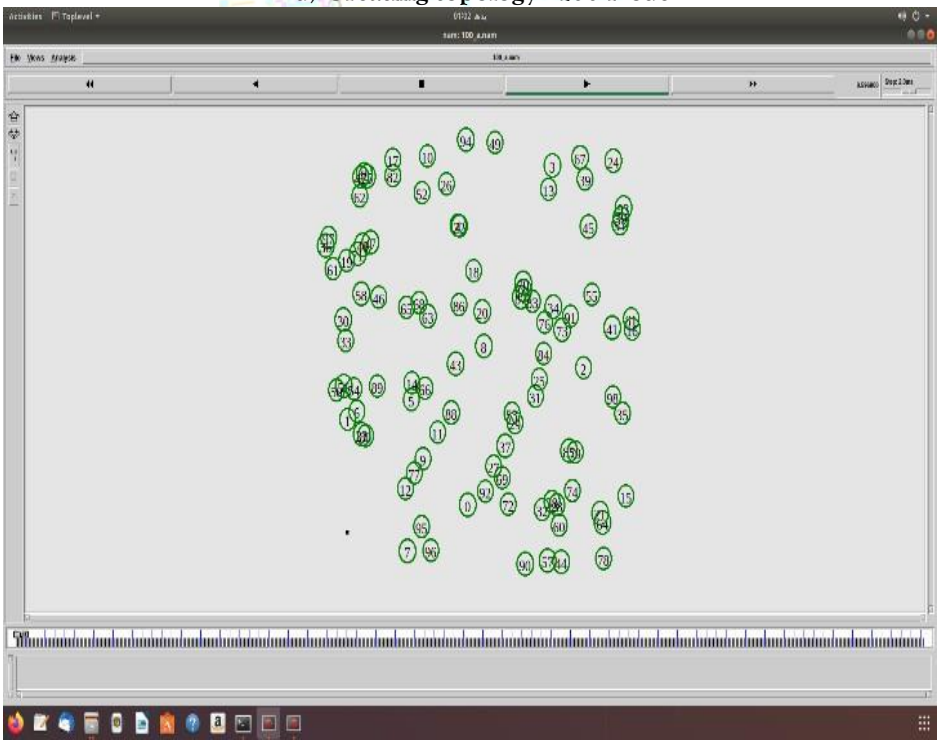


Figure 10: 100 Node Topology

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

e) Creating topology - 200 Node

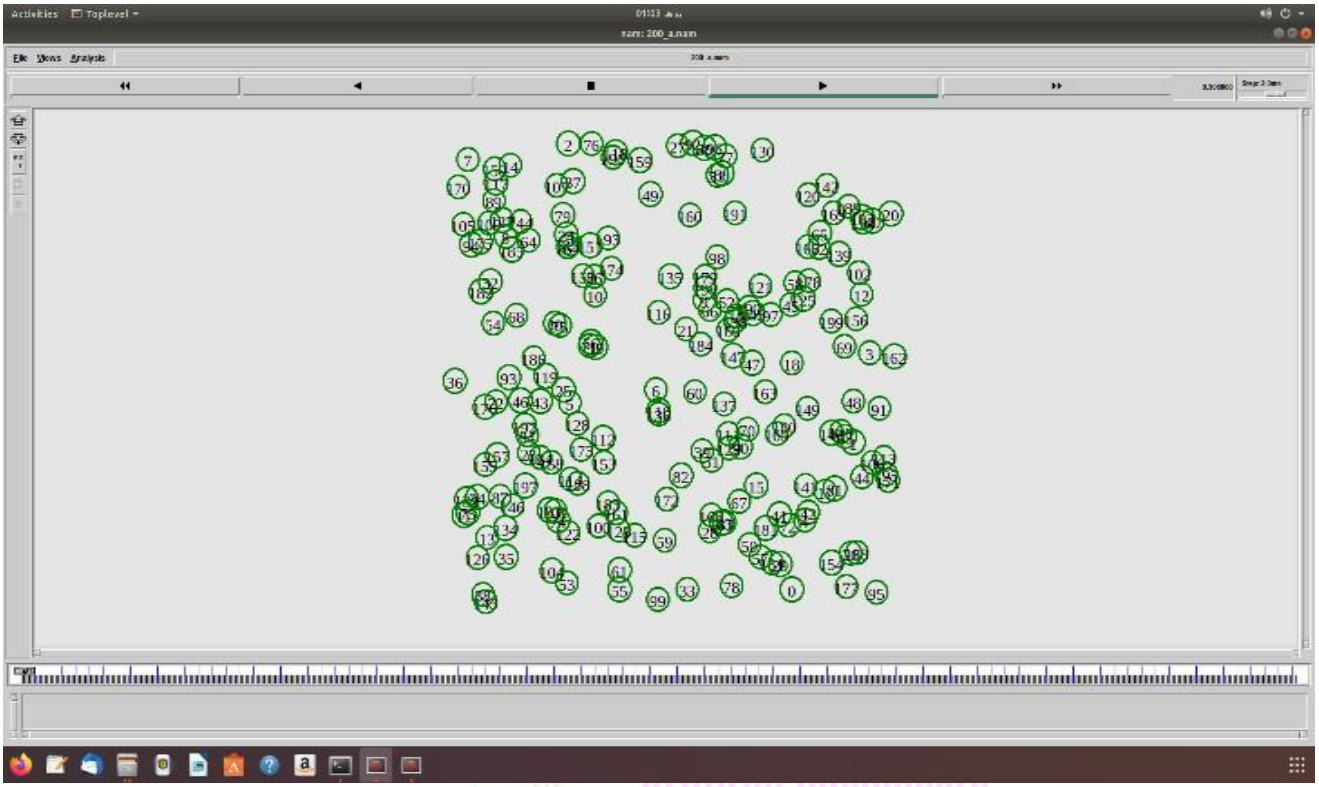
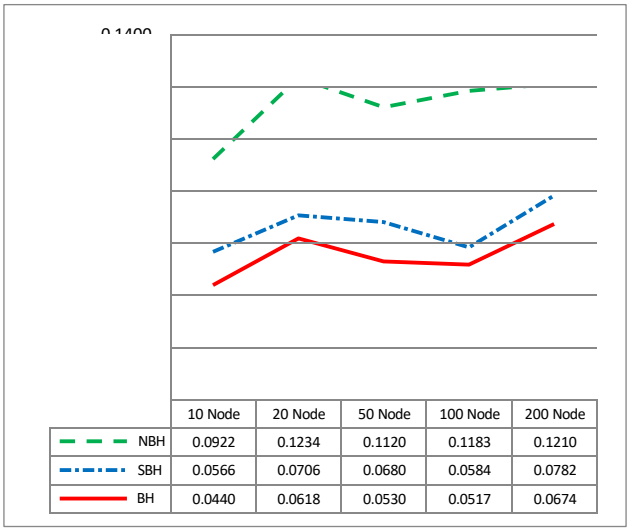


Figure 11: 200 Node Topology

3.



	10 Node	20 Node	50 Node	100 Node	200 Node
NBH	0.0922	0.1234	0.1120	0.1183	0.1210
SBH	0.0566	0.0706	0.0680	0.0584	0.0782
BH	0.0440	0.0618	0.0530	0.0517	0.0674

4. Experimental Observation

Before starting the observations, we first categorized the Performance Analyzer parameter into two different categories first one is data aggregation (Reliability) and the second is Resource Aggregation. In data aggregation, we consider four different parameters such as (End-to-end delay, packet delivery Ratio, Throughput, and jitter), and in Resource aggregation, we consider only one parameter (Network Routing Load).

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

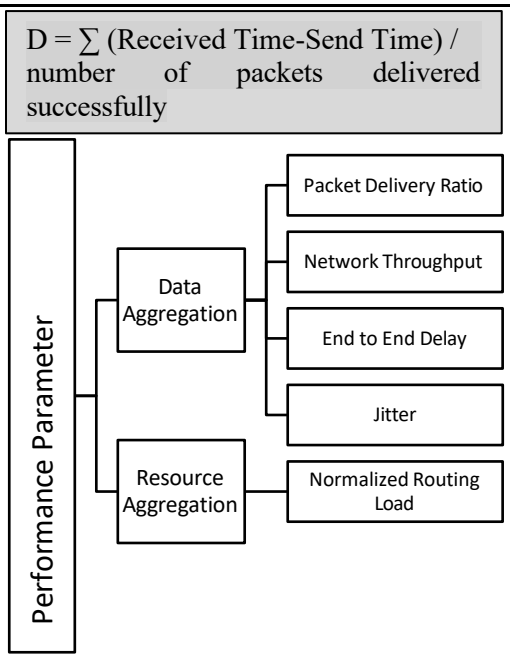


Figure 12: Performance Parameter

PDR = ∑ number of packets received / ∑ number of packets sent (packets drop + packets received)

5.1 Packet Delivery Ratio

The ratio of the successful packet received by the total sent from the Source node to the destination node is called A packet delivery Ratio (PDR).

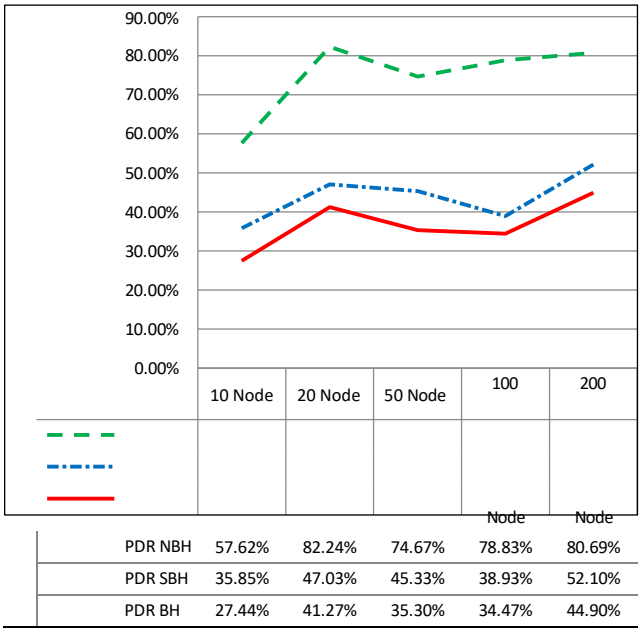


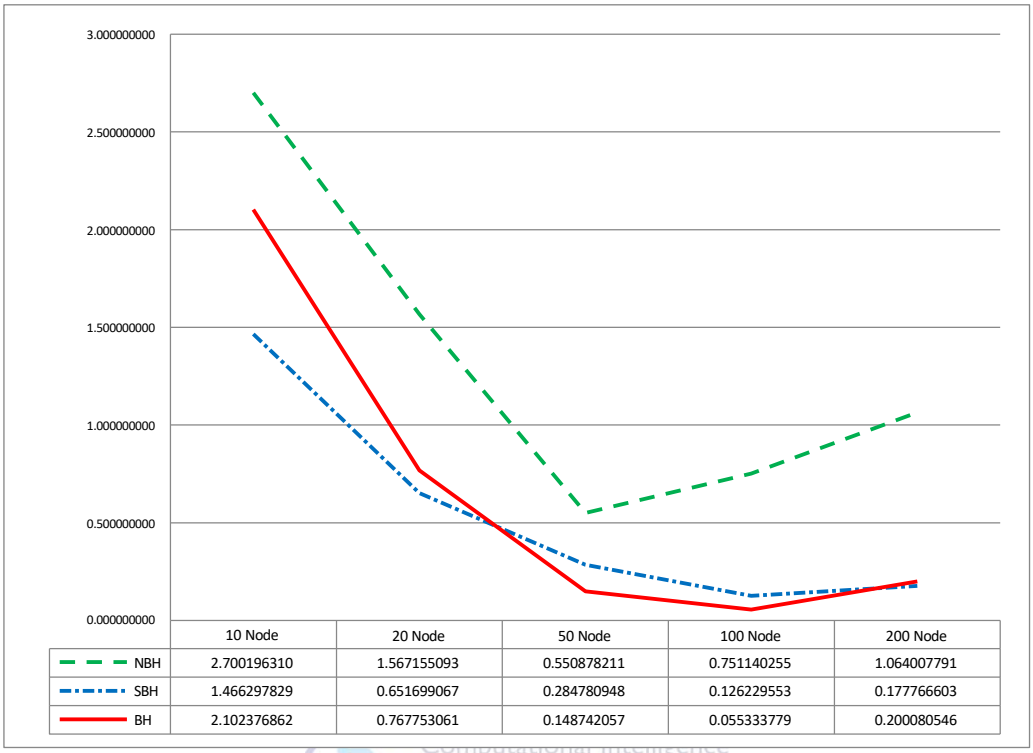
Figure 13: Packets Delivery Ratio Chart

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

5.2 Throughput

T = ∑number of bits received / Time

5.3 End-to-End Delay



	10 Node	20 Node	50 Node	100 Node	200 Node
NBH	2.700196310	1.567155093	0.550878211	0.751140255	1.064007791
SBH	1.466297829	0.651699067	0.284780948	0.126229553	0.177766603
BH	2.102376862	0.767753061	0.148742057	0.055333779	0.200080546

Figure 14: End To End Delay Chart

5.4 Jitter

Where packets are transmitted from the source node to the sink node then there is some delay and the variation of these delays is called jitter.

Figure 15: Jitter

Congestion

Congestion is defined as all packets coming to the junction for processing at the same time therefore nothing can get loaded

Packets Loss

Packed Loss is defined as the receiving computer not being able to process/ entertain the information when it arrives without/unexpected intervals

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

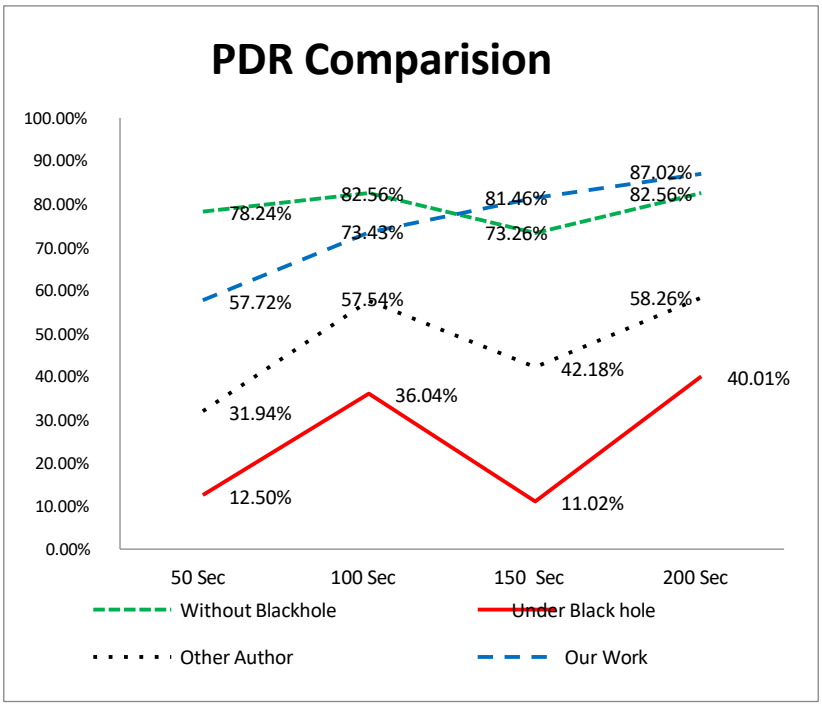
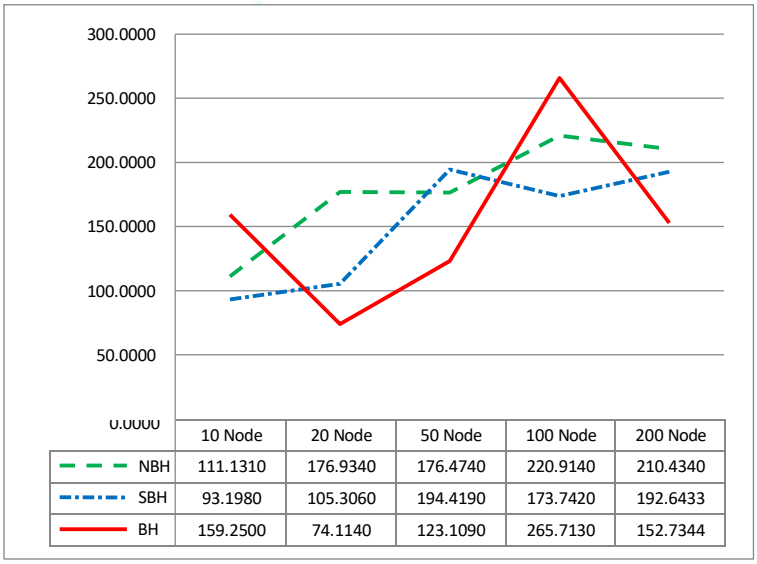


Figure 16: Jitter Current Chart



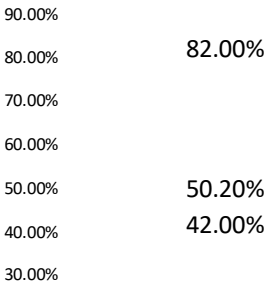
	10 Node	20 Node	50 Node	100 Node	200 Node
NBH	111.1310	176.9340	176.4740	220.9140	210.4340
SBH	93.1980	105.3060	194.4190	173.7420	192.6433
BH	159.2500	74.1140	123.1090	265.7130	152.7344

Figure 17: PDR Comparison in different time

5.5 Network Routing Load/ Overhead

Network routing overhead is the quantity of routing packets sent for maintenance and also for route discovery but as in MANET nodes are mobile selected paths for packet transmission might get interrupted [5]. This leads to rerouting of the path every time a node moves from its position.

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025



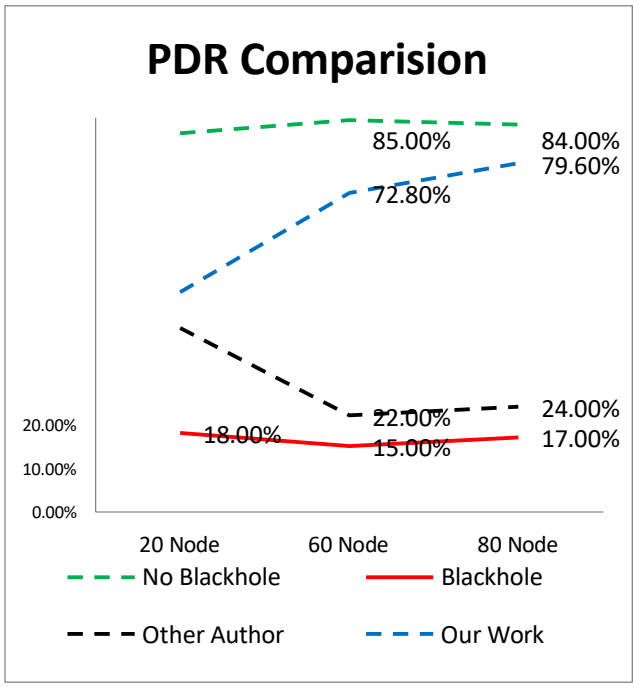
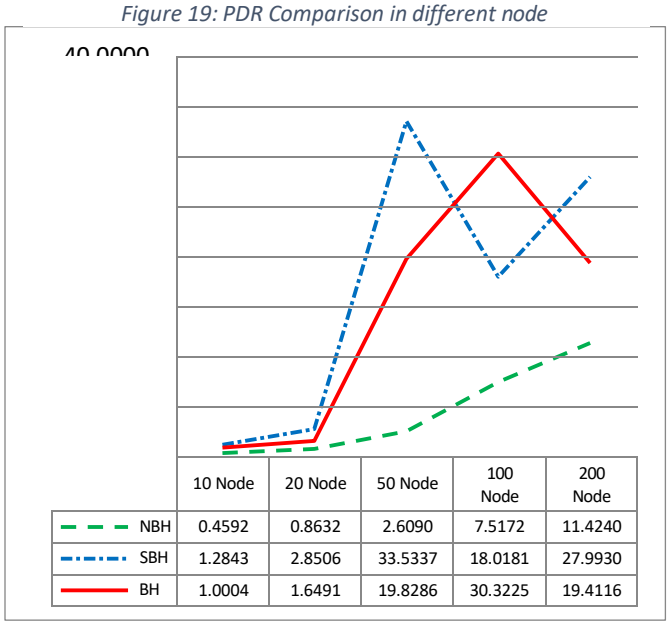


Figure 18: Network Routing Load Chart

Figure 19: PDR Comparison in different node



	10 Node	20 Node	50 Node	100 Node	200 Node
NBH	0.4592	0.8632	2.6090	7.5172	11.4240
SBH	1.2843	2.8506	33.5337	18.0181	27.9930
BH	1.0004	1.6491	19.8286	30.3225	19.4116

5.6 Comparison of our work with the work of other

Here, we evaluate our observations and those published in the report by Ahmed Ibrahim [29] on the variations in simulation times, such as (50 sec, 100 sec, 150 sec, and 200 sec). According to preliminary findings, our proposed techniques perform better than [29] in terms of improving the packet delivery ratio in wireless sensor networks with blackhole attacker nodes. This demonstrates how well our suggested remedy works to mitigate the effects of black hole attacks.

Here, we perform another evaluation between our observations and those published in the report [5]. According to preliminary findings, our proposed

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

techniques perform better than [5] in terms of improving the packet delivery ratio for a specific set of nodes (20 nodes, 40 nodes, and 80 nodes) in wireless sensor networks with blackhole attacker nodes. For this observation, our simulation time is 160 seconds and simulation are being 1100x750 and the mobility speed is 6 m/s.

5.6 Residual Energy

We are not working in Residual Energy for a solid justification that aligns with the scope of our research and the focus of our methodology. Below are some potential reasons for excluding residual energy from our investigation

Primary Focus on Security and Attack Mitigation:
The core aim of your research is to mitigate black hole attacks and enhance the reliability of Wireless Sensor Networks (WSNs) by identifying malicious nodes using Node Identification Numbers (node_id). Since black hole attacks primarily affect data transmission and routing, your research is focused on improving network security and communication integrity, rather than energy efficiency.

Energy Consumption Is Not Significantly Impacted by the Proposed Method
The proposed method focuses on node identification and verification of RREQ/RREP packets to reject malicious nodes. This mechanism adds some overhead due to the broadcasting and verification steps, but the impact on residual energy may not be significant enough to warrant inclusion.

Residual Energy Is Not Directly Affected by Node Behavior
The residual energy of nodes in a WSN is typically affected by factors such as data transmission frequency, distance between nodes, and network topology. In our case, the malicious behavior of black hole nodes (which drop or misdirect packets) does not directly cause increased energy consumption in other nodes, other than the overhead of rejecting and re-sending packets.
Since your proposed method is focused on detection and prevention of black hole attacks, energy consumption is secondary to the main objective of securing communication. Any energy consumption due to detection may be marginal compared to the overall benefit of reducing malicious interference.

Residual Energy Is a Secondary Concern in Attack Detection:
In many WSN security studies, especially those dealing with attacks like black hole attacks, energy consumption is often considered a secondary concern. The primary goal is to protect the network from malicious activities that compromise the integrity and reliability of communication. Once the attack mitigation techniques are validated, residual energy could be considered in future work as part of an overall network optimization strategy

5. Conclusion

In conclusion, the research conducted in this proposed thesis has delved into the critical issue of "disrupting the communication and reliability of sensor node" of black hole attacks from a list of issues i.e. compromised the data integrity, disrupt the communications, reliability of any sensor node and energy consumption in Wireless Sensor Networks (WSNs). The study has made clear how crucial it is to create strong security procedures to condense the dangers connected with black hole assaults. Additionally, this thesis offers a sophisticated understanding of black hole attacks in addition to making a substantial contribution to the body of information already available on WSN security. Through a wide-ranging examination of existing literature, analysis of attack scenarios, and the theoretical assessment of numerous defence mechanisms, we have gained valuable insights into the challenges associated with securing WSNs against black hole attacks. As we strive to enhance both Data Aggregation (PDR, network throughput, end-to-end delay, and jitter) and Resource aggregation (normalized Routing load).

6. Result and Discussion

Most importantly, we have shown that the Packet Delivery Ratio (PDR) with a black hole is 35.30% with a black hole but after the implementation of blackhole mitigation technique we increase it to 45.33%, and the throughput of the network with a

Air journal of Artificial Intelligence
ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

black hole is 0.0530 but after implementing proposed techniques it also increases to 0.0680 may be greatly increased by deploying proposed techniques specifically for wireless sensor networks. The enhancement of PDR and throughput makes a strong argument for the application of the suggested security measures in practical settings the findings of the experiments reported in this thesis demonstrate a favourable relationship between the implementation of strong security measures and an improvement in the network's data transmission efficiency and dependability. The work presented here lays a strong foundation for creating and putting into place strong countermeasures that will protect these vital networks' functionality and integrity. We can create the conditions for Wireless Sensor Networks to have a more secure and dependable future by working together and being innovative.

7. Future Work

Many different tests, experiments, and adaptions are left for future work due to limited time and resources such as (experiments in real data usually take a lot of time even take number of days to finish a single observation). Future research mainly focuses on in-depth analysis and examination of particular mechanisms; fresh suggestions also attempt to propose alternative methodologies in just simple curiosity. In the literature review we study there are numerous IDS proposed by our different scholars for specific blackhole detection and prevention, testing of these predefined IDS, and comparing with our techniques also in our future scope. There are a variety of future works accomplished in long-term and short-term plans some of them are elaborated on in the below sections.

a) While significant work has been accomplished in this research paper, we investigate the only blackhole attack in wireless sensor networks using AODV Routing protocols their description of simulation parameters and observation results are explained in Chapter 5 and Chapter 6 respectively, and also provide its mitigation techniques in chapter 7. Observation results work fine and show some improvements with AODV Routing protocols which means our solution is routing protocols (AODV) dependent as well as attack-dependent (blackhole). So therefore, in the future, we propose a hybrid solution that is not Routing Protocol dependent It works for all routing protocols such as (AODV, DSDV, and DSR) as well as our future hybrid solution is not Attack Dependent it works similarly not for all but at least some famous active attacks like (Blackhole, Wormhole, Sybil attack, sinkhole and hello flood attack).

b) In the future engineering stage, we also increase the number of blackhole nodes instead of single blackhole nodes we use groups of blackhole nodes in different sizes of networks and observe their effectiveness in different network performance parameters (PDR, network throughput, end-to-end delay, Normalized routing load, and jitter also). This paper mainly focuses on single blackhole attacker nodes in different sizes of networks therefore this is also a suggestion for future works.

c) As we know energy is the major resource for any sensing node therefore, we are responsible for caring about its utilization efficiently, because recharging is not an easy task for any wireless node, so your system must be as energy-efficient as possible. In this thesis, we proposed our techniques for evaluating the (PDR, end-to-end delay, network throughput, and jitter), but not considering the energy consumption of any wireless sensor nodes in wireless sensor network WSNs. So, this area is also available in our queue for future goals.

REFERENCES

[1] A. A. Alalwan, "Investigating the impact of social media advertising features on customer purchase intention," *Int. J. Inf. Manag.*, vol. 42, pp. 65–77, 2018.

[2] S. Alhabash, J. Mundel, and S. A. Hussain, "Social media advertising: Unraveling the mystery box," in *Digital Advertising*, Routledge, 2017, pp. 285–299.

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

[3] I. Antoniadis, C. Assimakopoulos, and S. Paltsoglou, "Engagement and reactions of brand posts on brand fan pages in Facebook: An investigation of brand posts' characteristics," *Int. J. Internet Mark. Advert.*, vol. 15, no. 4, pp. 352–367, 2021.

[4] V. Arya, J. Paul, and D. Sethi, "Like it or not! Brand communication on social networking sites triggers consumer-based brand equity," *Int. J. Consum. Stud.*, vol. 46, no. 4, pp. 1381–1398, 2022.

[5] V. Arya, D. Sethi, and H. Verma, "Are emojis fascinating brand values more than textual language? Mediating role of brand communication to SNS and brand attachment: An insight from India," *Corporate Commun.: Int. J.*, 2018.

[6] L. Aureliano-Silva, S. Strehlau, and V. Strehlau, "The relationship between brand attachment and consumers' emotional well-being," *J. Relationship Mark.*, vol. 17, no. 1, pp. 1–16, 2018.

[7] R. P. Bagozzi, S. Romani, S. Grappi, and L. Zarantonello, "Psychological underpinnings of brands," *Annu. Rev. Psychol.*, vol. 72, pp. 585–607, 2021.

[8] S. Belaid and A. Temessek Behi, "The role of attachment in building consumer–brand relationships: An empirical investigation in the utilitarian consumption context," *J. Prod. Brand Manag.*, vol. 20, no. 1, pp. 37–47, 2011.

[9] G. Belch and M. Belch, *Advertising and Promotion: An Integrated Marketing Communication Perspective*, McGraw-Hill Education, 2019.

[10] X. Bian and S. Haque, "Counterfeit versus original patronage: Do emotional brand attachment, brand involvement, and experience matter?" *J. Brand Manag.*, vol. 27, pp. 438–451, 2020.

[11] S. Bose, S. Pradhan, M. Bashir, and S. K. Roy, "Customer-based place brand equity and tourism: A regional identity perspective," *J. Travel Res.*, vol. 61, no. 3, pp. 511–527, 2022.

[12] J. Brakus, "Experiential attributes and consumer judgments," in *Handbook on Brand and Experience Management*, B. H. Schmitt and D. Rogers, Eds. Edward Elgar, 2008.

[13] J. J. Brakus, B. H. Schmitt, and L. Zarantonello, "Brand experience: What is it? How is it measured? Does it affect loyalty?" *J. Mark.*, vol. 73, no. 3, pp. 52–68, 2009.

[14] I. Brun, L. Rajaobelina, L. Ricard, and T. Amiot, "Examining the influence of the social dimension of customer experience on trust towards travel agencies," *Tourism Manag. Perspect.*, vol. 34, Art. no. 100668, 2020.

[15] D. Centeno and D. Mandagi, "Destination brand gestalt and its effects on brand attachment and brand loyalty," *Philippine Manag. Rev.*, vol. 29, no. 1, pp. 1–24, 2022.

[16] V. S. Chand and C. Fei, "Self-brand connection and intention to purchase a counterfeit luxury brand in emerging economies," *J. Consum. Behav.*, vol. 20, no. 2, pp. 399–411, 2021.

[17] Y. P. Chang and X. B. Dong, "Impact of consumer interaction behavior on purchase intention in an SNS environment," *Inf. Dev.*, vol. 32, no. 3, pp. 496–508, 2016.

[18] M. L. Cheung, G. D. Pires, P. J. Rosenberger, and M. J. de Oliveira, "Driving consumer–brand engagement and co-creation by brand interactivity," *Mark. Intell. Plan.*, vol. 38, no. 4, pp. 523–541, 2020.

[19] S. M. Correia Loureiro and H. R. Kaufmann, "Explaining love of wine brands," *J. Promotion Manag.*, vol. 18, no. 3, pp. 329–343, 2012.

[20] M. E. David, K. Carter, and C. Alvarez, "An assessment of attachment style measures in marketing," *Eur. J. Mark.*, vol. 54, no. 12, pp. 3015–3049, 2020.

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

[[21] M. F. Diallo, J.-L. Moulins, and E. Roux, "Unpacking brand loyalty in retailing," *Int. J. Retail Distrib. Manag.*, vol. 49, no. 2, pp. 204–222, 2021.

[22] R. Donvito *et al.*, "Does personality congruence explain luxury brand attachment?" *J. Bus. Res.*, vol. 120, pp. 462–472, 2020.

[23] A. D. Ball and L. H. Tasaki, "The role and measurement of attachment in consumer behavior," *J. Consum. Psychol.*, vol. 1, no. 2, pp. 155–172, 1992.

[24] R. S. Ebrahim, "The role of trust in social media marketing on brand equity and loyalty," *J. Relationship Mark.*, vol. 19, no. 4, pp. 287–308, 2020.

[25] M. Eisend, "Have we progressed marketing knowledge?" *J. Mark.*, vol. 79, no. 3, pp. 23–40, 2015.

[26] A. Fedorikhin, C. W. Park, and M. Thomson, "Beyond fit and attitude," *J. Consum. Psychol.*, vol. 18, no. 4, pp. 281–291, 2008.

[27] S. Fournier, "Consumers and their brands," *J. Consum. Res.*, vol. 24, no. 4, pp. 343–373, 1998.

[28] F. G. Gilal *et al.*, "Brand attachment and brand passion," *Cent. Eur. Manag. J.*, vol. 29, no. 1, pp. 14–38, 2021.

[29] H. Y. Ha and H. Perks, "Effects of brand experience on the web," *J. Consum. Behav.*, vol. 4, no. 6, pp. 438–452, 2005.

[30] J. Hemsley-Brown, "Antecedents and consequences of brand attachment," *Int. J. Consum. Stud.*, vol. 47, no. 2, pp. 611–628, 2023.

[31] C. W. Park *et al.*, "Brand attachment and brand attitude strength," *J. Mark.*, vol. 74, no. 6, pp. 1–17, 2010.

[32] H. A. Voorveld, "Brand communication in social media," *J. Advert.*, vol. 48, no. 1, pp. 14–26, 2019.

[33] Z. Zubair, R. Baharun, and F. Kiran, "Role of traditional and social media in developing consumer-based brand equity," *J. Public Affairs*, vol. 22, no. 2, Art. no. e2469, 2022

.