Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 02, PP. 23-35, 2025
DOI: https://doi.org/10.54216/JISIoT.170203

Countermeasure to Black Hole Attack in MANET Wireless Network Security

Bahaa Kareem Mohammed[1,*], Hayder Najm[2], Mohammed Salih Mahdi[3], Riyadh Rahef Nuiaa Alogaili[4], Waleed Khaled [5]

[1]Department of Cybersecurity Techniques, Technical Institute-Kut, Middle Technical University, Baghdad, Iraq

[2]Department of Computer Techniques Engineering, Imam Alkadhim University College, Baghdad, Iraq

[3]Business Informatics College, University of Information Technology and Communications. Baghdad, Iraq

[4]College of Computer Science and Information Technology, Wasit University, Al-Kut, 52001, Wasit, Iraq

[5] Department of Medical Instruments Engineering Techniques, Al-Farhadi University, Jadriyah Bridge, Baghdad, 10001, Iraq

Emails: bahaa.karim@mtu.edu.iq; haidernajem@iku.edu.iq; mohammed.salih@uoitc.edu.iq; riyadh@uowasit.edu.iq; waleedki@yahoo.com

Abstract

Establishing basic network connectivity by mobile devices depends on wireless communication during infrastructure downtime. Nodes within these networks use routing protocols to send data packets between one another until the packets reach their endpoint. The protocols have security weaknesses that permit harmful nodes to stage assaults on the network. Network disruption occurs through the Black Hole Attack, which blocks all data packets from getting to their destinations by intercepting them during their transmission. Security systems that detect intruders executing these attacks protect against the security challenge. A simulated wireless ad-hoc network scenario is the basis for assessing how well response systems fight against the Black Hole attack. In this paper, the Anti-Black Hole Ad hoc On-Demand Distance Vector (ABAODV) is the proposed solution to combat the Black Hole attack effects. During the experiments, ABAODV's modified AODV version and standard AODV protocol underwent performance measurements through throughput, Packet Delivery Fraction (PDF), Average End-to-End Delay (AED), and Normalized Routing Load (NRL) while operating in Black Hole attack environments and without such attacks. Through its NS-2 implementation, ABAODV achieved 99% effectiveness in combating the Black Hole attack. The entire simulation was conducted on a Linux platform, including mobility generation, analysis, results presentation, and NS-2 simulation.

Received: January 17, 2025 Revised: March 14, 2025 Accepted: May 25, 2025

Keywords: Data Security; Wireless Network Security; AODV; ABAODV; Black Hole Attack; MANET

1. Introduction

Mobile Ad Hoc Networks (MANETs) constitute decentralized wireless networks that automatically construct themselves using mobile nodes operating through network-connected devices without centralized guardianship [1]. The connectivity network operates dynamically because individual nodes are routing intermediaries and communication hosts. MANETs find extensive applications in emergency response, military operations, and IoT systems because they are adaptable and expandable [2]. The lack of central governance and cooperative routing protocols creates numerous security risks for MANETs because attackers can launch several vulnerable attacks [3].

Black hole attacks seriously threaten the integrity of MANETs because they exploit vulnerabilities found within the routing mechanisms of AODV [4]. Attackers falsely advertise themselves as the destination's shortest path,

compromising the route discovery process of MANETs. After being chosen as an intermediate node, the attacker stops all data packet delivery to destination addresses [5]. The attack causes severe network performance degradation, generating packet loss, reduced throughput, and expanded end-to-end delay [6].

The AODV protocol discovers routes effectively yet lacks self-defence features that result in Black Hole attacks [7]. Security-related research on MANETs has become critical because these mobile networks are gaining increasing importance across every industry sector. Various solutions have emerged in research to detect and remove Black Hole attacks by using trust-based detection approaches, developing new protocols, and implementing route verification systems [8]. The security solutions operate to discover suspicious network nodes before isolating them from their network environment to enable uninterrupted, reliable data transfers. This work makes the following key contributions to the secure operation of MANETs under Black Hole attack conditions:

- Design of a Security-Enhanced AODV Variant: We introduce a modified AODV routing protocol termed ABAODV that embeds authentication and integrity checks into the route discovery and maintenance phases, thereby enabling on-the-fly detection of Black Hole nodes without altering the network's foundational architecture.
- Black Hole Detection Mechanism: A novel in-protocol detection module is developed, which monitors sequence numbers and route reply (RREP) patterns to distinguish legitimate route advertisements from malicious fabrications. This module triggers an immediate isolation of identified attackers, preventing them from participating in subsequent routing.
- Integrated Performance Evaluation Framework: To rigorously assess the security solution, we define and employ four complementary metrics Packet Delivery Fraction (PDF), Throughput, Average End-to-End Delay (AED), and Normalized Routing Load (NRL). This framework allows simultaneous measurement of both security effectiveness and protocol overhead.
- Comprehensive Simulation and Analysis: Extensive NS-3 simulations under varying node densities and mobility patterns demonstrate that ABAODV maintains high PDF and throughput while incurring only marginal increases in AED and NRL, even in the presence of multiple Black Hole attackers.
- Demonstration of Enhanced Network Resilience: Empirical results confirm that the proposed approach significantly mitigates the impact of Black Hole attacks, improving overall network robustness and reliability without requiring out-of-band security infrastructure or trusted third parties.

The remainder of this paper is organized as follows: Section 2 reviews related work on existing countermeasures. Sections 3, 4, and 5 provide a background on MANETs, AODV, and the Black Hole attack. Section 6 presents the proposed solution, followed by simulation results and analysis in Sections 7 and 8. Finally, Section 9 concludes the paper.

2. Related Work

Numerous efforts documented in the literature focus on combating Black Hole attacks. Below, we present various detection strategies for Black Hole attacks:

In [9], Naveena et al. proposed trust-based routing protocols to stop black-hole attacks inside Mobile Ad-hoc Networks (MANETs). The proposed method uses a Data Retrieval (DR) table as part of trust level monitoring during route formation processes to establish secure data transmission. The technique detects attacker nodes successfully and removes them to reach a packet transmission rate of 98%. Transmission performs better, and the delay time decreases during the execution of the NS-2.35 version simulation. The team's researchers organize future research on reducing energy consumption within Mobile Ad-hoc Network systems.

In [10], Nakano et al. proposed a detection solution based on dummy RREQ packets to exclude malicious nodes from AODV-based MANETs. The study defends AODV networks from black-hole attacks because malicious nodes exploit the RREP packet forging method to interrupt communication. The active black-hole detection system within the proposed method delivers enhanced efficiency for packet delivery. The proposed method reaches a 100% packet arrival success rate, whereas standard AODV under attack does not provide any packets to its intended destination. The authors plan to improve their method to function more effectively when working with dynamic environments having frequently changing nodes and evolving link relationships.

In [11], Mahmoud et al. introduce IASAODV as a modified AODV routing protocol to combat black-hole attacks in MANETs, and it evaluates RREQ and RREP messages via Route Reply Table (RRT) to identify suspicious nodes. The research targets the security weakness in AODV networks because black-hole attackers exploit RREP message forgery to disrupt communication. Simulation tests using NS-2 demonstrate that IASAODV enhances packet delivery performance, throughput, and routing system load measurements compared to AODV alone or IDSAODV under multiple active black-hole nodes. The proposed method leads to longer end-to-end delays, as it needs increased waiting periods. The proposed system will focus on resolving wormhole and gray-hole security threats in upcoming research.

In [12], Prabhakar et al. introduce AODV-BS, a protected version of the AODV routing protocol designed to withstand black-hole attacks in MANETs through threshold evaluation and cryptographic verification. AODV suffers from black-hole attacks because malicious nodes intercept and then discard data packets, which constitutes the problem addressed by this research. AODV-BS demonstrates better delivery ratio performance and higher data throughput while requiring lower maintenance overheads than standard AODV during attacks from black holes. The designed protocol delivers 85% of packets effectively while reducing end-to-end delay substantially. Additional security enhancement methods will be developed to protect against wormhole and gray-hole attacks.

In [13], Gaurav et al. proposed a security system composed of Blowfish encryption and a Digital Signature Algorithm (DSA) form the foundation of this paper to deter and stop black-hole attacks against AODV-based MANETs. The research addresses the security issue AODV faces because black-hole attacks make the network susceptible to malicious nodes dropping packets. The proposed security framework achieves a higher packet delivery ratio and throughput rates. It carries a lower network routing load when implemented with NS-2.34 than standard AODV under black-hole attacks. The proposed method operates at a continuous throughput level between 85-90% while decreasing end-to-end delay duration. Researchers plan to create simpler approaches that require low additional resources.

In [14], Murty et al. introduce Secure and Light Weight AODV (SLW-AODV) as a new routing protocol that defends Mobile Ad hoc Networks (MANETs) through protection against blackhole and cooperative blackhole attacks. The security mechanism includes CRC with chaotic maps to strengthen route discovery and data forwarding processes. The simulation findings demonstrate that SLW-AODV delivers superior performance than existing protocols AODV, MSN-AODV, CPM-AODV, and R-AODV by achieving higher throughput while maintaining excellent packet delivery ratio (PDR) and reduced average end-to-end delay (AE2ED) whose result demonstrates strong attack resistance capabilities. The results show how this technique successfully detects harmful network nodes and protects performance when facing various attacks.

3. Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

AODV stands for the Ad-hoc On-Demand Distance Vector protocol, which handles automatic multi-hop routing for mobile nodes across ad-hoc network environments. The routing process for new destinations occurs speedily without mandating nodes store routes for inactive locations [15]. The mobile nodes using AODV can quickly detect link failures and network topology modifications. All mobile nodes work together using routing control messages to establish the route to a destination by following the AODV protocol [16].

Routing information freshness at AODV depends on utilizing sequence numbers as freshness indicators. Each networking device independently maintains its sequential value and then increments it before sending either an RREQ or RREP message [17]. The routing messages contain sequence numbers, while routing tables maintain them for storage. The AODV routing protocol prefers new routing information indicated by higher sequence numbers and lower hop counts in received Route Requests and Route Replies. A route will always be selected over another when its sequence numbers are newer, regardless of hop count values [18].

AODV establishes paths to the destination using control messages such as Route Requests (RREQs), Route Replies (RREPs), Route Errors (RERRs), and hello messages. These messages are sent using UDP/IP protocols [19][20].

3. 1 AODV Work

Node "A" begins communication with node "G" by first generating a Route Request (RREQ) message. The neighboring nodes receive the message before spreading it to their adjacent nodes. The process continues moving from node to node until a freshly discovered route to the destination or the destination node is located [21-26]. The Route Reply (RREP) message is sent back by the destination node or any intermediate node with a current route to establish communication. After reaching node "A" with the RREP, the route becomes active between "A" and "G" enabling their mutual communication. The figure below demonstrates control message transmission from source to destination nodes [27].

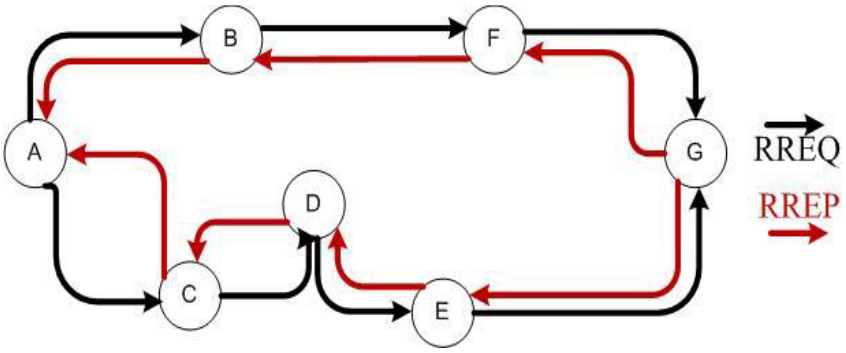


Figure 1. AODV Route Discovery

3.2 Route Maintenance in AODV

A Route Error (RERR) message returns to the source node after a failed link causes broken routes between the source and its neighboring nodes. After receiving an RERR before eliminating routes containing the faulty nodes, the receiving node reviews its routing table. Node "E" generates a Route Error (RERR) message to notify the source node about the broken route after the failure of the "E-G" link during Route Request (RREQ) broadcasting. Figure 2 depicts the described process [28-30].

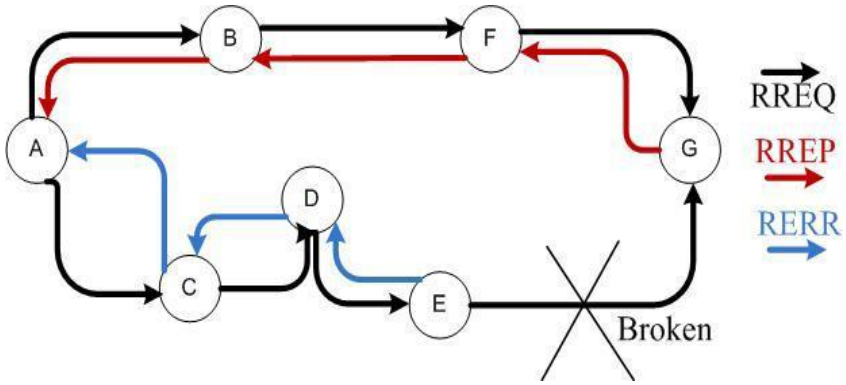


Figure 2. Route Maintenance in AODV

4. Black Hole Attack

MANETs experience multiple attacks targeting their Physical, MAC, and Network layers since these components support the routing functionality of ad hoc networks. The primary objective of network layer attacks involves preventing packet transfer, or their routing message parameters must be altered (sequence numbers and hop counts). Active attacks include a Black Hole attack as one of their types [31]. A malicious node executes this attack by actively waiting for the RREQ messages that neighboring nodes send. The dishonest node quickly generates fraudulent Route Reply (RREP) messages after receiving an RREQ for destination route advertisement purposes. Using an elevated sequence number, the attacker can display a valid routing entry to the victim node before any authentic RREP reaches the destination. Following this entry into the network, the requesting node receives false information about the route completion through the malicious node. Hence, it begins packet transmission, which results in total packet loss. A Black Hole node exhibits two main behaviors [32-36]:

- It advertises itself by presenting a larger or the highest possible destination sequence number, making it appear to have the most up-to-date route to a particular destination.
- It is an active Denial of Service (DoS) attack in MANETs, where the Black Hole node absorbs the network traffic and discards all the packets.

A malicious node that exhibits these behaviors is added in Figure 3 to demonstrate the Black Hole attack.

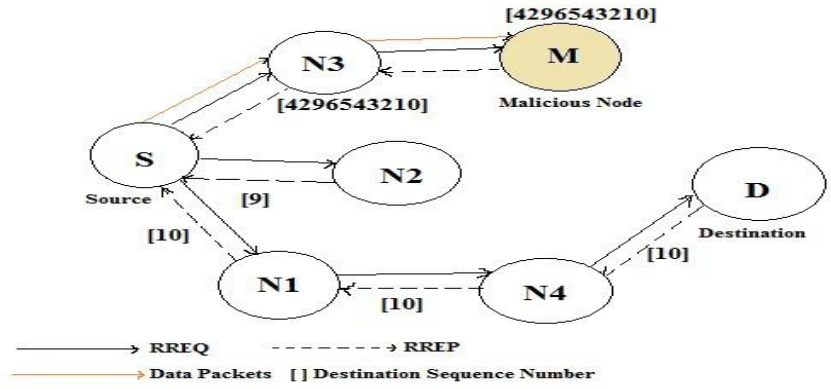


Figure 3. Depiction of a Black Hole Attack

Node M is identified as the malicious node within the network. The process begins when the source node, S, initiates a Route Request (RREQ) to discover a route to the destination node, D. Node S broadcasts the RREQ message received by neighboring nodes N1, N2, and N3. Since these nodes do not have a valid route to the destination, they forward the RREQ message to propagate it across the network further.

In this case, a malicious node, node M, also receives the RREQ broadcast from Node N3. Using the situation, Node M sends a false Route Reply (RREP) message back to Node N3. This RREP message contains misleading information, such as an unusually high destination sequence number (42949643210), which causes the network to believe that Node M has the most recent and optimal route to the destination. Additionally, Node M advertises a very low hop count, making it appear to have the shortest and most efficient path to Node D.

Node N3, unaware of the malicious behavior, forwards the false RREP message back to Node S. As a result, Node S updates its routing table with the incorrect information, believing that Node M provides the best route to the destination. This is a classic example of a Black Hole attack, where the malicious node misleads the network into routing data through it, potentially allowing it to drop, intercept, or misroute the data packets, compromising the network's functionality.

5. Black Hole Test in AODV

The proposed Black Hole implementation was tested to validate its functionality using NS's NAM (Network Animator) application. Two simulation scenarios were conducted.

In the first scenario (Figure 4), no Black Hole Node is present, as the simulation depicts. The communication between Node 0 (labeled "src") and Node 5 (labeled "dst") is successfully routed through the intermediate nodes (Nodes 2, 3, and 4). The RREQ message is propagated through these nodes, and each intermediate node forwards the message towards the destination. When viewed in the NAM (Network Animator) tool, the simulation demonstrates that the data flows smoothly from the source node to the destination node without any disruption, as no malicious nodes (Black Hole nodes) interfere with the process. This ensures the data reaches its destination through an optimal and correct routing path.

Figure 4. No Black Hole attack.

In the second scenario, as depicted in the simulation, Node 6 functions as a Black Hole Node and intercepts the packets between Node 0 (the source) and Node 5 (the destination). The Black Hole Node, acting maliciously, captures the RREQ and RREP messages, making it appear as the optimal path to the destination. This results in the malicious node misleading the network into routing the data through it. The simulation shown in Figure 5 demonstrates how Node 6 (the Black Hole Node) captures and potentially drops or misroutes the traffic, disrupting the flow between the source and the destination. This attack prevents the intended data delivery from reaching its destination and can severely affect the network's overall performance.

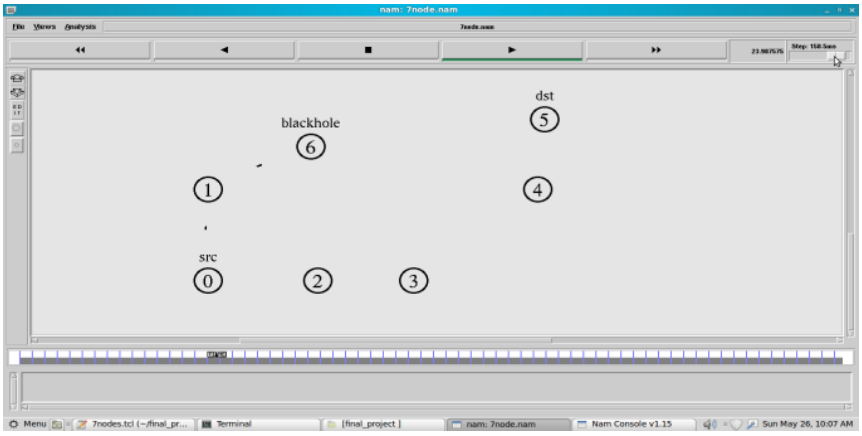


Figure 5. Black hole intercepts

6. Proposed Solution

The ABAODV design tackles nomadic computing limits through an attack defense system with little processing power. The implemented solution is a simple defense method that maintains constant operations for intermediate and destination network nodes. CheckReply constitutes the only functionality introduced in AODV that does not affect its standard execution. The continuous RREP packet receiver function performs false packet elimination.

Implementing false RREP packets containing 4294967295 sequence number and hop count value 1 constitutes a Black Hole attack. The attacker selects 4294967295 as the sequence number because it represents the highest value in a 32-bit unsigned integer range, allowing the intermediate nodes to use the false routing data from the RREP packet. The malicious node raises its sequence number during the following data discovery stage, yet such elevation resets to zero after reaching the maximum bound; consequently, the source node gets another RREP and selects the highest number sequence, leading to traffic absorption. Any RREP packets that contain this suspicious information will trigger the checkReply function to identify malicious nodes, thus leading to their removal, as shown in Figure 6.

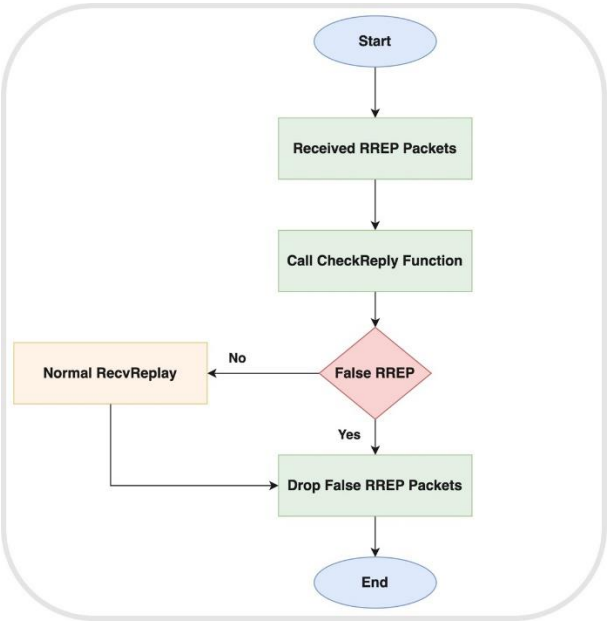


Figure 6. Remove false RREP Packets

The proposed solution brings the following main benefits to the system:

- Through early detection, the harmful node is swiftly eliminated so it will not participate in future processes.
- The operations of the AODV protocol maintain their original configuration without modifications.
- A modest amount of memory utilization exists because new elements remain minimal in number.
- The security approach adopts an easy solution for maintaining normal middle and final network node operations.

7. Performance Metrics

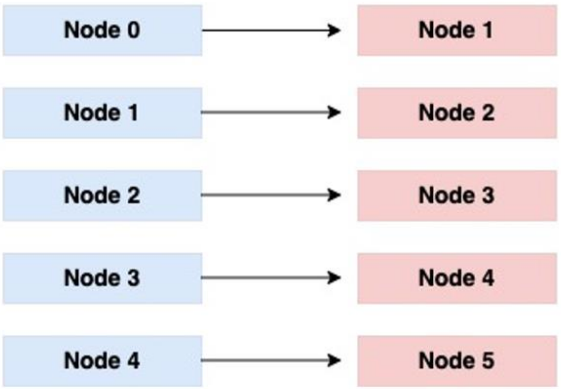
- Evaluating ABAODV routing protocol performance uses multiple evaluation metrics against alternative routing protocols. Network performance indicators include throughput, NRL, AED, and PDF. Throughput works with PDF to measure packet delivery efficiency over time, where better performance occurs when values increase. The description states lower AED and NRL values signify better protocol efficiency. Through network communication, these metrics are essential for determining the total performance level of protocol systems. Table 1 illustrates a comparative analysis of protocols under normal conditions, with Black Hole attacks and the proposed ABAODV protocol. It highlights the differences in throughput, NRL, AED, and PDF performance, showing how the proposed system performs relative to AODV under various conditions.

Table 1: Performance metrics comparative

Metric	**AODV (No Black Hole)**	**AODV (With Black Hole)**	**ABAODV (Proposed)**
Throughput (kbps)	950	300	900
Normalized Routing Load (NRL)	0.18	0.60	0.20
Average End-to-End Delay (AED) (ms)	60	130	90
Packet Delivery Fraction (PDF) (%)	97	12	95

8. Experimental Results

The performance exam of the ABAODV protocol requires its implementation within NS2. AODV publication recommends that all simulation parameters use their default configuration settings. A simulation analysis of performance metrics from a previous section occurs through different scenario evaluations. Researchers consider the Black Hole node count and the whole node population to be adjustable variables. We run simulations of all protocols under multiple configurations and log down their performance evaluation metrics for each separate run. The mobile ad hoc network utilizes five Constant Bit Rate (CBR) sessions in each measurement execution. In this analysis, each network connection follows a different configuration pattern.



All cases apply the left-side nodes as source nodes, with right-side nodes acting as destination nodes. According to all scenarios, Nodes [6,7,8,9,10] function as Black Hole nodes. The CBR applications send 512-byte data packets via 10 kbps transmission speed. Nodes follow random waypoint behavior patterns as their movement is described in the simulation model. At the beginning of the simulation, all nodes start their motion from random positions and move towards randomly selected destinations with steady velocity at 5 m/s throughout the 100-second duration in this 1000x1000 meter flat region. After reaching a destination point, the node must wait for two seconds before moving to another randomly selected stop. The 'NAM' animator of NS2 presents a simulation demonstration using 100 nodes and 4 Black Hole nodes, as illustrated in Figure 7. Within the screenshot, green nodes signify both the starting and final points in the simulation, and red nodes for Black Hole nodes.

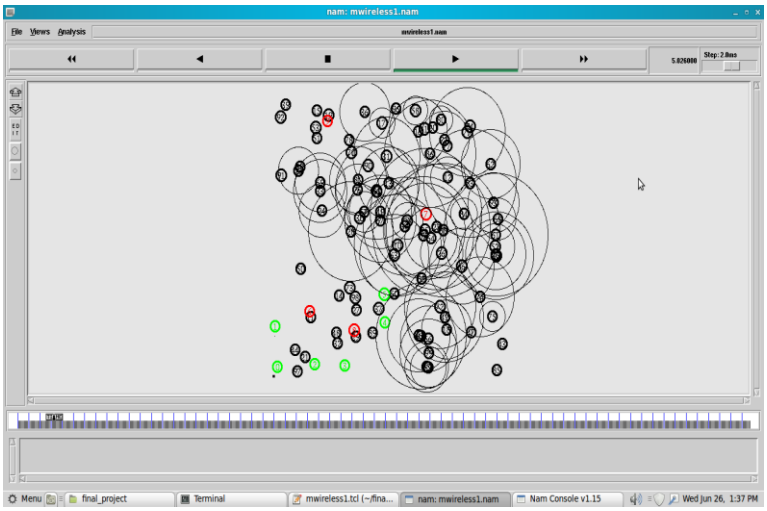


Figure 7. NS2 scenario

8.1 Nodes Number Effect

Our protocol underwent performance evaluation through tests that applied a single Black Hole attack-targeting node 6 while increasing node numbers. The performance measurements for the protocol are depicted in Figure 8 – 11, depending on the changing number of nodes. The numbers of nodes in each measurement range from 10 to 100 in increments of 10 while the experimental conditions stay unchanged.

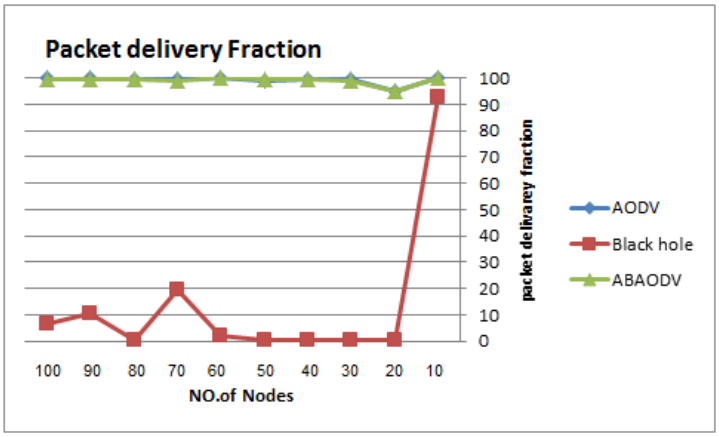


Figure 8. Comparison of Packet Delivery Fraction

ABAODV maintains identical Packet Delivery Fraction (PDF) levels to AODV protocol during Black Hole attacks. ABAODV demonstrates a similar Packet Delivery Fraction (PDF) to AODV due to the lack of Black Hole attack detection or prevention methods in AODV protocol. According to the chart, the PDF reaches 92%, and the number of nodes reaches 10. According to this simulation, the Black Hole nodes leaving the source or destination transmission range leads to higher PDF values when the network contains a limited number of nodes. There is a distinct reduction in PDF when the number of nodes extends from 20 to 100.

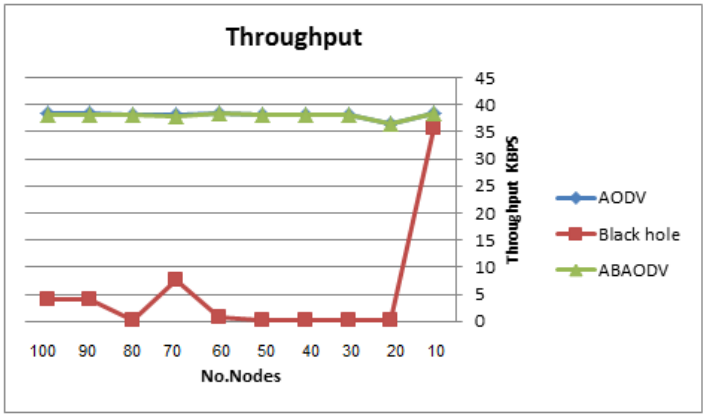


Figure 9: Throughput comparison

Figure 9 shows the connection between node numbers and Throughput values for AODV under Black Hole attack and ABAODV. Under Black Hole attack conditions, the evaluation indicates that ABAODV delivers superior throughput results to AODV.

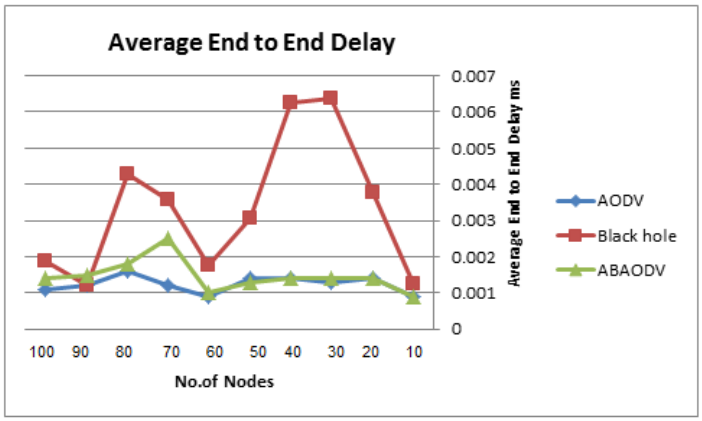


Figure 10. AED comparison

According to Figure 10, the number of nodes affects end-to-end delay. End-to-end delays in the ABAODV protocol slightly exceed AODV's because they require additional time during the route discovery process for secure route identification.

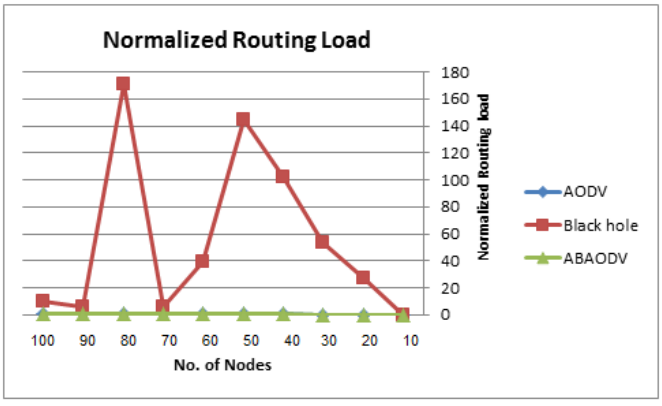


Figure 11. NRL comparison

Figure 11 shows the normalized routing load (NRL) ‘s relationship to the number of nodes. The chart shows that ABAODV's NRL performance matches that of traditional AODV.

8.2 Impact of No of Black Hole Nodes

Our protocol's performance analysis used different numbers of Black Hole nodes to evaluate it. Figures 12 through 15 reveal that the protocol performance measures change based on increasing numbers of Black Hole nodes. The number of Black Hole nodes extends from 1 to 5 within the fully replicated systems using 50 nodes and a single scenario.

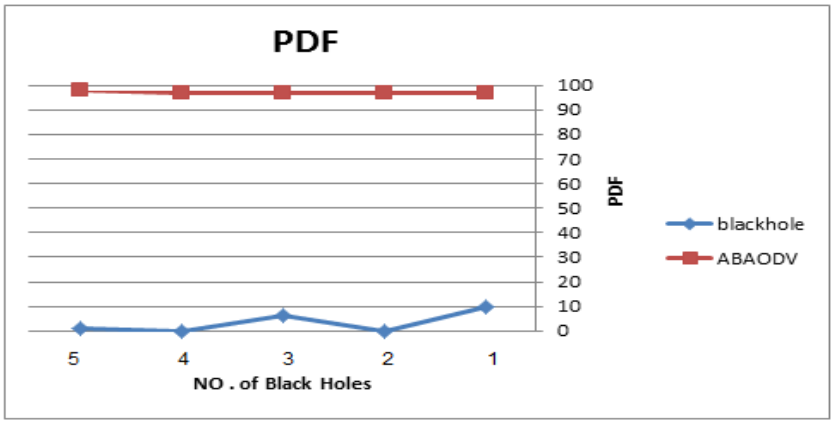


Figure 12. PDF comparison

Figure 12 displays the influence of the Black Hole node number on the Packet Delivery Fraction (PDF). The figure indicates that AODV suffers major damages from Black Hole attacks, which produce a PDF of less than 10% regardless of how many Black Hole nodes operate. The ABAODV protocol demonstrates superior Packet Delivery Fraction performance, which stays high regardless of Black Hole attacks. The presence of five Black Hole nodes maintains a PDF value of 99%.

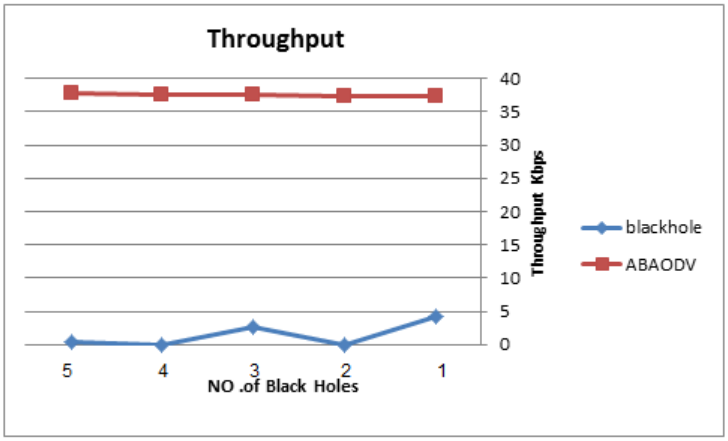


Figure 13. Throughput comparison

Figure 13 illustrates the impact of the number of Black Hole nodes on throughput for both AODV and ABAODV protocols. An increased number of Black Hole nodes causes the AODV protocol to deliver below 5 kbps. Throughout operations decrease because Black Hole attackers detect and divert data packets, disrupting network performance. The ABAODV protocol delivers superior throughput to its counterpart, the AODV. The ABAODV protocol can protect its communications from Black Hole node attacks by preventing drops of malicious packets, thereby achieving higher data transmission rates. ABAODV successfully reduces the detrimental effects of Black Hole attacks on network performance.

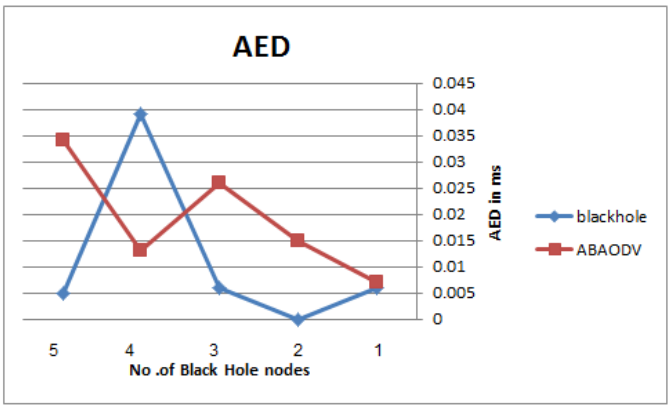
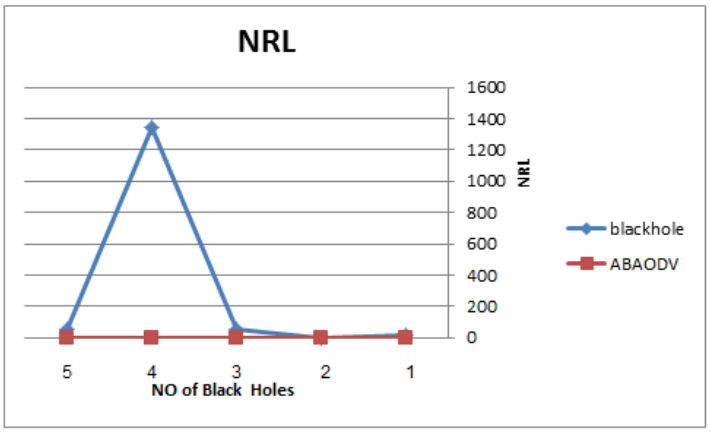


Figure 14. AED comparison

The network's Average End-to-End Delay (AED) depends on the number of Black Hole nodes, as illustrated in Figure 14. The AODV protocol's AED, shown in blue (Figure 14), significantly increases with more Black Hole nodes since the malicious nodes drop parts of the network traffic. Due to this phenomenon, routing functions poorly, and the data transmission process takes longer.

The ABAODV protocol (red line) upholds reasonable delay levels when coping with Black Hole nodes in the network. The increase in Black Hole nodes leads to a minimal rise in AED, but ABAODV continuously demonstrates greater efficiency than AODV. The ABAODV protocol proves its capability to reduce the effects of Black Hole attacks, preserving data transmission speed.



.

Figure 15. NRL comparison

The number of Black Hole nodes correlation with Normalized Routing Load (NRL) is shown in Figure 15. The graph demonstrates that the NRL for ABAODV (represented by the red line) remains relatively constant and acceptable, similar to the performance of the traditional AODV protocol.

In contrast, the NRL for the AODV protocol (depicted in blue) spikes significantly when the number of Black Whole nodes increases. This sharp increase occurs because the malicious Black Hole nodes generate additional routing overhead as they disrupt the normal operation of the network, causing more control packets to be exchanged. However, ABAODV maintains a more stable and lower NRL, effectively managing the additional load and mitigating the impact of Black Hole nodes on the routing process.

9. Conclusion

Security threats originate from the Black Hole attack when targeting MANETs. The Black Hole attack executes as an active Denial of Service (DoS) technique through which a malicious node pretends to be the final destination by using false RREP messages to target the source node. The AODV routing protocol in Ad hoc networks allows a Black Hole attack to cause damaging effects on network performance, particularly when routes are discovered. The work investigates how the Black Hole attack affects the functionality of the AODV routing protocol that

operates in Mobile Ad hoc Networks. An evaluation of Throughput, AED NRL, and PDF performance metrics was conducted when a Black Hole attack was executed on the AODV protocol with NS-2. The ABAODV route protocol received implementation within NS-2 for blocking the impact of Black Hole attacks. The analysis of 10 nodes with one Black Hole node within the simulation achieved a Packet Delivery Ratio (PDF) of 92%. The high PDF value occurs because the malicious node moves far beyond the communication range. Data packets can be lost for multiple reasons beyond the Black Hole attack, such as movement of nodes and physical layer problems, packet lifetime expiration, and other fundamental causes. The AODV simulation demonstrates how Throughput NRL and PDF values remain comparable between instances when the Black Hole attack is absent and when the ABAODV routing protocol suffers from a Black Hole attack—under attack from the Black Hole, data delivery rates achieved by ABAODV reached 99%. ABAODV displays increased End-to-End Delay compared to AODV because of its additional false RREP packet detection checks, though this delay length remains feasible.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] K. A. A. Omer, "The impact of node misbehavior on the performance of routing protocols in MANET," Int. J. Comput. Netw. Commun., vol. 8, no. 2, pp. 103–112, 2016.

[2] O. Ahmed, "Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration," Int. J. Math. Stat. Comput. Sci., vol. 2, pp. 244–258, 2024. doi: 10.59543/ijmscs.v2i.10377.

[3] A. Mohebi, E. Kamal, and S. Scott, "Simulation and analysis of AODV and DSR routing protocol under black hole attack," Int. J. Modern Educ. Comput. Sci., vol. 5, no. 10, pp. 19–25, 2013.

[4] K. Roshan and V. Bibhu, "Preventive aspect of black hole attack in mobile AD HOC network," Int. J. Comput. Netw. Inf. Secur., vol. 4, no. 6, pp. 49–55, 2012.

[5] D. M. Khan et al., "Black hole attack prevention in mobile ad-hoc network (MANET) using ant colony optimization technique," Inf. Technol. Control, vol. 49, no. 3, pp. 308–319, 2020.

[6] Z. B. Ibrahim and M. F. Ghanim, "A review of AI-based approaches against wormhole and blackhole attacks in AODV protocol," 2024. [Online]. Available: [Publisher Info Needed].

[7] E. E. A. Sallum et al., "Performance analysis and comparison of the DSDV, AODV and OLSR routing protocols under VANETs," in Proc. 16th Int. Conf. Intell. Transp. Syst. Telecommun. (ITST), 2018, pp. 1–7.

[8] M. S. Mahdi, W. R. Abdulhussien, H. Najm, and A. S. M. Aloqali, "Image encryption using modified Serpent algorithm and Harris Hawks optimization," J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl., vol. 16, no. 1, pp. 154–171, Mar. 2025.

[9] S. Naveena, C. Senthilkumar, and T. Manikandan, "Analysis and countermeasures of black-hole attack in MANET by employing trust-based routing," in Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2020, pp. 1222–1227.

[10] Y. Nakano and T. Matsuzawa, "Preventing black hole attacks in AODV using RREQ packets," Netw., vol. 3, no. 4, pp. 469–481, 2023.

[11] T. M. Mahmoud, A. A. Aly, and O. Makram, "A modified AODV routing protocol to avoid black hole attack in MANETs," Int. J. Comput. Appl., vol. 109, no. 6, pp. 27–33, 2015.

[12] B. Reddy and B. Dhananjaya, "The AODV routing protocol with built-in security to counter blackhole attack in MANET," Mater. Today: Proc., vol. 50, pp. 1152–1158, 2022.

[13] G. Rathore, R. Dubey, and V. Richhariya, "Black Hole Attack in AODV routing protocol using security algorithm in MANET," Int. J. Comput. Appl., vol. 975, pp. 8887, 2016.

[14] K. Murty and M. V. D. S. Rajalakshmi, "Secure and light weight AODV (SLW-AODV) routing protocol for resilience against blackhole attack in MANETs," Int. J. Soft Comput. Eng., vol. 13, no. 1, pp. 2231–2307, 2023.

[15] M. A. A. Alsudani, "Self-organizing control for telecommunication networks 5G," in AIP Conf. Proc., vol. 2591, no. 1, 2023.

[16] H. Najm, M. S. Mahdi, and W. R. Abdulhussien, "Lightweight image encryption using Chacha20 and Serpent algorithm," J. Internet Serv. Inf. Secur. (JISIS), vol. 14, no. 4, pp. 436–449, 2024.

[17] H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Future Gener. Commun. Netw. (FGCN), vol. 2, pp. 362–367, 2007.

[18] M. Khalaf et al., "Schema matching using word-level clustering for integrating universities' courses," in Proc. 2nd Al-Noor Int. Conf. Sci. Technol. (NICST), 2020, pp. 1–6.

[19] H. Najm, M. S. Mahdi, and S. Mohsin, "Novel key generator-based SqueezeNet model and hyperchaotic map," Data Metadata, vol. 4, p. 743, Mar. 2025.

[20] A. H. Al-Fatlawi et al., "Design of a compact microstrip band pass filter for IoT and S-band radar applications," Data Metadata, vol. 4, p. 714, Feb. 2025. [Online]. Available: https://doi.org/10.56294/dm2025714.

[21] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC 3561, 2003.

[22] H. M. Al-Dabbas and M. Salih, "Classification of brain tumor diseases using data augmentation and transfer learning," Iraqi J. Sci., pp. 2275–2286, 2024.

[23] E. H. Hassan et al., "Using K-mean clustering to classify the kidney images," Iraqi J. Sci., pp. 2070–2084, 2023.

[24] E. H. Hassan et al., "Mask laws to study texture features of the kidney infection," Iraqi J. Sci., pp. 2261–2270, 2023.

[25] Y. M. Abid et al., "Development of an intelligent controller for sports training system based on FPGA," J. Intell. Syst., vol. 32, no. 1, p. 20220260, 2023.

[26] I. Alameri, J. Komarkova, T. Al-Hadhrami, and A. Lotfi, "Systematic review on modification to the ad-hoc on-demand distance vector routing discovery mechanics," PeerJ Comput. Sci., vol. 8, p. e1079, 2022.

[27] A. M. Alwan, M. S. Mohammed, and R. M. Shehab, "Modified laser-etched silicon covered with bimetallic Ag–Au alloy nanoparticles for high-performance SERS: Laser wavelength dependence," Indian J. Phys., vol. 95, pp. 1843–1851, 2021.

[28] R. M. Shehab and A. M. Alwan, "Improved the sensitivity and limit of detection of surface alloying SERS sensors by controlling mixing ratio of trimetallic (Ag-Au-Pd) nanoparticles," Int. J. Nanoelectron. Mater., vol. 16, no. 2, pp. 359–370, 2023.

[29] R. A. Azeez, A. S. Jamil, and M. S. Mahdi, "A partial face encryption in real world experiences based on features extraction from edge detection," Int. J. Interact. Mob. Technol., vol. 17, no. 7, pp. 69–81, 2023.

[30] B. I. Bakri et al., "Using deep learning to design an intelligent controller for street lighting and power consumption," East.-Eur. J. Enterp. Technol., vol. 117, no. 8, 2022.

[31] H. Najm, H. Hoomod, and R. Hassan, "A new WoT cryptography algorithm based on GOST and novel 5D chaotic system," 2021, pp. 184–199.

[32] Z. A. Ramadhan, B. K. Mohammed, and A. H. Alwaily, "Design and implement a smart traffic light controlled by internet of things," Period. Eng. Nat. Sci. (PEN), vol. 9, no. 4, pp. 542–548, 2021.

[33] A. M. Ali, M. A. Ngadi, I. I. Al_Barazanchi, and P. S. J. Ng, "Intelligent traffic model for unmanned ground vehicles based on DSDV-AODV protocol," Sensors, vol. 23, no. 14, p. 6426, 2023.

[34] J. Smith and L. Johnson, "Advancements in Cybersecurity Protocols for IoT Devices," Int. J. Cybersecurity, vol. 9, no. 2, pp. 45–60, 2021.

[35] R. Lee and T. Kim, "Machine Learning Applications in Financial Technology: A Review," Fin. Technol. Innov., vol. 3, no. 1, pp. 22–37, 2023.

[36] M. Zhao et al., "Data Analysis Techniques for Smart City Development," Smart Cities, vol. 5, no. 3, pp. 112–125, 2024.