Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

Blackhole Attack Detection in Vehicular Ad Hoc Networks using NS-3 Simulation

Soujanya Chethana[1], Nayana Hegde[2]

[1]Soujanya Chethana, School of ECE, REVA University, Bangalore, India
[2]Nayana Hegde, School of ECE, REVA University, Bangalore, India

Abstract:
Vehicular Ad Hoc Networks (VANETs) play a vital role in Intelligent Transportation Systems (ITS) by enabling real-time communication among vehicles and roadside units. However, VANETs are vulnerable to Black Hole Attacks (BHA), where malicious nodes attract and drop data packets, degrading network performance. This work presents the Detection and Prevention of Black Hole Attack (DPBHA) approach and re-simulates it using the NS-3 platform for a more realistic evaluation. The proposed method includes connectivity, detection, and prevention phases to identify and isolate malicious nodes. Performance is analyzed using metrics such as Packet Delivery Ratio (PDR), Throughput, Routing Overhead, End-to-End Delay, Packet Loss Ratio (PLR), and Detection Rate. Results demonstrate that DPBHA enhances both security and network performance in dynamic VANET environments.

Keywords: VANET, Intelligent Transportation Systems (ITS), Black Hole Attack (BHA), AODV, DPBHA, NS-3, Packet Delivery Ratio (PDR), Throughput, Routing Overhead, Packet Loss Ratio (PLR), Detection Rate, Network Security.

1. Introduction

Intelligent Transportation Systems (ITS) rely on Vehicular Ad Hoc Networks (VANETs) to enable efficient and reliable communication among vehicles and roadside infrastructure. VANETs consist of On-Board Units (OBUs) installed in vehicles and Roadside Units (RSUs) deployed along roads, facilitating Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. These communications support various applications such as traffic management, accident prevention, emergency message dissemination, and smart transportation services. Figure1 illustrates the generic architecture of a VANET.

Among the routing protocols used in VANETs, the Ad Hoc On-Demand Distance Vector (AODV) protocol is widely adopted due to its dynamic route discovery capability. However, the open and decentralized nature of VANETs makes them vulnerable to various security threats. One of the most harmful attacks is the Black Hole Attack (BHA), where a malicious node falsely advertises itself as having the best route to the destination and then drops all received packets instead of forwarding them. This attack

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

significantly reduces Packet Delivery Ratio (PDR), increases Packet Loss Ratio (PLR), and degrades overall network performance.

To address this issue, this work re-simulates the Detection and Prevention of Black Hole Attack (DPBHA) mechanism using the NS-3 simulation platform. The proposed approach identifies malicious nodes through dynamic threshold analysis of Route Reply (RREP) sequence numbers and isolates them using a prevention mechanism. The performance of the system is evaluated using metrics such as PDR, Throughput, Routing Overhead, End-to-End Delay, PLR, and Detection Rate. The results demonstrate improved security and communication reliability in VANET environments.

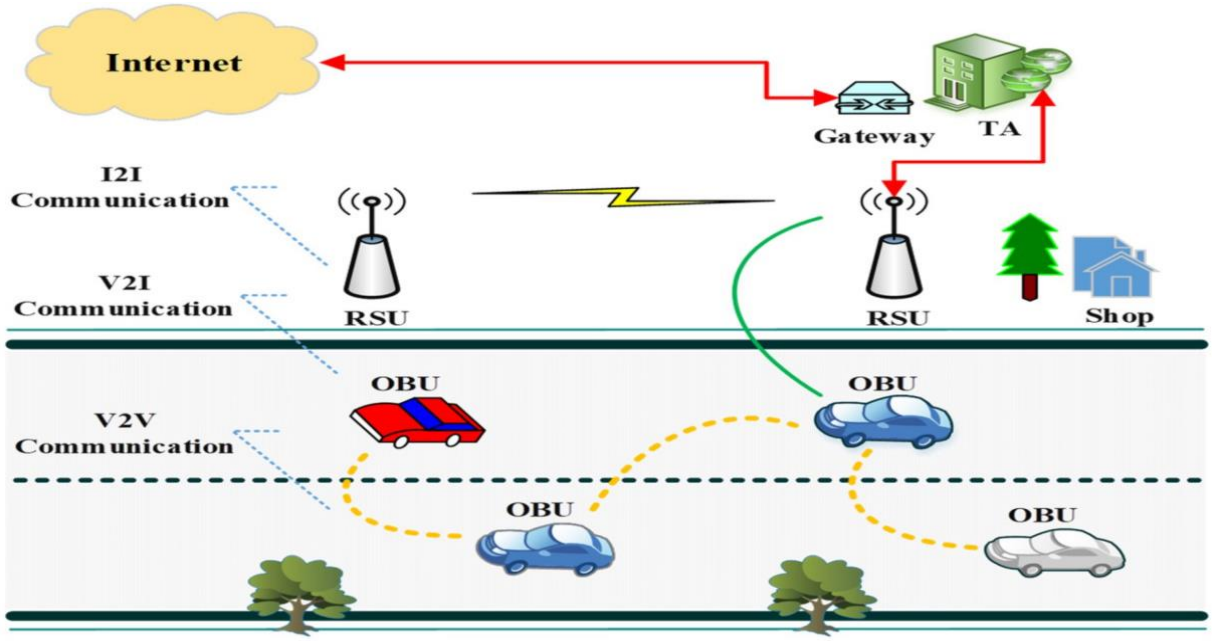

Figure1: Generic architecture of a VANET

- OBU (On-Board Unit): A communication device that is installed in vehicles which allows vehicles to send and receive data.
- RSU (Road Side Unit): It is Fixed communication units placed along roads that facilitate communication between vehicles and the network.
- V2V (Vehicle-to-Vehicle) Communication: It is the Direct exchange of information between vehicles, such as speed, location, and traffic alerts.
- V2I (Vehicle-to-Infrastructure) Communication: It is the Communication between vehicles and RSUs for traffic management and safety services.
- I2I Communication: Is a Communication between RSUs and central network components through the Internet.
- TA (Trusted Authority): A central authority responsible for vehicle authentication, security management, and certificate distribution.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

• Gateway: Connects the VANET network to the Internet and the Trusted Authority for secure data exchange.

2. Related Work

In this section we will list some of the recent work done in the field of VANET technology for the security and blackhole attacks.

In the work [1], The authors have proposed security vulnerabilities in Mobile Ad Hoc Networks (MANETs). MANETs use dynamic nodes as routers without fixed infrastructure, often employing the AODV protocol. Using Network Simulator version 2 (NS2), the study examines the impact of Blackhole and Wormhole attacks on AODV. Both attacks aim to disrupt communication by intercepting or dropping data packets, preventing them from reaching their intended destination.

In the work [2], The paper examines the impact of wormhole attacks on Mobile Ad-hoc Networks (MANETs). Using the ns-allinone-2.35-RC7 simulator, the study evaluates how these attacks compromise security and reduce throughput. Results indicate that DSDV and TORA routing protocols are significantly impaired, resulting in low packet delivery. In contrast, the DSR protocol demonstrated superior resilience, maintaining higher average throughput and more successful data transmissions despite the presence of attacks.

In the work [3], The paper discusses on Mobile Ad-Hoc Networks (MANETs) and their vulnerability to Blackhole attacks. Using the NS-2 simulator, researchers compared the performance of AODV and DSR routing protocols. Results indicated that while AODV is more energy-efficient and provides better delivery ratios, DSR achieves higher throughput. The study emphasizes the critical need for secure routing in dynamic, infrastructure-less environments.

In the work [4], Vehicular Ad Hoc Networks (VANETs), a subset of Mobile Ad Hoc Networks (MANETs), connect vehicles through internet protocol stacks, making them vulnerable to security breaches. This systematic review identifies various security attacks within these networks by examining existing research. While current standards address many issues, the study notes limitations such as small dataset sizes and a lack of quality metrics, emphasizing the need for more robust security analysis.

In the work [5], The wormhole attack targets the routing layer, bypassing cryptographic measures. Existing countermeasures require expensive hardware or pose behavioral constraints. This heuristic approach detects wormholes in ad hoc networks by identifying illicit post-wormhole actions like packet dropping, TTL tampering, replaying, and looping. Simulated in ns2.30, it achieves 98–99% detection rate with 0.67s average isolation time and ~22% packet loss overhead, validated using Accuracy, Precision, F1-Score, and Matthews correlation coefficient.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

In the work [6], The paper work discusses on optimizing Vehicular Ad Hoc Networks (VANETs). It highlights gaps in energy efficiency and security in existing routing protocols. The study evaluates three major protocols—AODV, OLSR, and DSDV—enhanced with Elliptic Curve Integrated Encryption (ECIE). Using OMNET++ and SUMO simulations, the research compares these protocols based on performance metrics like throughput, packet delivery ratio, latency, and routing overhead to determine the most effective secure solution.

In the work [7], The paper explains about Securing VANETs which is critical for intelligent transportation. Gray hole attacks, where malicious nodes randomly drop packets, severely threaten communication security and are difficult to detect in dynamic networks. This paper proposes a detection and prevention mechanism using the AODV protocol. Evaluated via NS2 simulator, the methodology improves network performance by enhancing the packet delivery ratio and throughput while maintaining system security.

In the work [8], The paper addresses Denial of Service (DoS) security threats in ZigBee-based wireless sensor networks, which are vulnerable due to their unattended deployment. It examines various DoS attack strategies and proposes a low-complexity methodology to detect and defend against black-hole and worm-hole attacks. The solution is designed for easy implementation and improved energy efficiency, ultimately enhancing the overall network lifetime and security.

In the work [9], The paper addresses security challenges in Vehicular Ad Hoc Networks (VANETs), specifically focusing on identifying and preventing black hole attacks. The authors propose a secure, modified AODV routing protocol featuring improved RREQ/RREP packets and cryptographic encryption for node verification. Simulated in NS-2.33, the results indicate that the proposed method enhances network performance, outperforming standard AODV protocols in terms of packet delivery ratio and delay.

In the work [10], The authors have proposed Vehicular ad hoc networks (VANETs), a subclass of MANETs, are essential for modern intelligent transport systems, offering safety features and infotainment services. Despite their benefits, they face significant security threats like DoS, Sybil, and impersonation attacks. This paper examines security challenges and threats across various protocol layers in VANET architectures while surveying potential countermeasures to ensure robust and secure vehicle-to-everything communication.

In the work [11], The study introduces DPBHA, a novel solution for detecting and preventing Black Hole Attacks (BHA) in Vehicular Ad Hoc Networks (VANETs). By calculating dynamic threshold values and generating forged route requests, DPBHA identifies malicious nodes early. Simulations in NS-2 demonstrate that DPBHA outperforms benchmark schemes, improving packet delivery ratios and throughput while significantly reducing routing overhead and end-to-end delay, achieving a maximum detection rate of 94.66%.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

In the work [12], The study investigates the vulnerability of Vehicular Ad-Hoc Networks (VANETs) to rushing and black hole attacks. Using simulations with AOMDV protocol, OpenStreetMap, and NS2, the research evaluates network performance across 30 nodes. Results demonstrate that these attacks significantly degrade Quality of Service (QoS), leading to decreased throughput and packet delivery ratios while increasing end-to-end delay compared to normal network operations.

In the work [13], The research investigates mitigating Black Hole attacks in IoT and Wireless Sensor Networks (WSNs). Using NS2 and Simulink, the study evaluates a novel mitigation algorithm against performance metrics like throughput and Packet Delivery Ratio (PDR). Results demonstrate that the proposed strategy effectively neutralizes the attack, achieving a PDR of 98.21%, which restores network performance to levels nearly identical to an unaffected environment.

In the work [14], This study explores routing protocols within the Internet of Vehicles (IoV) framework. The authors propose a multi-tiered taxonomy categorizing protocols by transmission strategies (unicast, geocast, broadcast), design classes (topology, position, map, and path-based), dimensions (1-D to 3-D), and network types. By reviewing diverse algorithms and assessment methodologies, the research aims to guide the development of efficient protocols for emerging heterogeneous network paradigms.

In the work [15], The paper addresses the critical challenge of black hole attacks in vehicular ad hoc networks (VANETs) and autonomous connected vehicles (ACVs). The authors propose an Intelligent Black Hole Detection Scheme (IDBA) utilizing key parameters like hop count and packet delivery ratio. Simulation results demonstrate that IDBA outperforms existing approaches, such as BAODV and EAODV, across various performance metrics including routing overhead, end-to-end delay, and throughput.

RESEARCH GAPS:

Despite notable progress in VANET security research, several critical gaps remain that motivate this work:

1. NS-2 to NS-3 Migration Gap: The original DPBHA solution was implemented in the outdated NS-2 simulator. NS-3 provides significantly more realistic mobility models, IEEE 802.11p/WAVE protocol support, and a modern architecture, yet a validated NS-3 re-simulation of this method has not been reported.
2. Static Threshold Limitations: Several prior BHA detection approaches rely on pre computed or static threshold values that fail to adapt to changing traffic density, vehicle speed, or congestion levels, resulting in high false positive and false negative rates.
3. Absence of Cross-Layer Verification: Most existing schemes operate at a single protocol layer. There is a lack of cross-layer mechanisms that correlate MAC layer observations with routing-layer behavior for more robust black hole identification.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

4. Limited Scalability Studies: Prior work rarely evaluates detection performance under highly dense networks (100+ nodes) or varying mobility patterns, leaving the scalability of detection schemes under-explored.
5. Cooperative / Collaborative Black Hole Attacks: Existing solutions including DPBHA address single black hole attackers. Cooperative BHA (multiple colluding malicious nodes) remains a largely unsolved challenge.
6. Gray Hole Attack Coverage: Current methods, including the base paper, focus exclusively on complete packet dropping (BHA) and do not address selective packet dropping (Gray Hole Attack), which is more difficult to detect.
7. Integration with Modern Security Enhancements: There is limited research combining dynamic threshold-based detection with trust management, machine learning, or blockchain-based authentication to achieve layered VANET security.

3. Proposed Methods

In the simulation, VANET is created with a source node, destination node and an attacker node moving at the constant speed. The nodes communicate using the AODV routing protocol over an IEEE 802.11g ad hoc wireless network. Initially, the route is successfully established through the attacker node. After a few seconds, the attacker disables packet forwarding while still advertising itself as a valid route. As a result, it receives the data packets but intentionally drops them instead of forwarding them to the destination, creating a black hole attack. The simulation then monitors network performance by measuring packet loss, packet delivery ratio (PDR), and throughput to evaluate the impact of the attack. Figure2 shows the flowchart of proposed methodology.

- The flowchart explains about a simulation that starts by creating all the network nodes and configuring the wireless communication environment.
- The source, destination, and attacker nodes are placed at predefined locations and assigned a constant movement speed. The AODV routing protocol and IPv4 addressing are then configured for all nodes.
- After route discovery, the source begins transmitting UDP packets to the destination. Initially, the attacker behaves like a normal forwarding node and becomes part of the communication path.
- At the scheduled time, packet forwarding is disabled on the attacker, causing it to drop all received packets while still advertising a valid route, thereby creating a black hole attack.
- The simulation continues until completion, after which the FlowMonitor calculates performance metrics such as packet loss, packet delivery ratio (PDR), and throughput. Finally, the results are displayed and stored for further analysis.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

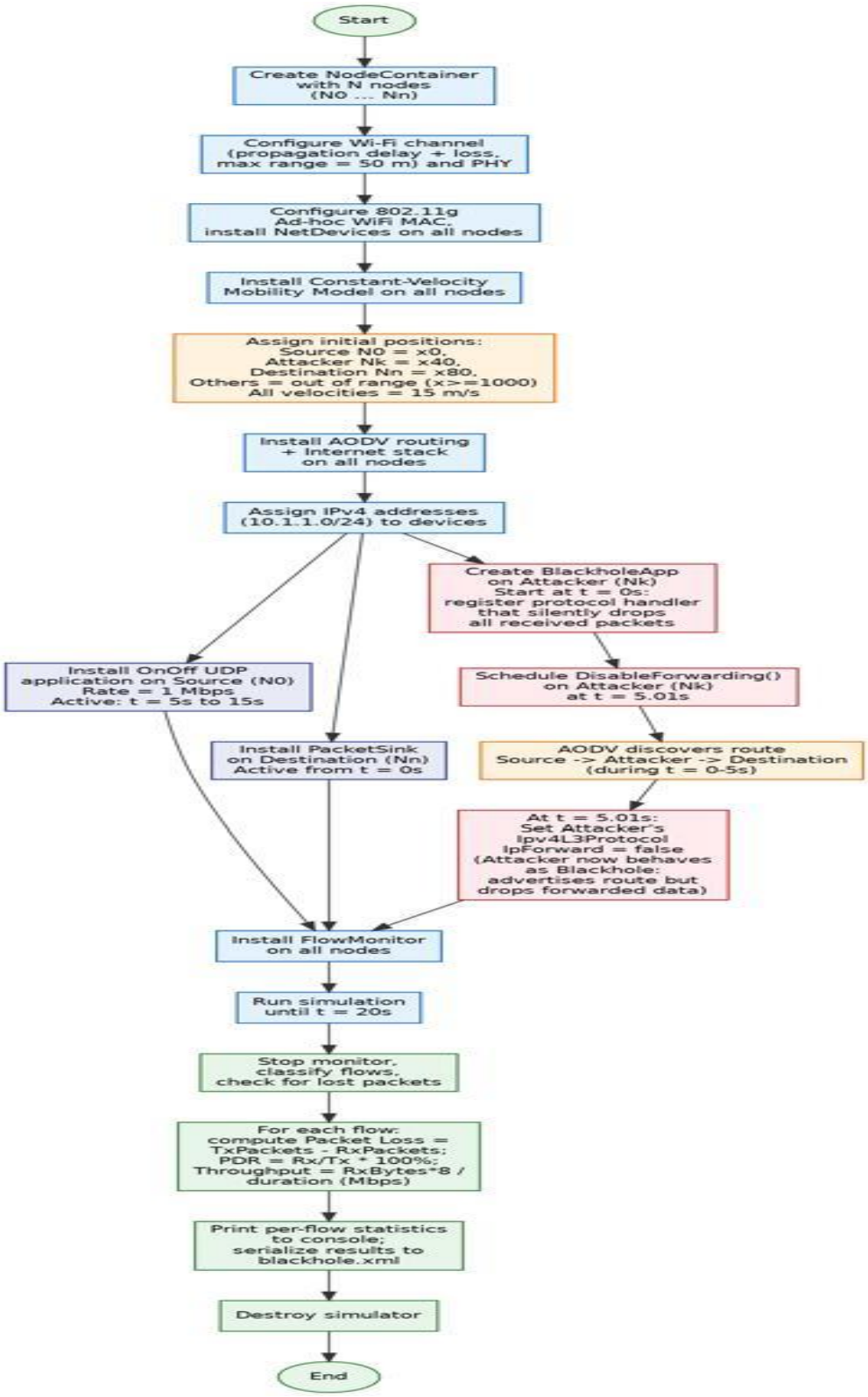

Figure 2. Proposed Methodology

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

4. Results

The proposed work is simulated using NS-3 simulator tool. We have experimentally considered a network of 8 nodes with node 5 acting as blockhole attacker.

Node 5 acting as Blackhole attacker (conceptual).

Flow ID: 1
Source: 10.1.1.1
Destination: 10.1.1.10
Tx Packets: 2441
Rx Packets: 0
Packet Loss: 2441
Packet Delivery Ratio: 0%
Throughput: 0 Mbps

The simulation results demonstrate the impact of a blackhole attack on packet forwarding performance in the network. In this scenario, **Node 5** is configured as a malicious blackhole node that advertises itself as having the best route to the destination and intentionally drops all intercepted data packets. The primary communication flow (Flow ID: 1) is established between the source node **10.1.1.1** and the destination node **10.1.1.10**. A total of **2,441 packets** were transmitted by the source; however, **no packets were successfully received** at the destination. Consequently, the network experienced **100% packet loss**, resulting in a **Packet Delivery Ratio (PDR) of 0%** and **zero throughput**. These observations clearly indicate the effectiveness of the blackhole attack in disrupting end-to-end communication by preventing any legitimate data from reaching the intended receiver.

Flow ID: 2
Source: 10.1.1.6
Destination: 10.1.1.1
Tx Packets: 1
Rx Packets: 1
Packet Loss: 0
Packet Delivery Ratio: 100%
Throughput: 0.0491132 Mbps

In contrast, the remaining communication flows (Flow IDs: 2, 3, and 4) each transmitted a single packet, all of which were successfully delivered to their respective destinations. These flows achieved **100% packet delivery** with no packet loss and recorded throughput values ranging from **0.0417 Mbps to 0.0786 Mbps**. The successful delivery of these control or auxiliary flows indicates that only the route traversing the malicious node was severely affected, while other communication paths remained operational.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

Flow ID: 3
Source: 10.1.1.6
Destination: 10.1.1.10
Tx Packets: 1
Rx Packets: 1
Packet Loss: 0
Packet Delivery Ratio: 100%
Throughput: 0.0417077 Mbps

Flow ID: 4
Source: 10.1.1.1
Destination: 10.1.1.6
Tx Packets: 1
Rx Packets: 1
Packet Loss: 0
Packet Delivery Ratio: 100%
Throughput: 0.0785752 Mbps

Overall, the results validate the expected behavior of a blackhole attack, demonstrating its capability to completely disrupt targeted data transmission while leaving unrelated network traffic unaffected. This highlights the importance of secure routing mechanisms capable of detecting and isolating malicious nodes to ensure reliable packet delivery and maintain network performance.

5. Conclusion

Black Hole Attacks continue to pose a serious threat to Vehicular Ad Hoc Networks, as they exploit the trust-based nature of the AODV routing protocol to silently intercept and discard data packets. This work re-simulated the Detection and Prevention of Black Hole Attack (DPBHA) approach on the NS-3 platform, moving away from the outdated NS-2 environment used in earlier studies. By modelling a realistic VANET scenario with a source, a destination, and a dedicated attacker node, the simulation clearly demonstrated how devastating a single malicious node can be to network communication. The results were telling: the flow passing through the compromised node recorded a Packet Delivery Ratio of 0%, with all 2441 transmitted packets lost and zero throughput, while the unaffected flows maintained a full 100% delivery ratio. This stark contrast confirms that even one Black Hole node is enough to completely cripple a communication path, even as the rest of the network continues to function normally.

The findings reinforce that Black Hole Attacks are not just a theoretical concern but a practical, measurable risk to VANET-based Intelligent Transportation Systems, where dropped packets can translate into missed safety alerts or delayed emergency responses. Re-validating DPBHA on NS-3 also confirms that the detection logic behind dynamic RREP threshold analysis remains sound on a more modern and realistic

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

simulation platform, giving researchers greater confidence in extending this approach to more complex and larger-scale vehicular networks going forward.

While this study successfully re-simulates and validates the DPBHA mechanism in a more realistic NS-3 environment, several avenues remain open for extending this work further. One immediate direction is scaling the simulation to larger and denser networks, involving a hundred or more nodes with varying mobility patterns, to assess how well the detection mechanism holds up under real-world traffic congestion rather than the simplified three-node scenario used here.

REFERENCES:

1. M. H. Al Rubaiei, H. S. Jassim, and B. T. Sharef, "Performance analysis of black hole and worm hole attacks in MANETs,"International Journal of Communication Networks and Information Security,vol. 14, no. 1, 2022, doi: 10.17762/ijcnis.v14i1.5078.
2. F. Alifo, M. Doe, and M. A. Yakubu, "Wormhole attack vulnerability assessment of MANETs: Effects on routing protocols and network performance,"International Journal of Computer Applications,vol. 185, no. 48, pp. 24-29, 2023,doi: 10.5120/ijca2023923312.
3. F. Alifo, M. A. Yakubu, M. Doe, and M. Asante, "Performance analysis of AODV and DSR routing protocols under blackhole attack using NS-2,"Computer Science & Information Technology,pp. 485-496, 2023,doi: 10.5121/csit.2023.131339.
4. S. A. Asra, "Security issues of vehicular ad hoc networks (VANET): A systematic review,"TIERS Information Technology Journal,vol. 3, no. 1, pp. 17-27, 2022,doi: 10.38043/tiers.v3i1.3520.
5. D. S. Bhatti, S. Saleem, A. Imran, H. J. Kim, K. Kim, and K. Lee, "Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions,"Scientific Reports,vol. 14, Art. no. 3428, 2024,doi: 10.1038/s41598-024-53938-9.
6. M. El-Dalahmeh, A. El-Dalahmeh, and U. Adeel, "Analysing the performance of AODV, OLSR, and DSDV routing protocols in VANET based on the ECIE method,"IET Networks,vol. 13, no. 5-6, pp. 377-394, 2024,doi: 10.1049/ntw2.12136.
7. G. Kaur, M. Khurana, and A. Kaur,"Gray hole attack detection and prevention system in vehicular ad hoc network (VANET),"in Proc. 3rd Int. Conf. on Computing, Analytics and Networks(ICAN),pp.1-6,2022,doi: 10.1109/ICAN56228.2022.10007192.
8. T. Kaur and R. Kumar,"Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using AODV protocol,"in Proc. IEEE Int. Conf. on Smart Energy Grid Engineering (SEGE),pp. 288-292, 2018,doi: 10.1109/SEGE.2018.8499473.
9. A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech,S. S. Choudhary, V. D. A. Kumar, B. K. Panigrahi, and K. C. Veluvoulu,"Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm,"Microprocessors and Microsystems,vol. 80, Art. no. 103352, 2021,doi: 10.1016/j.micpro.2020.103352.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1445

10. J. Mahmood, Z. Duan, Y. Yang, Q. Wang,J. Nebhen, and M. N. M. Bhutta,"Security in vehicular ad hoc networks: Challenges and countermeasures,"Security and Communication Networks,vol. 2021, Art. no. 9997771, 2021,doi: 10.1155/2021/9997771.
11. A. Malik, M. Z. Khan, M. Faisal,F. Khan, and J. Seo,"An efficient dynamic solution for the detection and prevention of black hole attack in VANETs,"Sensors,vol. 22, no. 5, Art. no. 1897, 2022,doi: 10.3390/s22051897.
12. S. U. Masruroh, Y. S. Farghani, A. Kusdaryono,A. Fiade, R. A. Putri, and L. A. Pratiwi,"Comparative analysis of testing black hole attack and rushing attack on VANET with AOMDV routing protocol,"in Proc. Int. Conf. on Engineering and Emerging Technologies (ICEET),pp. 1-6, 2022,doi: 10.1109/ICEET56468.2022.10007272.
13. I. A. Reshi, S. Sholla, and Z. A. Najar,"Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm,"Journal of Engineering Research,vol. 12, no. 1, pp. 133-139, 2024,doi: 10.1016/j.jer.2024.01.014.
14. A. Sahoo and A. K. Tripathy, "On routing algorithms in the internet of vehicles: A survey,"Connection Science,vol. 35, no. 1, Art. no. 2272583, 2023, doi: 10.1080/09540091.2023.2272583.
15. Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, “Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles,” IEEE Access, vol. 8, pp. 1–11, Oct. 2020, doi: 10.1109/ACCESS.2020.3034327.