Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 11(2) 2026

Journal of Computing Research and Innovation

Behavioural Investigation of Blackhole and Sinkhole Attacks using AODV Routing Protocol in VANET

Ahmad Yusri Dak[1*], Adib Ahza Aktar[2]

[1,2]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) Perlis Branch, Arau Campus, 02600 Arau, Perlis, Malaysia.*

ARTICLE INFO

Article history:
Received 24 October 2025
Revised 8 June 2026
Accepted 8 June 2026
Online first
Published 1 September 2026

Keywords:
VANET
AODV
Blackhole
Sinkhole
NS-2
SUMO

DOI:
10.24191/jcrinn.v11i2.580

ABSTRACT

A Vehicular Ad-hoc Network (VANET) enables communication between vehicles (V2V) and roadside infrastructure (V2I). This technology aims to enhance road safety, traffic efficiency, and passenger comfort by sharing real-time information, such as hazard warnings, forming the backbone of Intelligent Transportation Systems (ITS) and autonomous driving. Within these environments, the Ad-hoc On-Demand Distance Vector (AODV) routing protocol is frequently employed. AODV discovers paths on-demand using route requests and replies in VANETs, this allows for efficient adaptation to high vehicle mobility by establishing fresh routes only when communication is required. However, the dynamic and open nature of VANETs makes them vulnerable to security threat i.e. malicious actors can deploy Blackhole and Sinkhole attacks to disrupt the network, causing severe performance degradation including packet loss, increased latency, and reduced throughput which can lead to significant traffic risks in modern transportation system. This research aims to simulate Blackhole and Sinkhole attacks using the AODV routing protocol in a VANET. The methodology involves simulating these attacks within a controlled environment using NS-2, SUMO and OpenStreetMap to generate realistic traffic scenarios. The performance of AODV protocol is assessed by analysing key metrics, which is throughput, end-to-end delay (EED), packet delivery ratio (PDR), and routing overhead (RO). Findings indicate that both Blackhole and Sinkhole attacks significantly degrade VANET performance, with sinkhole attacks causing the most severe impact at high node densities. At a density of 100 nodes, a Sinkhole attack reduces throughput by 31% (from 62.21 to 42.99 kbps) and the PDR by 5.4% (from 83.23% to 78.73%) compared to normal traffic conditions. Meanwhile, Blackhole attacks increase routing overhead by 29% (from 7.21 to 9.28) and delay by 23% at moderate densities. Furthermore, variations in packet size amplify these disruptions. These results underscore the urgent need for adaptive, attack-resistant routing protocols to maintain traffic efficiency and reliability.

1. INTRODUCTION

The rapid increase in global traffic density has spurred the development of Intelligent Transportation Systems (ITS) to enhance road safety and improve traffic flow. A cornerstone of this advancement is the

[1*] Corresponding author. *E-mail address*: ahmadyusri@uitm.edu.my
https://doi.org/10.24191/jcrinn.v11i2.580

Vehicular Ad Hoc Network (VANET), a self-organizing network that enables seamless wireless communication between vehicles (V2V) and roadside infrastructure (V2I). VANETs facilitate the real-time exchange of critical information such as accident alerts, traffic conditions, and emergency updates which is vital for a secure and efficient transportation network (Kugali & Kadadevar, 2020). To manage this communication, routing protocols such as Ad hoc On-Demand Distance Vector (AODV) are employed to dynamically establish paths that adapt to the network's constantly changing topology.

However, the decentralized and open-access nature of VANETs renders them susceptible to a variety of security threats. Among the most potent and destructive are Blackhole and Sinkhole attacks. A Blackhole attack involves a malicious node falsely advertising the shortest path to a destination and subsequently dropping all received data packets (Waoo & Tiwari, 2021). Similarly, a Sinkhole attack lures surrounding nodes into routing their traffic through a compromised node, which can then drop, alter, or selectively forward packets, creating significant security and privacy risks (Malik et al., 2022). These attacks not only degrade technical network performance causing packet loss, increased end-to-end delay, and reduced throughput but also pose severe societal risks, ranging from compromised data integrity to life-threatening traffic accidents.

This study and identifies that VANETs are critical for ITS, they are inherently vulnerable due to their high-mobility nature. Many existing studies focus on single attack types or limited metrics within general Mobile Ad Hoc Networks (MANETs). Specifically, there is a need for a more granular analysis of how these routing attacks behave under varying node densities and packet sizes in a realistic urban simulation. The novelty of this work lies in its dual-scenario comparative analysis, using a combination of NS-2, SUMO, and OpenStreetMap to ground simulations in real-world geographic layouts. By assessing a comprehensive suite of metrics including PDR, throughput, EED, and routing overhead, the study reveals the "deceptive efficiency" of Sinkhole attacks, which maintain performance at low densities but cause a severe collapse in high-density environments. This provides a technical benchmark for developing adaptive, intelligent security protocols for modern ITS. The insights gained from this research provide valuable benchmarks for understanding VANET vulnerabilities, contributing directly to the development of more resilient systems and ensuring the reliability of future transportation infrastructure.

2. RELATED WORK

Vehicular Ad-hoc Networks (VANETs) are a cornerstone of Intelligent Transportation Systems (ITS), facilitating crucial Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication to enhance road safety and traffic efficiency (Dak et al., 2025). However, the inherent characteristics of VANETs such as their dynamic topology, open wireless medium, and decentralized nature render them highly susceptible to security threats. Among these, Blackhole and Sinkhole attacks pose significant risks due to their direct impact on data availability and network integrity (Dak, 2012).

According to Parida et al. (2024), a Blackhole attack occurs when a malicious node exploits the Ad hoc On-Demand Distance Vector (AODV) routing protocol by falsely advertising itself as the shortest path to a destination. Upon receiving a Route Request (RREQ), the attacker immediately broadcasts a fraudulent Route Reply (RREP) containing a high sequence number and minimal hop count. This lures legitimate traffic through the malicious node, which then drops all intercepted data packets, leading to severe data loss, increased latency, and the failure of safety-critical applications. A Sinkhole attack is closely related; here, a malicious node strategically positions itself to attract a significant portion of network traffic by advertising an exceptionally attractive route. Once traffic is redirected, the attacker may drop, eavesdrop on, or modify the data. Solutions for Sinkhole attacks are often implicit, as their malicious behaviour frequently culminates in packet dropping, which is subsequently addressed by Blackhole detection mechanisms (Waoo & Tiwari, 2021).

Recent research has focused on developing robust detection and prevention mechanisms for Blackhole attacks in AODV based VANETs. A common approach involves leveraging the AODV route discovery

https://doi.org/10.24191/jcrinn.v11i2.580

process. For instance, Muthusamy (2025) proposed the Improved Detection and Prevention Source Authentication (IDPSA) and the Detection and Prevention of BHA (DPBHA) algorithms. These utilize dynamic thresholds on RREP destination sequence numbers (DSN) and forged RREQ packets to identify and isolate malicious nodes. These methods have demonstrated significant improvements in network performance, with DPBHA achieving a 94.66% detection rate and 98.6% accuracy, alongside an increased Packet Delivery Ratio (PDR) and reduced End-to-End (E2E) delay.

A significant trend in the field is the increasing reliance on Artificial Intelligence (AI) and Machine Learning (ML) for attack detection. Madani et al. (2025) proposed a model utilizing Extreme Gradient Boosting (XGBoost) and Support Vector Machines (SVM) for anomaly detection, achieving 98.67% accuracy. Similarly, the Multivariate Statistical Detection Scheme (MVSDS) proposed by Ajjaj et al. (2022) continuously verifies network traffic against a multivariate normality assumption to detect abnormal activities in real-time without modifying the underlying routing algorithm. Furthermore, the Enhanced AODV (E-AODV) protocol developed by Kudrenko and Stoliar (2025) integrates adaptive trust mechanisms and behavioral monitoring to enhance resilience against Blackhole and Gray Hole attacks. These AI/ML approaches highlight a shift toward more intelligent, adaptive security solutions capable of identifying complex attack patterns.

Most studies rely on network simulators such as NS-2, NS-3, and SUMO for implementation and evaluation, often incorporating realistic mobility traces. While this provides a controlled testing environment, it also highlights the ongoing challenge of bridging the "simulation-reality gap" for real-world deployment. Common limitations across existing literature include a primary focus on single Blackhole attacks, often failing to address cooperative or Gray Hole variants. Additionally, the susceptibility of neural networks to adversarial attacks remains a concern. Future research must expand solutions to cover complex attack types, optimize AI/ML for computational efficiency, and develop comprehensive security frameworks.

Table 1: Comparative summary of blackhole/sinkhole attack mitigation in AODV-VANETs

Author	Attack Type(s) Addressed	Detection Technique	Key Performance Metrics Evaluated	Result and Analysis	Limitations
Muthusamy (2025)	Black Hole Attack	Uses dynamic threshold on RREP DSN and forged RREQ packets to confirm malicious nodes.	Throughput (TP), Routing Overhead (ROH), Packet Delivery Ratio (PDR)	• Significantly decreases ROH (33.8% to 26.7% vs AODV, 6.3% to 4.3% vs DPBHA); • Improved Throughput and PDR.	Does not test performance under varying vehicle speeds, weather conditions, or urban vs. highway scenarios, which can influence detection accuracy.
Madani et al. (2025)	Black Hole Attack	Use Extreme Gradient Boosting (XGBoost) based on Support Vector Machine (SVM) for anomaly detection.	Accuracy, F1 Score, Precision Score, Recall Score, Packet Delivery Ratio (PDR), Packet Loss Rate (PLR)	• Achieved accuracy Throughput to 98.67%;	Simulation with a single attacker node and small network size, limiting its realistic validation for complex, multi-attacker real-world MANET environments
Ajjaj et al. (2022)	Black Hole	Use Multivariate Statistical Detection Scheme (MVSDS)	Throughput (TH), Dropped Packets Ratio (DPR),	• Detects abnormal activities in real-time;	Its scope is restricted to single-attacker detection without offering an

https://doi.org/10.24191/jcrinn.v11i2.580

	Attack (mainly)	to verifies conformity of network traffic data	Overhead Traffic Ratio (OTR)	•	Min-Max Normalization improves data sensitivity;	active mitigation or reaction scheme
Kudrenko and Stoliar (2025)	Black Hole, Gray Tunnel attacks	incorporating adaptive trust mechanisms, response timing analysis, and behavioral monitoring.	Packet Delivery Ratio (PDR), End-to-End Delay, Packet Loss Rate (PLR)	•	Outperforms standard AODV in delivery efficiency and security reliability.	Simulation results may not accurately reflect real MANET conditions such as interference, fading, and mobility.

3. METHODOLOGY

In simulation scenario, realistic map data from OpenStreetMap was utilized to create a detailed simulation environment. By using the SUMO mobility model, simulations were conducted with diverse packet sizes: 1000, 2000, 3000, 4000, and 5000. These simulations were executed in NS2, SUMO and OpenStreetMap where data traffic was transmitted using the AODV routing protocol, its incorporating blackhole and sinkhole attacks as well as scenarios without both attacks. The performance metrics were then analysed to evaluate the impact of these attacks on the network.

The workflow of the research for this study is structured into six key phases to systematically investigate the impact of Blackhole and Sinkhole attacks on VANETs as shown in Fig. 1. Workflow is essential in establishing the network environment used in the VANET simulation. Each step must be followed to ascertain that the simulation setup most accurately reflects real-case vehicular network scenarios.

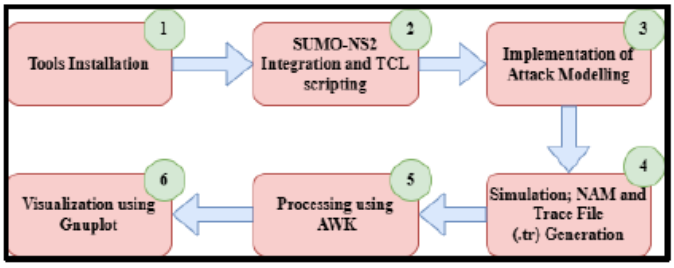

Fig. 1. Workflow of the research

The core of the methodology is the network design and simulation phase, which leverages a combination of specialized tools to model the VANET environment. Network Simulator 2 (NS-2) was chosen as the primary tool for simulating network communication and assessing the performance of the AODV routing protocol due to stability and popularity of the chosen tool. NS-2 provides a robust framework for creating and managing network nodes, data packet transmissions, and the implementation of various routing protocols. To ensure that the simulation scenarios were as realistic as possible, the Simulation of Urban Mobility (SUMO) was employed. SUMO generates dynamic and varied vehicle mobility patterns, which are essential for replicating the unpredictable nature of real-world traffic. The integration of NS-2 and SUMO allowed for the creation of realistic scenarios where the behaviour of vehicles and their communication could be accurately modelled as presented in Fig. 2.

https://doi.org/10.24191/jcrinn.v11i2.580

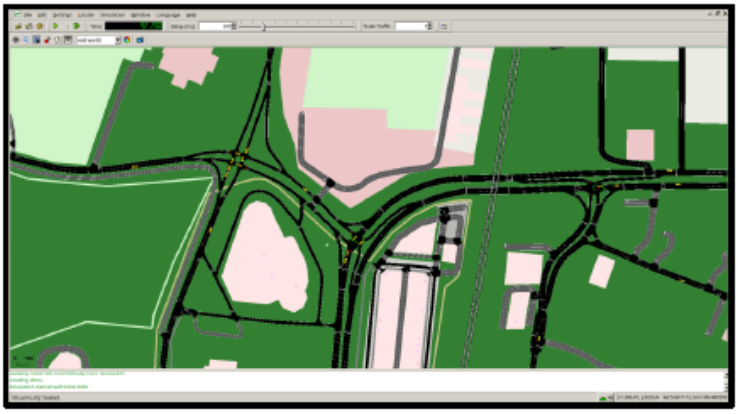

Fig 2. Integration between Ns-2 and SUMO

In this phase, a specific VANET area of 1000m x 1000m and 2100m x 1800m was defined, representing an urban traffic landscape as exposed in Table 2 (simulation parameter). OpenStreetMap was utilized as a mapping tool to import real-world geographic data into the simulation, grounding the study in a practical context and enhancing the accuracy and reliability of the results. This setup enabled the controlled introduction of Blackhole and Sinkhole attacks to observe their effects on network performance. The subsequent network testing and simulation phase involved conducting a series of experiments under varying conditions to collect data on network performance with and without the presence of these attacks.

Table 2 Simulation Parameter

Parameter	Value/Detail
Mobility Model	SUMO (Real-world street maps)
Node Density	20 to 100 Vehicles
Traffic Type	CBR (Constant Bit Rate)
Metrics	PDR, Throughput, End-to-End Delay

The data analysis phase focused on evaluating the collected data based on four key performance metrics: network throughput, Packet Delivery Ratio (PDR), End-to-End Delay (EED), and Routing Overhead (RO). Throughput was used to measure the successful data transmission rate, while PDR calculated the ratio of successfully received packets to the total number of packets sent. EED assessed the average time taken for a packet to travel from its source to its destination, and RO quantified the number of control packets generated to maintain network connectivity. Finally, the documentation phase organized these findings into a comprehensive and accessible report, with results presented visually to clearly illustrate the impact of the attacks. This structured methodology provides a solid framework for understanding the vulnerabilities of VANETs and contributes to the development of more secure Intelligent Transport Systems.

The research assumes an untrusted environment where nodes operate without a centralized certificate authority, rendering the network susceptible to routing-layer exploits. In this context, the study focuses on two primary attack models: the Blackhole Attack and the Sinkhole Attack. In a Blackhole attack, a malicious node exploits the AODV route discovery process by falsely claiming to possess the shortest path to a destination; once it attracts the traffic, it silently drops all intercepted packets, causing complete data loss for that route. Similarly, in a Sinkhole attack, a compromised node advertises deceptive routing updates such as a high route preference to attract traffic from neighboring nodes. Once positioned as a central hub, the attacker can drop, alter, or selectively forward packets, creating severe routing inefficiencies and providing a gateway for further malicious activity.

https://doi.org/10.24191/jcrinn.v11i2.580

The simulation framework utilizes Network Simulator 2 (NS-2) and the Ad-hoc On-demand Distance Vector (AODV) protocol, a choice that remains both academically and practically justified. NS-2 is a well-established tool for wireless network simulation, offering the flexibility and granular performance metrics necessary to analyze complex vehicular interactions. AODV, a reactive routing protocol, is selected due to its widespread application in VANETs and its documented vulnerability to network-layer disruptions. Because AODV relies on the trust of route advertisements during the discovery phase, malicious nodes can easily participate and broadcast false information, making it the ideal protocol for evaluating the performance degradation caused by Blackhole and Sinkhole maneuvers in a controlled, realistic environment.

4. RESULT AND ANALYSIS

The evaluation was conducted across two primary scenarios: varying node densities and different packet sizes as discussed in next sub-section.

4.1 Impact of number of nodes in VANET

a. Throughput vs. Number of Nodes:

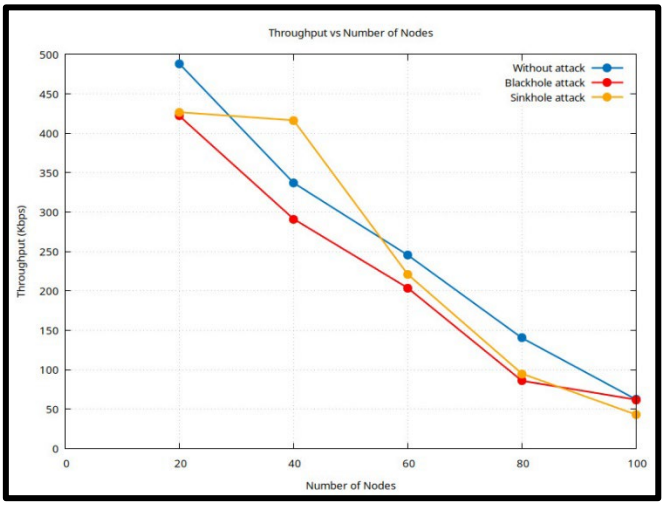

Fig. 3. Throughput(kbps) vs increasing no of nodes

Fig. 3 illustrates that both Blackhole and Sinkhole attacks significantly degrade VANET throughput, with their impact intensifying as node density increases. In these scenarios, malicious nodes drop or manipulate data, causing substantial packet loss and latency. As node density rises, the resulting traffic congestion exacerbates these effects by increasing delays and complicating attack detection. This leads to a sharp decline in the Packet Delivery Ratio (PDR), higher end-to-end delay, and a throughput reduction of up to 85% over time, which severely compromises VANET communication and safety. According to Bani Younes and Boukerche (2015), higher node density increases the potential for traffic volume, if the network infrastructure cannot manage this surge, the result is diminished speeds, longer delays, and an increased risk of accidents.

Furthermore, while normal operations exhibit a gradual decline in throughput due to natural traffic congestion, blackhole attacks consistently yield lower performance by discarding packets across all

https://doi.org/10.24191/jcrinn.v11i2.580

densities. In contrast, Sinkhole attacks initially maintain throughput levels comparable to normal conditions at low node densities but exhibit a precipitous decline as density increases, ultimately causing more damage than Blackhole attacks in high-density environments. These findings highlight the distinct disruption mechanisms of each attack and underscore the critical need for effective security strategies to preserve VANET integrity, particularly in densely populated networks.

b. Packet Delivery Ratio (PDR) vs. Number of Nodes:

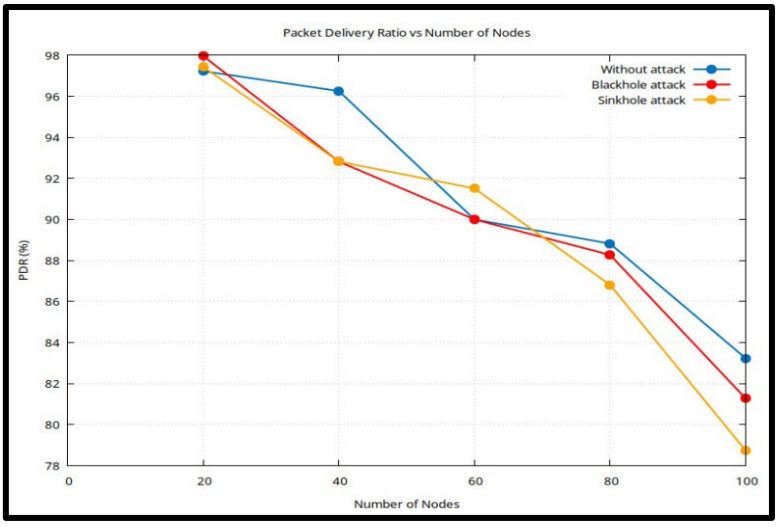

Fig. 4. Packet delivery ratio vs number of nodes

The findings presented in Fig. 4 indicate that both Blackhole and Sinkhole attacks negatively impact the Packet Delivery Ratio (PDR) in VANETs, with the severity of these effects intensifying as node density increases. Compared to a network with no attacks, both malicious activities drastically reduce the PDR. For instance, at a density of 30 nodes, the PDR drops from approximately 57.7% to 36.4% under a Blackhole attack and falls below 10% at higher densities. These disruptions occur because malicious nodes selectively or entirely drop data packets, significantly reducing the volume of successful deliveries. As node density grows, PDR degradation is exacerbated by increased network congestion and the wider spread of the attack, which severely compromises communication reliability as mentioned by Azmir & Ruslan (2024). Under normal conditions, routing remains efficient, resulting in a higher PDR; however, these attacks critically impair network performance and vehicular safety. In contrast, Sinkhole attacks lead to more substantial and persistent delivery failures at high densities by continuously misrouting traffic through compromised nodes. While all scenarios exhibit similar performance at low node densities, the more aggressive PDR degradation under Sinkhole attacks highlights their highly disruptive nature in dense VANET environments. These results underscore the urgent need for targeted security measures capable of detecting and mitigating such attacks to ensure reliable packet delivery.

c. End-to-End Delay (EED) vs. Number of Nodes:

As shown in Fig. 5, the results indicate that Blackhole attacks typically cause higher end-to-end delays than Sinkhole attacks, although these delays remain slightly below the peak observed in the no attack scenario. Furthermore, delays under Sinkhole attacks are generally lower and more stable than those under

https://doi.org/10.24191/jcrinn.v11i2.580

Blackhole attacks. Consequently, both types of attacks increase latency compared to an ideal stable state as node density rises (exceeding 60 nodes).

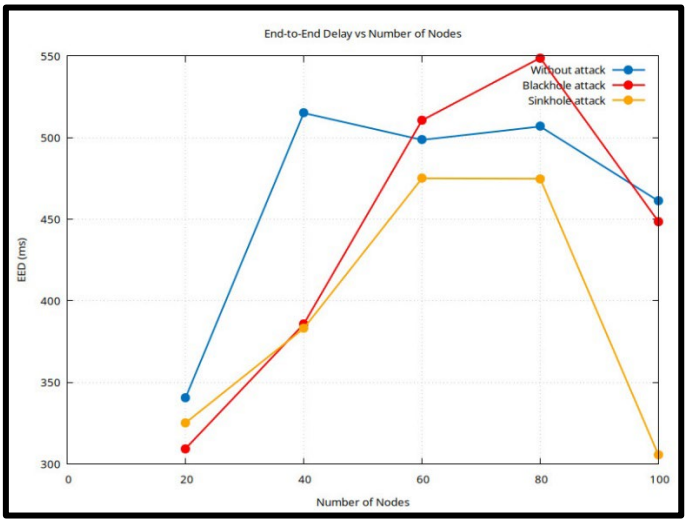

Fig. 5. End-to-End Delay (EED) vs. Number of Nodes

Initially, Blackhole attacks lead to lower delays at low node counts, as packets are discarded immediately upon reception rather than being processed and forwarded. However, as density increases, delays escalate significantly due to the overhead associated with frequent retransmissions and the constant need for route rediscovery. In contrast, while Sinkhole attacks maintain lower delays than both the normal and Blackhole scenarios at higher densities, they still severely degrade overall network performance. Ultimately, these findings confirm that malicious attacks progressively compromise VANET communication quality, a trend that is particularly pronounced in high-density environments.

d. Routing Overhead (RO) vs. Number of Nodes:

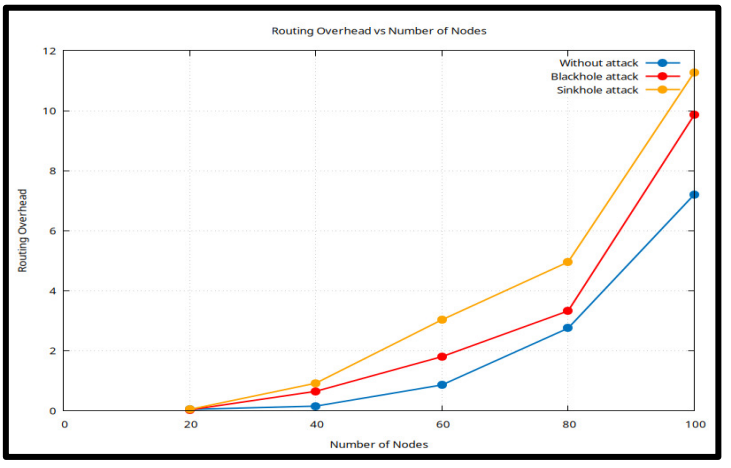

Fig. 6 Routing Overhead (RO) vs. Number of Nodes

https://doi.org/10.24191/jcrinn.v11i2.580

Fig. 6 demonstrates that both Blackhole and Sinkhole attacks significantly increase routing overhead (RO) in VANETs, with the impact intensifying as node density grows. Under normal conditions (the no attack scenario), the routing overhead increases gradually up to a density of 80 nodes, before rising to approximately 7kps at 100 nodes. In contrast, the Blackhole attack consistently generates higher overhead than the baseline, spiking sharply to approximately 10.0 at 100 nodes. The Sinkhole attack exhibits the most severe impact, with overhead exceeding all other scenarios and reaching nearly 12kps at the 100-node mark.

Consequently, both attacks substantially inflate routing overhead due to malicious disruptions within the network layer. Blackhole attacks trigger repeated route discovery processes because of continuous packet dropping, whereas Sinkhole attacks introduce even greater inefficiencies through the creation of routing loops and misleading paths. This surge in extra control messages reduces overall network efficiency, a finding that aligns with the research conducted by Kugali and Kadadevar (2020). These results highlight the inherent vulnerabilities of VANET routing protocols and underscore the necessity of implementing robust detection and mitigation strategies to minimize control traffic and maintain network stability.

4.2 Impact of packet sizes in VANET

The second scenario focused on evaluating the network's performance with varying packet sizes (1000, 2000, 3000, 4000, and 5000 bytes) while the number of nodes was fixed at 60.

a. Throughput vs. Packet Sizes:

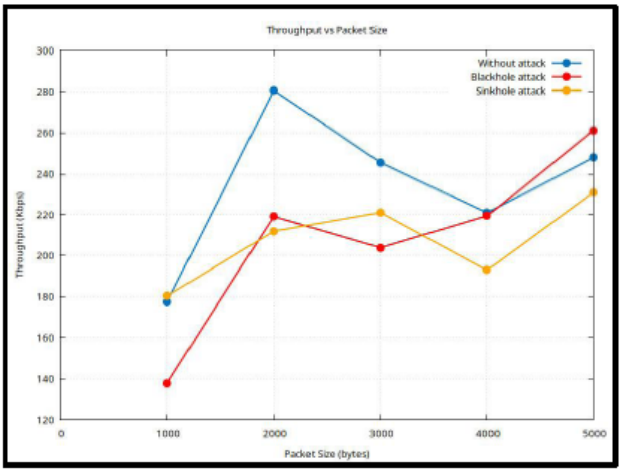

Fig. 7. Throughput vs. Packet Sizes

At small packet sizes (approximately 1,000 bytes), throughput is lowest under the Blackhole attack due to the high rate of packet loss resulting from malicious dropping. Conversely, smaller packets generally exhibit lower end-to-end delay because they can be transmitted more rapidly than larger payloads. As packet size increases, throughput improves across all scenarios, demonstrating that larger packets carry data more efficiently despite the presence of attacks.

Specifically, the Blackhole attack consistently results in the lowest throughput, although this metric climbs steadily with increasing packet size, reaching nearly 240 kbps at a 5,000-byte payload. Despite this

https://doi.org/10.24191/jcrinn.v11i2.580

growth, the Blackhole attack maintains a reduced throughput across all tested sizes compared to the baseline. Under both Blackhole and Sinkhole attacks, delay is elevated across all packet sizes because malicious nodes drop or reroute traffic, necessitating frequent retransmissions and the use of suboptimal paths. This delay increases more sharply as packet size grows, suggesting that routing attacks amplify latency issues as the payload scales. Consequently, while larger packets facilitate higher data volumes, they also incur significant delays that are further exacerbated by malicious interference.

Furthermore, while the Sinkhole attack performs slightly better than the Blackhole attack, it remains below the no-attack baseline, exhibiting a moderate throughput increase from 185 kbps to 230 kbps. Although larger packets help mitigate some throughput loss, they cannot fully counteract the disruptive impact of the attacks. The Sinkhole attack is particularly detrimental at larger packet sizes, where malicious nodes attract and discard high-volume traffic, leading to increased congestion and retransmissions. This magnifies throughput degradation, as the loss of fewer, larger packets has a more severe impact on overall data delivery efficiency than the loss of smaller segments. Therefore, while attacks significantly reduce throughput particularly at smaller packet sizes, larger packets provide a marginal recovery in data volume at the cost of increased network latency.

b. End-to-End Delay (EED) vs. Packet Sizes:

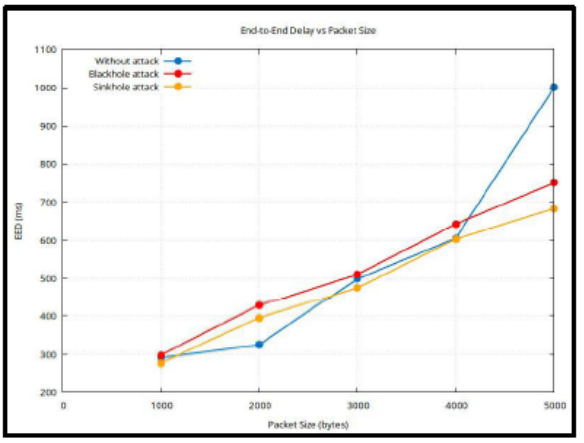

Fig. 8. End-to-End Delay (EED) vs. Packet Sizes

Fig. 8 illustrates that the End-to-End Delay (E2ED) increases proportionally with packet size across all evaluated scenarios. Under normal operating conditions (no-attack), the delay is notably higher, particularly as the payload size increases. Interestingly, the data shows that E2ED is slightly lower under Blackhole and Sinkhole attacks.

This phenomenon occurs because malicious nodes either discard or redirect packets prematurely, thereby truncating the total transmission time within the network. However, this reduction in latency does not signify improved performance; rather, it is a byproduct of severe packet loss and misrouting. Among the two malicious scenarios, the Sinkhole attack exhibits a marginally lower delay than the Blackhole attack. Ultimately, the reduced E2ED observed during these attacks is a misleading metric that reflects abnormal packet handling rather than network efficiency.

https://doi.org/10.24191/jcrinn.v11i2.580

c. Packet Delivery Ratio (PDR) vs. Packet Sizes:

Fig. 9 illustrates that the Packet Delivery Ratio (PDR) decreases as packet size increases across all evaluated scenarios. Under normal conditions (no-attack), the PDR remains consistently high, peaking above 95% for smaller packets before experiencing a gradual decline. In contrast, both Blackhole and Sinkhole attacks significantly reduce the PDR, with the impact becoming more pronounced as packet sizes increase

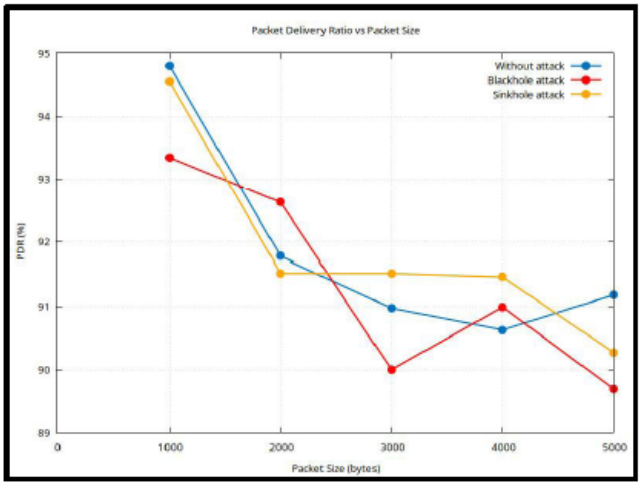

Fig. 9. Packet Delivery Ratio (PDR) vs. Packet Sizes

The Blackhole attack exhibits the poorest performance, primarily due to the malicious node's mechanism of discarding all intercepted packets. While the Sinkhole attack performs slightly better than the Blackhole scenario, it still results in substantial delivery degradation. These results indicate that both attacks severely compromise data reliability in VANETs especially as payloads grow thereby threatening network efficiency and communication integrity. In conclusion, the PDR is negatively correlated with both packet size and the presence of routing attacks, with the Sinkhole attack causing a particularly severe collapse in delivery rates at larger packet sizes.

https://doi.org/10.24191/jcrinn.v11i2.580

d. Routing Overhead vs Packet Size

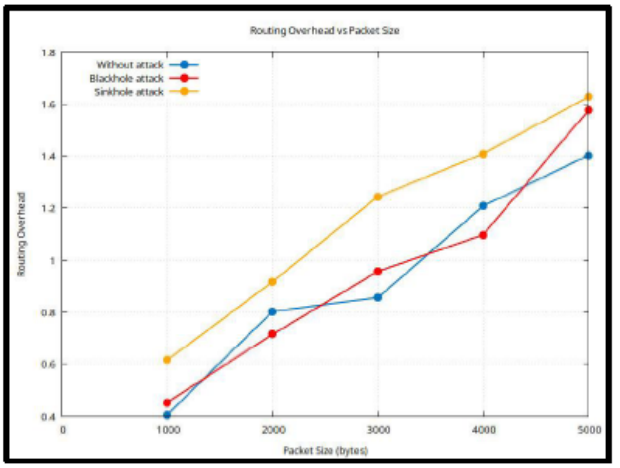

Fig. 10. Routing Overhead (RO) vs Packet Size

Fig. 10 illustrates that routing overhead (RO) increases in proportion to packet size across all evaluated scenarios. Under normal conditions (no attack), the overhead remains minimal and stable. In contrast, Blackhole and Sinkhole attacks significantly inflate routing overhead, with Sinkhole attacks exerting the most substantial impact.

This surge is primarily attributed to the propagation of fraudulent route advertisements, which trigger an excessive volume of routing control messages. Blackhole attacks similarly increase overhead by enticing and subsequently discarding packets, forcing the network to initiate redundant discovery processes. As packet sizes increase, the disruptive effects of both attacks become more pronounced, further straining network resources. In conclusion, routing efficiency in VANETs is severely compromised under these malicious conditions particularly in the presence of Sinkhole attacks—underscoring the critical need for robust security mechanisms to maintain optimal network performance and minimize control traffic.

5. CONCLUSION

The study establishes a clear benchmark for Blackhole and Sinkhole attacks degrade VANET performance using the AODV routing protocol. It quantifies degradation across four key metrics (throughput, PDR, EED and routing overhead) under varying node densities (20–100) and packet sizes (1000–5000 bytes)**.** By integrating NS-2 with SUMO and OpenStreetMap, the study creates a realistic vehicular mobility environment (2100 m × 1800 m urban area). This combination allows accurate modelling of traffic dynamics and attack propagation, bridging the gap between pure network simulation and real-world driving patterns.

This study provides a systematic comparative analysis of Blackhole and Sinkhole attacks on AODV. Both attacks significantly degrade performance, but with distinct profiles. Blackhole attacks cause consistent packet dropping, increasing routing overhead by 29% and delay by 23% at moderate densities. Sinkhole attacks exhibit "deceptive efficiency maintaining near-normal throughput at low densities but collapsing sharply at high densities, reducing throughput by 31% and PDR by 5.4% at 100 nodes. Notably, end-to-end delay appears lower under attacks, but this is misleading packets are dropped prematurely, not delivered efficiently.

https://doi.org/10.24191/jcrinn.v11i2.580

The research conclusively demonstrates that Sinkhole attacks pose a greater threat than Blackhole attacks in dense urban VANET environments due to their deceptive nature and catastrophic high-density collapse. The work establishes essential performance benchmarks for future adaptive, attack-resistant routing protocols. However, translation to real-world deployment requires validation beyond simulation and expansion to multi-protocol, multi-attack scenarios. For ITS safety, priority should be given to developing lightweight, real-time Sinkhole detection mechanisms for high-density vehicular networks.

3. ACKNOWLEDGEMENTS/FUNDING

The authors would like to acknowledge the support of lecturers and staffs from Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA(UiTM) Cawangan Perlis, Malaysia for providing the facilities and support on this research.

4. CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial or financial conflicts and declare the absence of conflicting interests with the funders.

5. AUTHORS' CONTRIBUTIONS

Adib Adza Aktar: Conceptualisation, methodology, testing and simulation writing-original; **Ahmad Yusri Dak**: Conceptualisation, supervision, writing- review and editing and validation.

6. REFERENCES

Ajjaj, S., El Houssaini, S., Hain, M., & El Houssaini, M. A. (2022). A new multivariate approach for real time detection of routing security attacks in VANETs. *Information (Switzerland)*, *13*(6). https://doi.org/10.3390/info13060282.

Bani Younes, M., & Boukerche, A. (2015). A performance evaluation of an efficient traffic congestion detection protocol (ECODE) for intelligent transportation systems. *Ad Hoc Networks*, *24*, 317–336. https://doi.org/https://doi.org/10.1016/j.adhoc.2014.09.005.

Dak A.Y., S. Y. and M. K. (2012). A literature survey on security challenges in VANETs. *International Journal of Computer Theory and Engineering,* *4*(6), 1007–1010. https://doi.org/10.7763/IJCTE.2012.V4.627.

Dak, A. Y., Mohd Azmir, M., Ruslan, R., & Mohd Radzi, N. A. (2025). VANET traffic simulation for blackhole attack detection using AODV routing protocol. *Journal of Information System and Technology Management*, *10*(38), 134–146. https://doi.org/10.35631/jistm.1038009.

Kugali, S. N., & Kadadevar, S. (2020). Vehicular ADHOC Network (VANET): A brief knowledge. *International Journal of Engineering Research & Technology (IJERT)*. https://doi.org/http://dx.doi.org/10.17577/IJERTV9IS060784.

Kudrenko, S. O., & Stoliar, A. L. (2025). Security mechanisms for AODV and E-AODV protocols against black hole and gray tunnel attacks. *Problems of Informatization and Management*, *1*, 119–125. https://doi.org/10.18372/2073-4751.81.20137.

Madani, A., Lashari, S., Uddin, S., Khan, A., Atta, M., & Ramli, D. (2025). detecting black hole attack using support vector machine with XGBoosting in mobile ad-hoc networks. *Journal of Informatics and Web Engineering*, *4*. https://doi.org/10.33093/jiwe.2025.4.2.13.

https://doi.org/10.24191/jcrinn.v11i2.580

Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J.-T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. *Sensors*, *22*(5). https://doi.org/10.3390/s22051897.

Muthusamy, A., P. L. D. M. and R. R. (2025). IDPSA: An improved detection and prevention source authentication of black hole attack in VANETS. (2025). *ICTACT Journal on Communication Technology*, *16*(2), 3485–3490. https://doi.org/10.21917/ijct.2025.0518.

Parida, D., Bhanja, U., & Okade, M. (2024). Sink-hole attack detection in VANET using machine learning techniques. In *2024 6th International Conference on Computational Intelligence and Networks (CINE)*, 1–6. https://doi.org/10.1109/CINE63708.2024.10880882.

Waoo, A., & Tiwari, V. (2021). Challenges in sinkhole attack detection in wireless sensor network. *Indian Journal of Data Communication and Networking*, *1*, 1–7. https://doi.org/10.54105/ijdcn.C5016.081421.

https://doi.org/10.24191/jcrinn.v11i2.580