Detection And Mitigation of Black Hole and Gray Hole Attack

Sajidha Thabassum B[#1], Chaitanya Patel G M [#2], Darshan Krishna Keshan[#2], Tegginamathada Basavananda[#2]

[#]*Electronics and Communication Department, Dr. Ambedkar Institute of Technology, nr. jnanabharathi campus nagarabhavi, Bengaluru 560056*

***Abstract*— A Mobile Ad Hoc Network (MANET) refers to a collection of wireless nodes that communicate with each other without relying on a fixed infrastructure, leveraging wireless technology and the latest advancements in mobile or dynamic devices. Due to the highly dynamic nature of their distributed structure, these networks are susceptible to various attacks, including Black Hole Attacks (BHA), Gray Hole Attacks (GHA), and others. Researchers have focused on identifying and defending against these specific assaults, particularly Gray Hole and Black Hole Attack nodes. In this review, a novel defense scheme is proposed to counter dual attacks in BHA and GHA by utilizing Artificial Neural Networks (ANNs) as a supervised neural algorithm and an optimization technique called Artificial Bee Colony (ABC). This approach employs advanced machine learning techniques to enhance the security of BHA and GHA systems. While research on protecting Mobile Ad-hoc Networks (MANETs) from dual threats is limited, this proposed approach shows promise in improving system security by selecting the most appropriate nodes to relay data packets. The network setup and design involve the utilization of NS2 (Network Simulator Version 2) software on the Linux platform, which is also employed to simulate the proposed Ad hoc communication system.**

***Keywords*— ABC, ANN, AODV, Black Hole Attack, Gray Hole Attack, MANET.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) is comprised of numerous low-cost nodes, which can either be fixed in position or randomly deployed to cover a given area. WSNs have gained popularity in various domains, involving the deployment of a large number of small nodes that sense environmental changes and transmit information through a flexible network infrastructure. These sensor nodes are well-suited for deployment in hostile environments or over vast geographical regions. Each sensor node possesses sensing, processing, storage, and communication capabilities. The nodes' deployment does not require predetermined locations, allowing for arbitrary placement in remote or inaccessible terrains, including disaster relief operations. WSNs can be organized in different configurations, and a solution designed for a flat network may not be optimal for a clustered network. Thus, adaptability to the specific network structure is crucial for efficiency and effectiveness. Due to their limited power and short communication range, sensor nodes in WSNs need to collaborate and form multi-hop wireless communication infrastructures to transmit their sensed and collected data to the nearest base station. Unlike wired networks, where physical cables provide some level of security, wireless sensor networks face numerous security challenges, especially in scenarios where nodes are deployed in hostile or dangerous terrains without physical protection. Additionally, the resource-constrained nature of sensor nodes makes security a critical concern. Implementing maximum security services on each node would significantly drain the system's resources, thereby reducing the nodes' operational lifespan.

Wireless networks, by their inherent nature of broadcast transmissions, are vulnerable to security attacks. Similarly, wireless sensor networks face unique vulnerabilities due to the placement of nodes in hostile or dangerous terrains where physical protection is lacking.

A. Black Hole Attack

The attack described is a form of Denial of Service (DoS) attack, sometimes referred to as a full packet drop attack. In this attack, a malicious node, known as the Black Hole Attack (BHA) node, attempts to divert data traffic towards itself by sending false Route Request (RREQ) packets with a low hop count and high destination sequence numbers. The presence of the malicious node can be detected during the route discovery phase. Since the network does not have static routes, dynamic routes are created using routing protocols such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing). In AODV, the source node initiates the

RREQ packet containing the destination node's address, and the packet is forwarded by neighboring nodes within their communication range.

If the neighboring node receiving the RREQ packet is not the destination node, it forwards the packet to the next node. However, if the packet is intercepted by the Black Hole node, it immediately sends a fake Route REPLY (RREP) packet back to the source node with an increased hop count, tricking the source node into believing it has established a route through the Black Hole node. The data packets from the source to the destination are then routed through the Black Hole node, resulting in all the data packets being dropped by the malicious node, disrupting the network's communication.

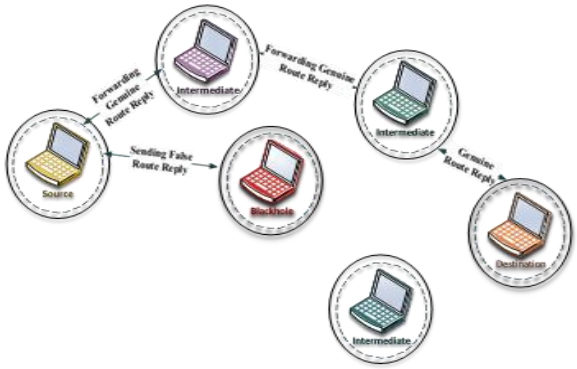


FIGURE 1. Sending FRREP by Black Hole Node

To illustrate this process, Figure 2 depicts a MANET topology consisting of seven nodes, with the source and destination nodes represented by the unheroic and orange laptops, respectively. The Black Hole node is represented by the red laptop, and the other nodes are intermediate nodes. The source node broadcasts the RREQ packet, and upon reaching the destination node, the destination regenerates the RREP packet. The regenerated RREP packet, along with a fake RREP with the highest hop count, is forwarded by the Black Hole node toward the source node. The source node, considering the packet with the highest hop count as the valid route, starts transmitting data towards the Black Hole node, mistaking it for the destination node. However, the Black Hole node drops the data packets instead of forwarding them to the actual destination.

FIGURE 2. Packet Drop by Black Hole Node

B. Gray Hole Attack

The Gray Hole Attack, also referred to as a partial packet drop attack, is a variation of the Black Hole Attack that exhibits similar characteristics. It involves selectively dropping specific data packets during the process of data transmission. In the initial phase, the Gray Hole node disguises itself as a normal node and behaves innocuously during the route discovery process. However, once the communication or data transmission begins, these nodes transform into malicious entities. The participation of the Gray Hole attack as a seemingly genuine node during the route discovery process, along with the partial dropping of data during data communication, can be observed in independent figures such as Figure 3 and Figure 4.

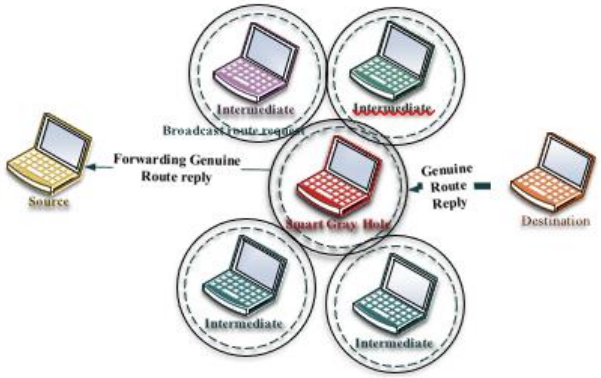
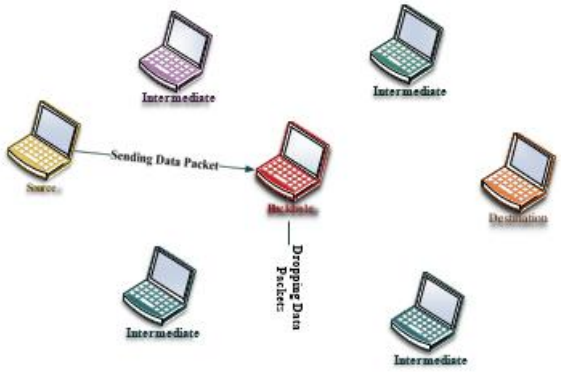


FIGURE 3. Participation of Gray hole Attack as a Normal Node during the Route Discovery process



Detecting the presence of the Gray Hole attack in Mobile Ad Hoc Networks (MANETs) can be quite challenging, as the malicious nodes mimic normal behavior during the route discovery phase. This makes it difficult for researchers to identify the Gray Hole attack in MANETs. Scholars have proposed various approaches to address the challenges posed by Black Hole and Gray Hole attacks in MANETs. However, many of these solutions only focus on mitigating a single type of attack, such as Black Hole, Warm Hole, or Gray Hole attacks, without considering

the others. Identifying the presence of Gray Hole attacks can be particularly intricate, as the malicious nodes actively participate in the route discovery process, attract data traffic, and selectively drop specific data packets. This behavior has earned them the label of "smart Gray Holes."

In summary, detecting and effectively countering Gray Hole attacks in MANETs necessitate the development of advanced security mechanisms and strategies.

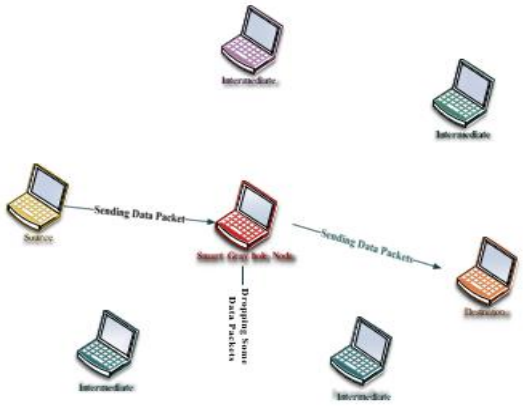


FIGURE 4. Partial packet Drop by GHA

II. MATERIAL AND METHODS

This study focuses on protecting a network against two types of attacks known as BHA and GHA. The identification of these malicious attacks was carried out using the ABC optimization algorithm (Tareq et al., 2017) in conjunction with the ANN approach (Canêdo et al., 2019). The following is a step-by-step description of the process Initially, a network of a specific size and range was designed by introducing N number of bumps into the system (N = 50 and 100). The network's requirements were listed in Table 1.

TABLE I

ORDINARY MEASURE

Matrix	Range
Node Range	50-100
Area of Network	1000 × 1000 mm2
Coverage Range	25% of the total area
Type of Model	Heterogeneous

The network was designed for a simulated area of 1000 × 1000 mm², where each node could communicate within a radius of 25 units. For example, if a node was located at position (500, 500), it could communicate with neighboring nodes whose positions ranged up to (525, 525) in both the x and y directions.

The communication capacity of the nodes was determined based on various parameters such as packet detection, coordinates, and energy consumption. After the nodes were placed, the source and destination nodes were defined. The data transmission process was performed using the AODV routing algorithm. The routing concept is illustrated in Fig. 5.

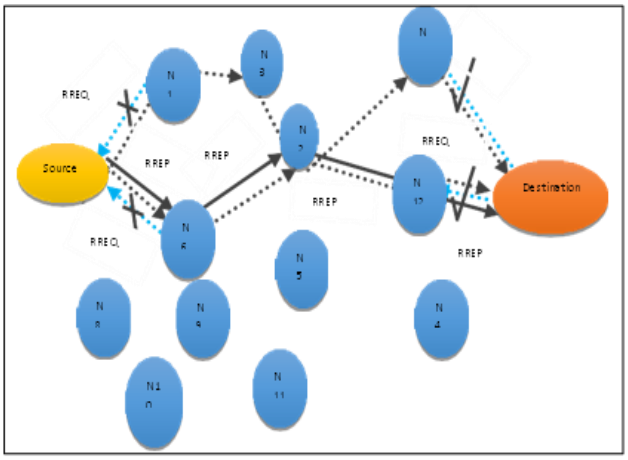


FIGURE 5. Route Discovery using AODV

In AODV, a route is established only when data needs to be transmitted. The process involves two steps: Route Request (RREQ) and Route Reply (RREP). When the source node wants to communicate with the destination node, it broadcasts a data packet containing the RREQ within its communication range (25 units). Upon receiving the data packet, each neighboring node stores the data in its routing table and forwards it to other neighboring nodes if it hasn't encountered the same data before (Taha et al., 2017; Abusalah et al., 2008). This way, the data packet reaches the destination node through multiple paths. In the AODV protocol, the most optimal route is selected for data transmission based on distance (Nakayama et al., 2008). Once the data packet reaches the destination node, it sends a route response packet back to the transmitting node via the shortest path. The route discovery process is depicted in Fig. 5, where the blue dotted line represents the Route Request transmitted by neighboring nodes, the dotted black line represents possible routes, and the solid black line represents the established route between the source and destination nodes (Gharavi, 2007). The crosses indicate nodes that receive the RREQ packet but are not the destination node, while the checkmarks represent nodes that have reached the requested destination and respond with the RREP packet (Fapojuwo et al., 2004).

III. RESULT AND DISCUSSION

After the simulation, the performance of the proposed approach using AODV (Under Threat), ABC with ANN

(After Prevention), and a comparison with the approach presented by Ali Zardari et al. (2019) was evaluated. The experiments were conducted in Network Simulator 2, following the setup shown in Figure 5.1. The evaluation was performed for 50 bumps and three mobility speeds, using three different scripts. Additionally, the system was tested against one Black Hole attack and two Gray Hole attacks.

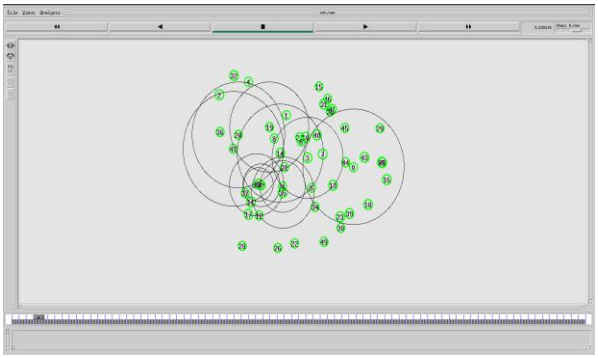


FIGURE 6. Experimental Setup

Several performance attributes were considered in the evaluation, including Throughput, Delay, Overhead, Packet delivery ratio, and Energy.

Throughput: Throughput measures the amount of data that can be transmitted over the network within a given period. It represents the rate at which data can be transferred between devices on the network and is typically expressed in bits per second (bps) or bytes per second (Bps).

Delay: Delay refers to the time it takes for a data packet to travel from its source to its destination. Various factors can contribute to delays, such as network congestion, the distance between network nodes, and processing delays.

Overhead: Overhead represents the additional data added to a packet as it traverses the network. This extra data is used for managing and controlling the transmission of data, ensuring that packets are delivered correctly.

Packet delivery ratio (PDR): which measures the percentage of data packets that are successfully delivered to their intended destinations over the network. PDR serves as an indicator of the network's reliability and indicates how well it performs in delivering packets.

Energy: Energy refers to the amount of power consumed by network devices and infrastructure for transmitting, receiving, and processing data. Energy consumption is an important consideration in network design, as it can impact performance, cost, and sustainability.

A. *Comparison of all three scenarios(proposed, with malicious node, normal AODV)*

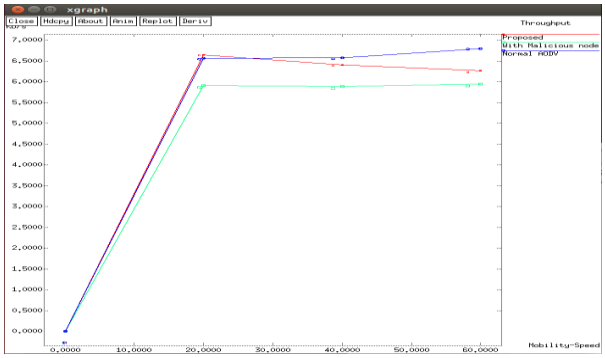


FIGURE 7: Graph of Mobility v/s Throughput

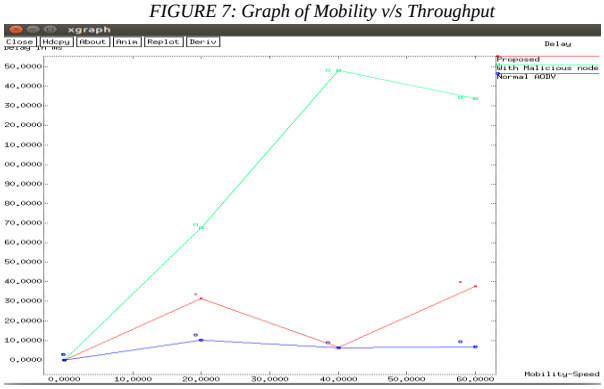


Figure 8: Graph of Mobility v/s Delay

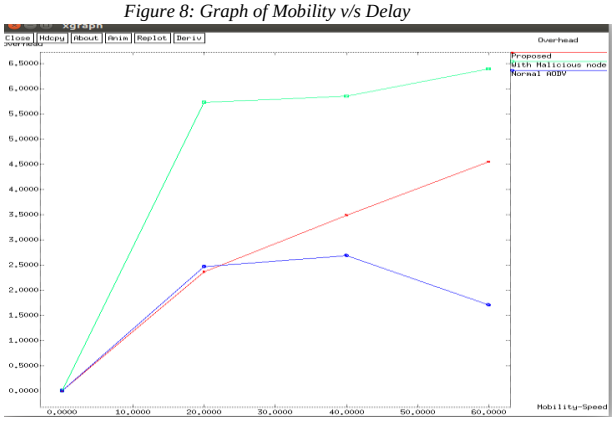


Figure 9: Graph of mobility v/s overhead

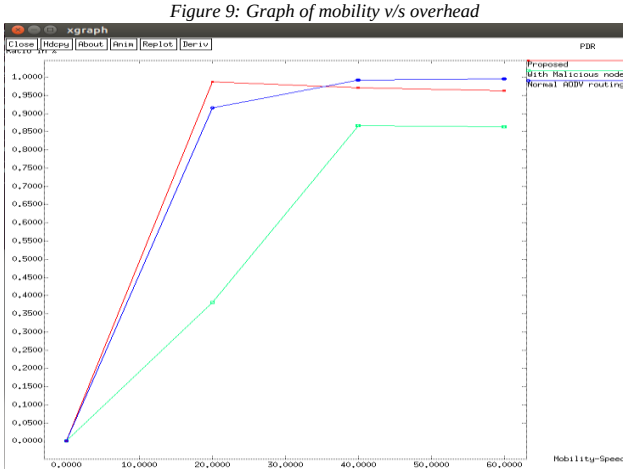


Figure 10: Graph of Mobility v/s Packet delivery ratio

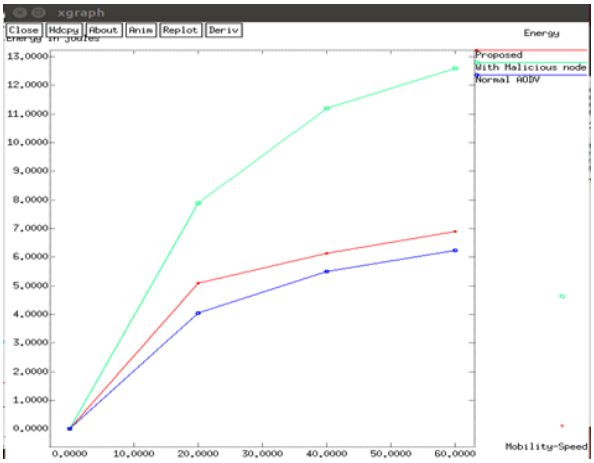


Figure 11: Graph of Mobility v/s Energy

B. *Results*

speed	Throughput (kbps)	Delay(ms)	Overhead	Pdr	Energy
20	5.91	67.61	5.731	0.38	7.9998
40	5.89	148.1	5.854	0.867	11.228
60	5.94	133.8	6.396	0.864	12.66

Table .1: With Malicious node

speed	Throughput (kbps)	Delay(ms)	Overhead	Pdr	Energy
20	6.65	31.44	2.361	0.987	5.0974
40	6.41	6.416	3.491	0.972	6.1442
60	6.27	37.67	4.549	0.962	6.8937

Table .2: Proposed Method

speed	Throughput (kbps)	Delay(ms)	Overhead	Pdr	Energy
20	6.57	10.11	2.47	0.916	4.0614
40	6.58	6.2	2.686	0.992	5.5
60	6.8	6.86	1.709	0.996	6.235

Table .3: Normal AODV Protocol

C. *Conclusion*

The presence of malicious nodes in a Mobile Ad Hoc Network (MANET) poses a significant challenge to its performance and continuity. Identifying these malicious nodes is crucial for enhancing the network's resilience. To improve the network's performance in the presence of two specific types of malicious nodes, namely BHA (Black Hole Attack) and GHA (Gray Hole Attack) nodes, a security mechanism using the ABC (Artificial Bee Colony) algorithm as a heuristic-based approach and ANN (Artificial Neural Network) as a machine learning technique has been employed.

The ABC algorithm mimics the intelligent behavior of honeybees and is utilized to classify the nodes into two lists: healthy nodes and affected nodes. The affected nodes list is further divided into BHA nodes and GHA nodes. By utilizing these classifications, the ANN is trained to enhance the network's performance. The performance analysis of the network is conducted based on metrics such as Packet Delivery Ratio (PDR), throughput, and packet detention.

REFERENCES

[1] BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map –ALY M. EL-SEMARY, AND HOSSAM DIAB – 2020

[2] A modified AODV protocol for preventing blackhole attacks in MANETs -Yugarshi Shashwat, Prashant Pandey, K. V. Arya & Smit Kumar – 2019

[3] Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks -Khalid Hussain Mohammadani1, Kamran Ali Memon, Imran Memon, Nazish Nawaz Hussaini4 and Hadiqua Fazal – 2020

[4] Mitigate Black Hole Attack Using Hybrid Bee Optimized Weighted Trust with 2 Opt AODV in MANET - Keerthika, N. Malarvizhi – 2020

[5] Improvement of Packet Delivery Fraction Due to Discrete Attacks in MANET Using MAD Statistical Approach - Sayan Majumder and Debika Bhattacharyya – 2021

[6] Maneuvering Black-Hole Attack Using Different Traffic Generators in MANETs - Fahmina Taranum and Khaleel Ur Rahman Khan – 2020

[7] Security methods against Black Hole Attacks in Vehicular Ad-Hoc Network - Krzysztof St, Aneta Poniszewska – 2019

[8] Performance Analysis of Adhoc On-demand Distance Vector Protocol under the Influence of Black-Hole, Gray-Hole, and Worm-Hole Attacks in Mobile Adhoc Network - Ausaf Umar Khan, Kamran Manish Devendra Chauhan, Milind Madhukar Mushrif, Bhumika Neole – 2021

[9] Mitigation Technique for Blackhole Attack in Mobile Ad Hoc Network - Sharma Hitesh Omprakash – 2020

[10] Analysis of security methods in Vehicular Ad-Hoc Networks against Worm Hole and Gray Hole attacks - Krzysztof St, Aneta Poniszewska – 2020

[11] A Comparison of Detection Techniques for Attacks on MANETs - Husna Gul, Maaz Bin Ahmad, Muhammad Asif – 2019

[12] Detection and Prevention of Blackhole Attack in AODV of MANET - Rajesh Puree, Bhabendu Kumar, Mohanta, Sangay Chedup – 2021
[13] A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET) - Muhannad Tahboush, Mary Agoyi – 2021
[14] An Adaptive Approach for Detecting Blackhole using TCP Analysis in MANETs - Vedant Sharma, Renu, Tanu Shree – 2020
[15] Blackhole Attack Implementation and Its Performance Evaluation Using AODV Routing in MANET - Anshu Kumari, Madhvi Singhal and Nishi Yadav – 2020
[16] P. Rani, Kavita, S. Verma and G. N. Nguyen, "Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network," in IEEE Access, vol. 8, pp. 121755-121764, 2020, doi: 10.1109/ACCESS.2020.300469