JCRINN
Journal of Computing Research and Innovation
e-ISSN : 2600-8793

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

Journal of Computing Research and Innovation 10(2) 2025

Journal of Computing Research and Innovation

Impact of Blackhole and Wormhole Attacks on DSDV Routing Protocol in VANET: Behavioural Analysis

Ahmad Yusri Dak[1*], Nuramarina Nasruddin[2], Nur Khairani Kamarudin[3]

[1,2,3]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perlis Branch, Arau Campus, 02600 Arau Perlis, Malaysia.*

ARTICLE INFO

Article history:
Received 16 March 2025
Revised 28 May 2025
Accepted 1 July 2025
Published 1 September 2025

Keywords:
VANET
Blackhole
Wormhole
DSDV
SUMO

DOI:
10.24191/jcrinn.v10i2.516

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) play a crucial role in Intelligent Transportation Systems (ITS) and the advancement of intelligent vehicles, enabling seamless and reliable communication between vehicles and infrastructure. This communication supports real-time applications such as collision avoidance, traffic control, and driver assistance. However, due to their dynamic topology and open-access medium, VANETs are highly vulnerable to security threats, particularly blackhole and wormhole attacks, which can disrupt data routing and severely degrade network performance. Despite the growing importance of VANETs, there is a limited number of studies that specifically examine the impact of blackhole and wormhole attacks on the Destination-Sequenced Distance-Vector (DSDV) routing protocol. This research addresses that gap by evaluating VANET performance under three conditions: no attack, a blackhole attack, and a wormhole attack. Key performance metrics including Packet Delivery Ratio (PDR), throughput, End-to-End Delay (EED), and Routing Overhead (RO) are analysed across various node densities using NS-2.35 and SUMO 1.18.0. Notably, the results show a 76.9% decline in throughput under the wormhole attack compared to the baseline scenario, highlighting the significant performance degradation caused by such threats. Overall, this study provides valuable quantitative insights into the vulnerabilities of VANETs and underscores the urgent need for more secure and resilient routing protocols to defend against these emerging attacks.

1. INTRODUCTION

In recent years, Vehicular Ad Hoc Networks (VANETs) have gained prominence in data transmission. They are increasingly used in Intelligent Transportation Systems (ITS) to support drivers, passengers, and services such as accident alerts and driver assistance systems (Mahmood et al., 2021). In addition, VANETs play a crucial role in safety applications by enabling communication between vehicles and roadside infrastructure. However, despite offering significant advantages for enhancing user safety, VANETs also

[1*] Corresponding author. *E-mail address*: ahmadyusri@uitm.edu.my

https://doi.org/10.24191/jcrinn.v10i2.516

pose various security challenges due to their open-access medium, high vehicle mobility, and dynamic topology changes. These characteristics result in a network topology that is highly dynamic and distinct, necessitating the use of efficient routing protocols. Reliable connectivity between vehicles and infrastructure is essential for effective communication, particularly under constantly changing network conditions, to ensure timely and accurate data transmission. In large-scale networks like VANETs, the Destination Sequenced Distance Vector (DSDV) protocol is effective as it offers loop-free routes using sequence numbers, employs proactive updates to prevent delays, and uses incremental updates to reduce overhead—advantages over other popular protocols such as AODV and DSR (El-Dalahmeh et al., 2024). In this study, the DSDV protocol periodically broadcasts its routing table to direct neighbours to maintain consistency in a rapidly changing topology (Sahoo & Tripathy, 2023). DSDV is based on the Bellman-Ford algorithm, where mobile nodes are required to broadcast their routing entries to nearby nodes (Alifo et al., 2023a).

Despite advancements in routing protocols for VANET security, inherent vulnerabilities persist, particularly concerning deception through false routing information disseminated by malicious nodes. These weaknesses can give rise to significant security threats, including blackhole and wormhole attacks, which compromise the reliability and integrity of VANET communications and hinder the implementation of real-time, dependable traffic management. A blackhole attack is a type of Denial of Service (DoS) in which a malicious node deceives other nodes by advertising the shortest path to a non-existent destination, thereby attracting and intercepting data transmissions. Once the data packets are routed through the attacker, they are simply dropped without notification, creating a "hole" in the communication pathway and preventing the data from reaching its intended recipient (Mahmood et al., 2021). Such disruptions can lead to delayed or lost safety-critical messages, such as collision alerts, ultimately degrading the performance and security of VANETs and increasing the risk of traffic congestion, accidents, and fatalities (Malik et al., 2022).

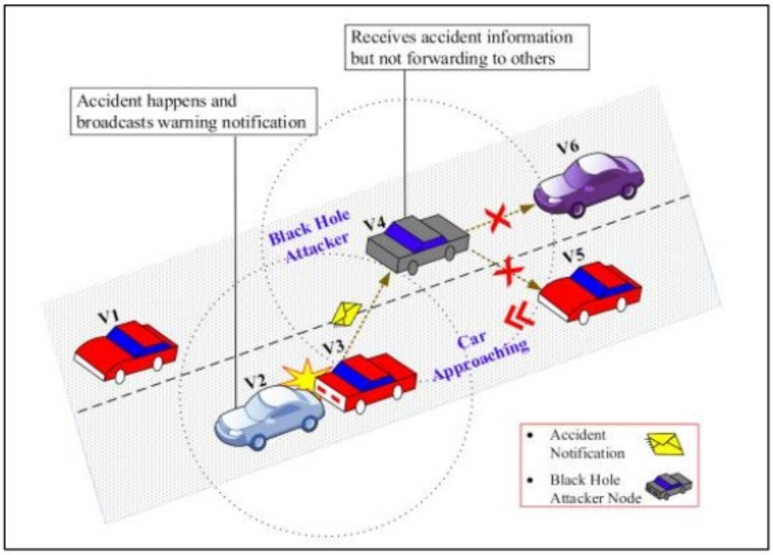

Receives accident information but not forwarding to others
Accident happens and broadcasts warning notification
V6
Black Hole Attacker
V4
V5
V1
V3
V2
Car Approaching
Accident Notification
Black Hole Attacker Node

Fig. 1. Illustration of blackhole attack on VANET

Fig. 1 illustrates how a blackhole attack can affect communication in a VANET scenario. In this case, vehicle V3 collides with vehicle V2 and sends an alert message to vehicle V4, which happens to be a malicious node. Instead of forwarding the alert to nearby vehicles V5 and V6, vehicle V4 drops the message

https://doi.org/10.24191/jcrinn.v10i2.516

entirely. This disruption could prevent other vehicles from receiving critical safety information in time, potentially leading to additional accidents or increased traffic congestion. In comparison, a wormhole attack is even more dangerous. Unlike the blackhole attack, which simply drops packets, the wormhole attack targets the routing layer and can bypass typical security measures such as cryptographic protections (Bhatti et al., 2024). It works by creating a tunnel between two colluding malicious nodes, allowing them to establish a shortcut in the network with a deceptively low hop count. This false route is then recorded in the routing tables, tricking legitimate nodes into using it (Asra, 2022). As a result, data can be intercepted, manipulated, or misrouted which leading to information theft, delays, or even complete breakdowns in communication (Bhatti et al., 2024). While these attacks don't block network channels directly, they severely disrupt the flow of information, affecting the core functionality and safety of VANET systems. Given these threats, this research seeks to simulate and analyse the performance of VANETs under blackhole and wormhole attacks using the DSDV routing protocol. The goal is to better understand how these attacks degrade network performance and to provide insights that can help automotive developers, researchers, and users design more secure and resilient communication systems for intelligent transportation.

2. RELATED WORK

In recent years, security has become a growing concern in both Vehicular Ad-Hoc Networks (VANETs) and Mobile Ad-Hoc Networks (MANETs), especially due to their vulnerability to various forms of cyberattacks. Among the most critical threats are blackhole and wormhole attacks, which can severely disrupt communication and degrade network performance. Several researchers (Al Rubaiei et al., 2022; Kaur & Kumar, 2018; Reshi et al., 2024) have explored these attack types and proposed different strategies to mitigate their effects. This section reviews recent studies that examine blackhole, wormhole, and greyhole attacks, with a focus on how well different routing protocols and detection methods perform under such conditions.

For example, Kumar et al. (2021) tackled the issue of blackhole attacks in VANETs by enhancing the AODV routing protocol. Their proposed solution involved improving the Route Request (RREQ) and Route Reply (RREP) processes and incorporating a cryptographic mechanism to verify node legitimacy. Using NS-2 simulations, they measured metrics such as Packet Loss Ratio (PLR), Packet Delivery Ratio (PDR), routing overhead, and End-to-End Delay (EED). Their findings showed that the enhanced protocol successfully detected and isolated malicious nodes, which led to improved delivery rates and overall network performance. In a similar line of study, Alifo et al. (2023b) evaluated how both AODV and Dynamic Source Routing (DSR) perform under blackhole attack conditions in MANETs. Their analysis revealed that AODV was more efficient in terms of energy consumption and delivery ratio, while DSR achieved better throughput. These results emphasize that the choice of routing protocol can significantly influence a network's resilience to attack, depending on the specific performance requirements. On the other hand, a study by Alifo et al. (2023a) focused on wormhole attacks and assessed their impact on DSDV, DSR, and TORA protocols in MANETs. The study found that DSDV and TORA were particularly vulnerable, with zero data delivery in some cases, while DSR offered relatively better protection, maintaining a modest PDR and higher throughput. This highlights the seriousness of wormhole attacks and the importance of developing robust mitigation strategies.

Another interesting approach was presented by Kaur et al. (2022), who addressed the less studied greyhole attack in VANETs. This type of attack involves selectively dropping or altering packets, making it harder to detect. The proposed detection mechanism used a three-phase method involving initialization, malicious node simulation, and system-wide broadcasts for detection. The approach led to significant improvements in both PDR and throughput, although it focused solely on greyhole attacks, leaving room for further research on more complex or combined threats. Lastly, Masruroh et al. (2022) studied blackhole and rushing attacks using the AOMDV routing protocol in a real-world traffic setting simulated with

https://doi.org/10.24191/jcrinn.v10i2.516

OpenStreetMap, SUMO, and NS-2. Their findings showed that both attack types degraded Quality of Service (QoS), with blackhole attacks having a more severe impact. This included lower throughput and delivery rates, along with increased packet loss and delay. What sets this current study apart is its focus on the DSDV routing protocol in a VANET environment, which has been less commonly explored. Unlike prior work that often centers on AODV or DSR in MANET settings, this research uses a more VANET-specific approach by incorporating realistic urban mobility simulations through SUMO and NS-2. It also evaluates the performance of DSDV under both blackhole and wormhole attacks, across different node densities (10 to 50 nodes). Notably, the results reveal a dramatic 76.9% drop in throughput under wormhole attacks, an insight not often highlighted in previous research. By comparing attack scenarios with a baseline (no-attack) condition, this study offers a clearer picture of how DSDV holds up under real-world VANET challenges, providing valuable input for future protocol development and security enhancement. Table 1 summarises the key findings, objectives, and limitations of the related work reviewed in this study.

Table 1. Summary of Related Work

Author	Issue	Research Objectives	Limitation and Results
(Kumar et al., 2021)	VANET and traditional AODV routing protocols are susceptible to blackhole attacks.	To propose a secure AODV routing protocol to detect and mitigate blackhole attacks in VANET	• Effectively detects and isolates malicious nodes, leading to a reduction in PLR.
(Alifo et al., 2023b)	Blackhole attacks in MANET can disrupt network services by dropping packets.	To evaluate the performance of AODV and DSR under blackhole attack	• DSR shows higher throughput, while AODV has better PDR and residual energy.
(Alifo et al., 2023a)	Wormhole attacks can severely compromise the integrity and efficiency of data transmission in MANET.	To simulate and evaluate the performance of different routing protocols (DSDV, DSR, TORA) under wormhole attack.	• Zero data transmission and PDR in DSDV and TORA. • Higher throughput and PDR, but with a slight delay in DSR.
(Kaur et al., 2022)	Greyhole attacks randomly modify and discard packets making it difficult to detect in VANET.	To propose the detection and prevention mechanism of AODV routing protocol under greyhole attack in VANET	• Effectively prevent the attack leading to a better result in PDR and throughput.
(Masruroh et al., 2022)	Blackhole and rushing attacks can disrupt VANET data communication.	To analyse and compare the effects of black hole and rushing attacks on VANET using AOMDV	• Blackhole attack results in lower throughput and PDR, higher PLR, and increased EED compared to rushing attack.

3. METHODOLOGY

In this research, the NS-2 simulator is used to model a VANET environment and analyse its behavior under different scenarios. The simulations vary the number of nodes (10, 20, 30, 40, and 50) to represent different levels of traffic congestion within a network area of 1000 × 1000 square meters. Table 2 outlines the simulation parameters, providing a detailed overview of the setup, configurations, and experimental conditions. By using NS-2, the study aims to gain deeper insights into the performance characteristics of VANETs, particularly in the presence of blackhole and wormhole attacks. The selected parameters were chosen to reflect realistic urban conditions and are consistent with standard values commonly used in VANET research.

https://doi.org/10.24191/jcrinn.v10i2.516

Table 2. Network Parameter

Parameter	Value
Simulator	NS-2.35
Mobility Model	SUMO Mobility (based on imported OSM map)
Routing Protocol	DSDV
Number of nodes	10, 20, 30, 40 and 50
Packet Size	1500 bytes
Simulation Time (s)	30, 60, 90, 120, and 150
Terrain Size (m)	1200 x 1400
Malicious Activity	Wormhole: 2 nodes Blackhole: 1 node
Performance Metric	EED, Throughput, PDR and Routing Overhead

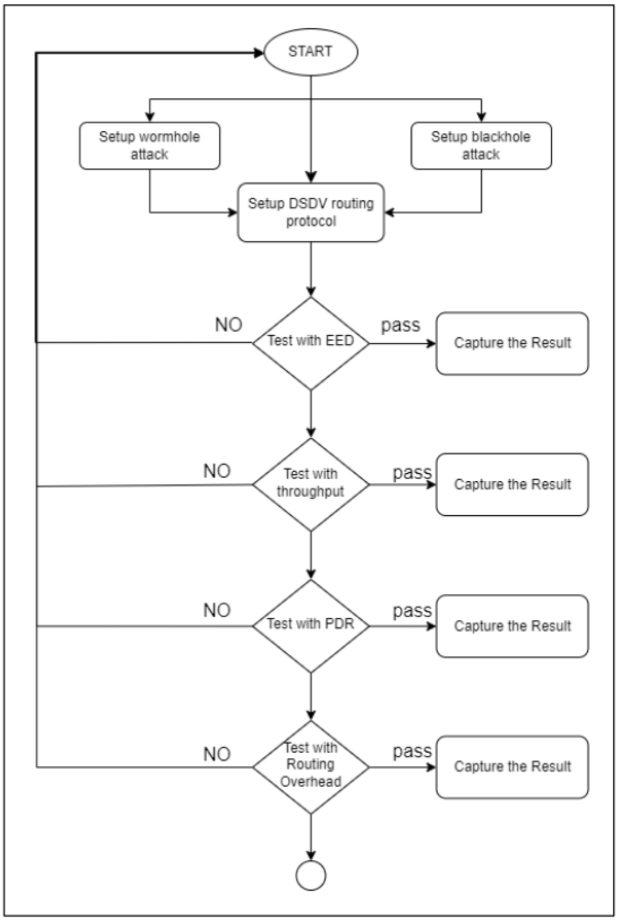


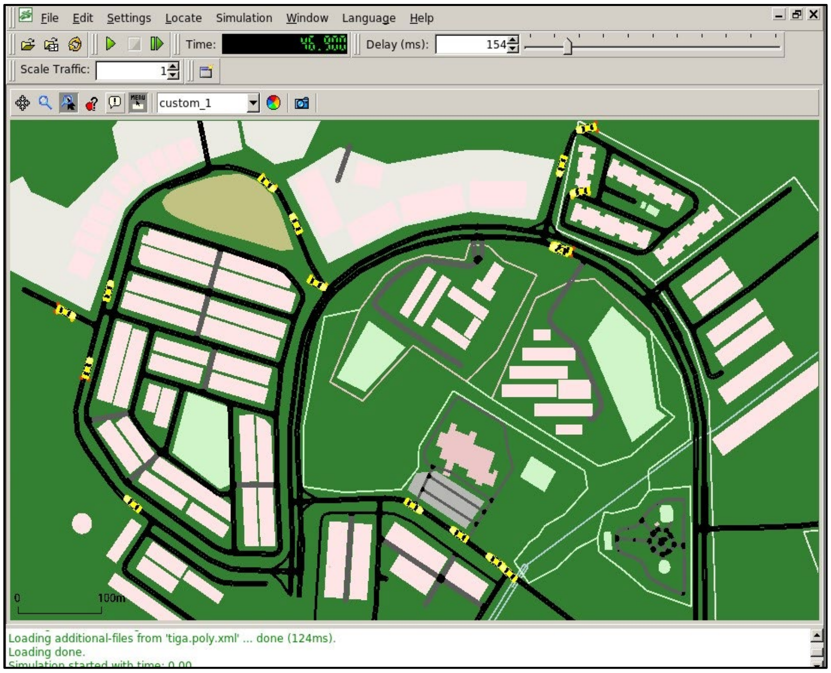
Fig. 2. Process flow for simulation phase

Fig. 2 shows the overall process used during the simulation phase of this research. To evaluate the network behaviour, each scenario was simulated using NS-2 for the networking components and SUMO to model realistic traffic flow and vehicle mobility. The research was carried out under three different

https://doi.org/10.24191/jcrinn.v10i2.516

conditions: a baseline scenario with no attacks, a scenario involving a single blackhole node disrupting communication, and a third scenario where two wormhole nodes form a tunnel to manipulate data routing. The performance of each setup was assessed based on four main metrics: End-to-End Delay (EED), throughput, Packet Delivery Ratio (PDR), and routing overhead. Data collected from each simulation was then analysed to understand how these attacks impact overall VANET performance.

Fig. 3 displays the SUMO graphical user interface (GUI), which visualizes traffic flow and vehicle movements on a map imported from OpenStreetMap (OSM). This setup reflects realistic mobility patterns, helping to ensure the accuracy and relevance of the simulation results.



```
Loading additional-files from 'tiga.poly.xml' ... done (124ms).
Loading done.
Simulation started with time: 0.00
```

Fig. 3. SUMO-GUI

4. RESULT AND ANALYSIS

Results and analysis section is a critical part of this research, as it presents and interprets the findings from simulations aimed at evaluating the impact of blackhole and wormhole attacks on the DSDV routing protocol in a VANET environment. The analysis focuses on four key performance metrics: Packet Delivery Ratio (PDR), throughput, End-to-End Delay (EED), and Routing Overhead (RO). These metrics were chosen to offer a well-rounded view of the network's behaviour under both normal conditions and in the presence of malicious attacks. Results are presented using a comparative approach, contrasting the baseline performance of DSDV (without attacks) against its performance under blackhole and wormhole attack scenarios. This comparison helps to identify specific vulnerabilities within VANETs and assess the extent to which each type of attack degrades overall network performance.

https://doi.org/10.24191/jcrinn.v10i2.516

4.1 Packet Delivery Ratio vs Number of Nodes

Fig. 4 illustrates how the Packet Delivery Ratio (PDR) changes as the number of nodes increases under three scenarios: without attack, with a blackhole attack, and with a wormhole attack. In the no-attack scenario, the PDR remains consistently high, ranging from approximately 98.7% to 99%, which reflects a stable and efficient network. Minor decreases in PDR at higher node counts can be attributed to increased congestion and packet collisions, but overall, the system performs reliably.

In contrast, both attack scenarios lead to noticeable reductions in PDR. The blackhole attack has a more significant impact, particularly as the network grows. At 30 nodes, for instance, the PDR drops to 95.56%, a decline of about 2.94% compared to the no-attack case (98.5%). This drop is due to the blackhole node attracting data by falsely advertising optimal routes and then discarding the packets, leading to direct data loss. Interestingly, the effect of the attack becomes less severe beyond 30 nodes, likely because the increased network density offers more alternate paths, reducing reliance on the malicious node. The wormhole attack also causes a decrease in PDR, but its impact is slightly less severe. At 30 nodes, the PDR falls to 95.55%, very close to the blackhole scenario. However, at 20 nodes, wormhole attacks result in a PDR of 97.35%, which is a smaller decline compared to the blackhole's 96.64%. This is because wormhole attacks typically involve tunneling packets between distant nodes, which disrupts routing paths but doesn't necessarily result in packet loss. As a result, some data still reaches its destination, maintaining a relatively higher PDR.

In summary, both attack types degrade network performance, but blackhole attacks are more damaging due to their tendency to drop packets entirely, while wormhole attacks primarily introduce routing inefficiencies that still allow some data to be delivered.

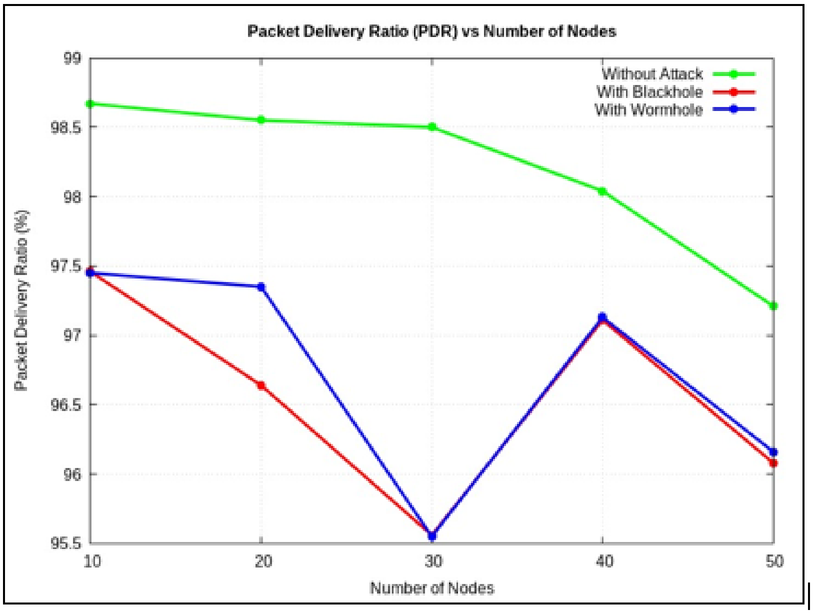


Fig. 4. Packet Delivery Ratio (PDR) vs Number of Nodes

4.2 Throughput vs Number of Nodes

Fig. 5 shows the variation in throughput as the number of nodes increases under three scenarios: without attack, with a blackhole attack, and with a wormhole attack. In the no-attack scenario, throughput

https://doi.org/10.24191/jcrinn.v10i2.516

remains relatively high and stable, especially at lower node densities (10–20 nodes), where it reaches around 760 kbps. This performance reflects efficient data transmission and network operation under normal conditions, thanks to the proactive nature of the DSDV routing protocol. However, as node density increases, throughput declines to about 254.71 kbps due to greater congestion and competition for the shared wireless medium.

The blackhole attack has a dramatic impact, particularly at 20 nodes, where throughput drops sharply to 141.02 kbps, an 81.4% reduction compared to the baseline. This decline occurs because malicious nodes attract data traffic by advertising false routes, then drop the packets instead of forwarding them, leading to significant data loss. Although the impact is slightly less at other node levels, throughput consistently suffers under blackhole conditions. Wormhole attacks also degrade throughput, especially at 30 nodes, where it falls to 79.15 kbps, representing a 69% drop from the baseline. Unlike blackhole attacks, wormholes misroute packets through unauthorized shortcuts between colluding nodes, which causes routing inefficiencies and potential loops. Although some data still reaches its destination, the detoured paths consume more bandwidth and increase delays, thereby reducing overall throughput.

In summary, both types of attacks reduce network throughput, but blackhole attacks have a more severe effect due to direct packet drops, whereas wormhole attacks cause routing disruptions that moderately impact data delivery efficiency.

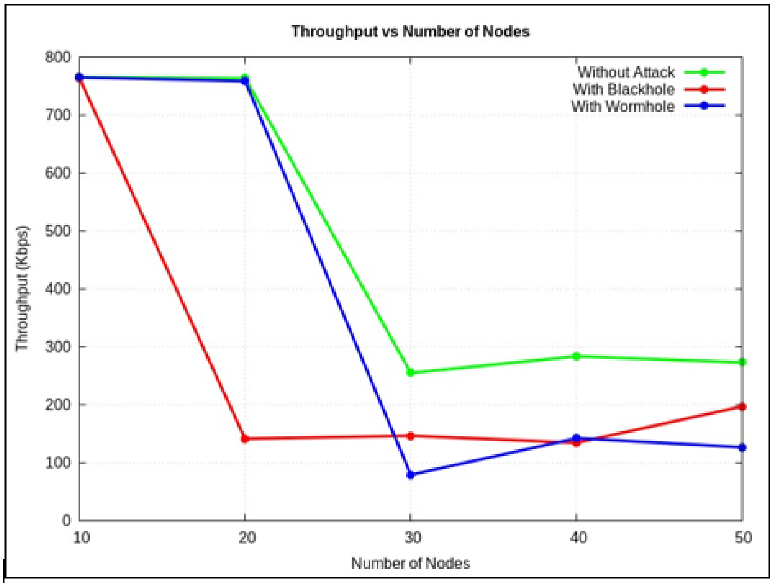


Fig. 5. Throughput vs Number of Nodes

4.3 End to End Delay (EED) vs Number of Nodes

Fig. 6 shows how End-to-End Delay (EED) changes as the number of nodes increases in three different scenarios: without any attack, with a blackhole attack, and with a wormhole attack. In the no-attack scenario, EED generally rises from 10 to 30 nodes, likely because more nodes in the network create congestion and delays as they compete to send data. Interestingly, the delay drops at 40 nodes, which might be due to a change in traffic flow or network structure during that simulation. However, at 50 nodes, the delay increases again, suggesting that higher congestion returns as the network becomes denser.

https://doi.org/10.24191/jcrinn.v10i2.516

When a blackhole attack is present, the delay becomes noticeably higher—especially at 10 nodes, where it jumps from 132.193 ms to 181.262 ms, a 37.1% increase. This happens because data packets are drawn toward the malicious node and then dropped, forcing the network to try retransmitting the data, which takes more time. At 20 nodes, there's a slight and unexpected drop in EED compared to the no-attack case. This might be due to the blackhole node not actively participating in routing during that run, which could have reduced congestion by chance. While not typical, it shows how certain network conditions can sometimes reduce the visible impact of an attack. For the wormhole attack, the impact on EED is more mixed. At 10 and 20 nodes, there's a moderate increase in delay, as expected, because the attack disrupts normal routing. But at 30 nodes, the EED actually goes down. This could be because the wormhole creates a shortcut between distant nodes, reducing the number of hops and resulting in quicker data delivery in some cases.

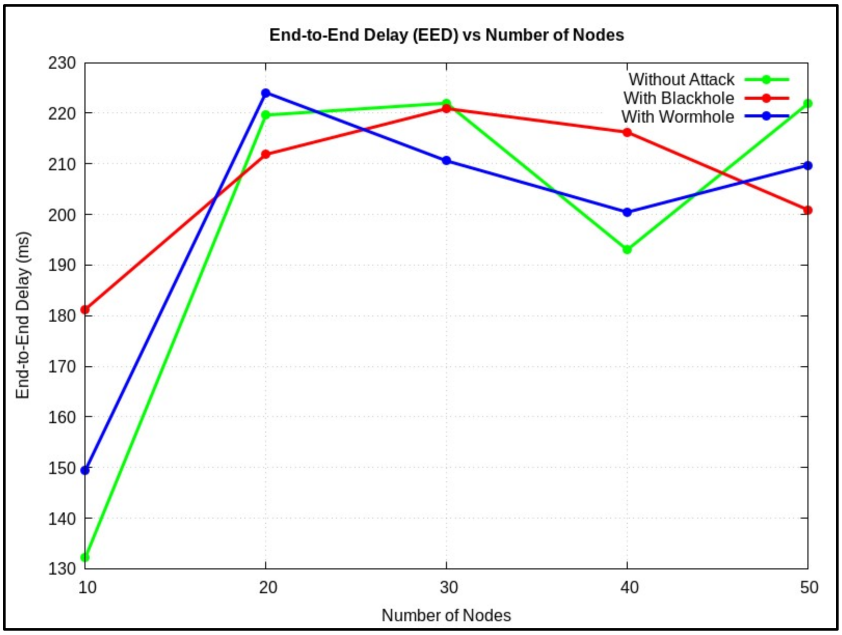


Fig. 6. End to End Delay (EED) vs Number of Nodes

4.4 Routing Overhead (RO) vs Number of Nodes

Fig. 7 illustrates how routing overhead changes with the number of nodes across different scenarios. In the no-attack scenario, the overhead increases gradually as the network grows. This is expected, as more nodes require more frequent routing updates and control messages to maintain connectivity and accurate routing tables. The DSDV protocol handles this growth efficiently, resulting in a steady but manageable rise in overhead, especially noticeable between 20 to 30 nodes and again from 40 to 50 nodes, reflecting the added complexity of a larger network.

When a blackhole attack is introduced, the routing overhead increases sharply. At 30 nodes, it spikes from 12.679 to 31.741, a jump of roughly 150 percent. This happens because the malicious node frequently advertises false routes, causing the network to constantly recalculate paths and send more control messages. Interestingly, at 50 nodes, the overhead actually drops below the no-attack level. This may be due to the network becoming dense enough to naturally route around the malicious node, reducing the disruption. The wormhole attack also raises routing overhead, but not as dramatically. At 30 nodes, it climbs to 22.317,

https://doi.org/10.24191/jcrinn.v10i2.516

around a 76 percent increase, mainly due to routing inconsistencies and loops created by the attack's shortcuts. However, by the time the network reaches 50 nodes, the overhead from wormhole attacks becomes the highest of all three scenarios. This suggests that in very dense networks, the confusion caused by the wormhole grows more severe, leading to more control traffic as the protocol tries to resolve these routing issues.

In summary, both attack types disrupt normal routing and increase overhead. Blackhole attacks have a more immediate and dramatic impact due to frequent false route advertisements, while wormhole attacks cause more gradual but still significant increases, especially as the network becomes more complex.

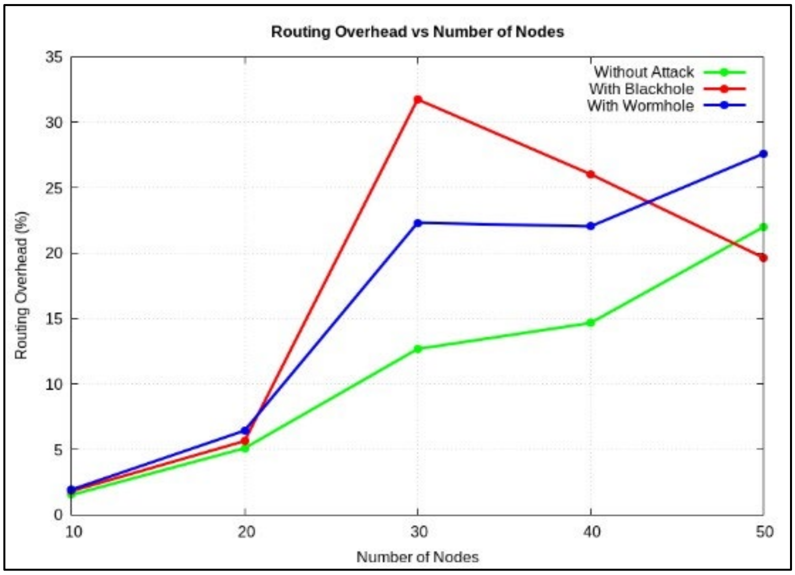


Fig. 7. End to End Delay (EED) vs Number of Nodes

5. CONCLUSION

This research provides meaningful insights into the performance and resilience of VANETs when subjected to blackhole and wormhole attacks, using the DSDV routing protocol as a baseline. The findings clearly show how these attacks can significantly impact key network metrics: namely Packet Delivery Ratio (PDR), throughput, End-to-End Delay (EED), and Routing Overhead (RO).

Under normal conditions, without any attacks, the network performs reliably. High PDR, stable throughput, and manageable delay and overhead highlight DSDV's effectiveness in maintaining communication in a dynamic VANET environment. However, when blackhole or wormhole attacks are introduced, this stability quickly breaks down. Blackhole attacks are particularly harmful, as malicious nodes drop packets outright, leading to sharp declines in PDR and throughput, increased delays, and a surge in routing overhead from constant path recalculations. Wormhole attacks, while slightly less destructive in terms of packet loss, still create serious disruptions by introducing false routes and increasing routing overhead, especially in denser networks. Interestingly, the results also show that blackhole attacks become somewhat less effective as the number of nodes increases, since the network can reroute data through alternative paths. In contrast, wormhole attacks tend to become more disruptive in larger networks due to the growing complexity of routing anomalies.

https://doi.org/10.24191/jcrinn.v10i2.516

These findings highlight the urgent need for stronger security mechanisms in VANETs. By identifying how and where vulnerabilities occur, this research offers practical guidance for automakers, researchers, and developers aiming to build more secure and resilient vehicular networks. Future work could explore improvements to the DSDV protocol or assess alternative routing strategies better equipped to resist these types of attacks. Ultimately, this study reinforces the importance of balancing performance and security in the future of intelligent transportation systems.

6. ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of Course Coordinator (Mrs Rafiza Ruslan), Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara (UiTM) Cawangan Perlis, Arau, Perlis, Malaysia for providing the facilities, guidance and moral support on this research.

7. 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.

8. AUTHORS' CONTRIBUTIONS

Ahmad Yusri Dak: Conceptualisation, methodology, formal analysis, visualization, investigation, data curation, writing-original draft, references; **Nuramarina Nasruddin**: Conceptualisation, funding acquisition, methodology, validation and writing – review & editing**; Nur Khairani Kamarudin**: validation and writing – review & editing.

9. REFERENCES

Al Rubaiei, M. H., Jassim, H. S., & Sharef, B. T. (2022). Performance analysis of black hole and worm hole attacks in MANETs. *International Journal of Communication Networks and Information Security (IJCNIS), 14*(1). https://doi.org/10.17762/ijcnis.v14i1.5078

Alifo, F., Doe, M., & Yakubu, M. A. (2023a). Wormhole attack vulnerability assessment of MANETs: Effects on routing protocols and network performance. *International Journal of Computer Applications, 185*(48), 24-29. https://doi.org/10.5120/ijca2023923312

Alifo, F., Yakubu, M. A., Doe, M., & Asante, M. (2023b). Performance analysis of AODV and DSR routing protocols under blackhole attack using NS-2. *Computer Science & Information Technology,* 485-496. https://doi.org/10.5121/csit.2023.131339

Asra, S. A. (2022). Security issues of vehicular ad hoc networks (VANET): A systematic review. *TIERS Information Technology Journal, 3*(1), 17–27. https://doi.org/10.38043/tiers.v3i1.3520

Bhatti, D. S., Saleem, S., Imran, A., Kim, H. J., Kim, K., & Lee, K. (2024). Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions. *Scientific Reports, 14*, 3428. https://doi.org/10.1038/s41598-024-53938-9

El-Dalahmeh, M., El-Dalahmeh, A., & Adeel, U. (2024). Analysing the performance of AODV, OLSR, and DSDV routing protocols in VANET based on the ECIE method. *IET Networks, 13*(5–6), 377–394. https://doi.org/10.1049/ntw2.12136

https://doi.org/10.24191/jcrinn.v10i2.516

Kaur, G., Khurana, M., & Kaur, A. (2022). Gray hole attack detection and prevention system in vehicular adhoc network (VANET). In *3rd International Conference on Computing, Analytics and Networks (ICAN)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICAN56228.2022.10007192

Kaur, T., & Kumar, R. (2018). Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using AODV protocol. In *IEEE International Conference on Smart Energy Grid Engineering (SEGE)* (pp. 288–292). IEEE. https://doi.org/10.1109/SEGE.2018.8499473

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. D. A., Panigrahi, B. K., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems, 80*, 103352. https://doi.org/10.1016/j.micpro.2020.103352

Mahmood, J., Duan, Z., Yang, Y., Wang, Q., Nebhen, J., & Bhutta, M. N. M. (2021). Security in vehicular ad hoc networks: Challenges and countermeasures. *Security and Communication Networks, 2021*(1), 9997771. https://doi.org/10.1155/2021/9997771

Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. *Sensors, 22*(5), 1897. https://doi.org/10.3390/s22051897

Masruroh, S. U., Farghani, Y. S., Kusdaryono, A., Fiade, A., Putri, R. A., & Pratiwi, L. A. (2022). Comparative analysis of testing black hole attack and rushing attack on VANET (Vehicular Ad-Hoc Network) with AOMDV routing protocol. In *International Conference on Engineering and Emerging Technologies (ICEET)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICEET56468.2022.10007272

Reshi, I. A., Sholla, S., & Najar, Z. A. (2024). Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm. *Journal of Engineering Research, 12*(1), 133–139. https://doi.org/10.1016/j.jer.2024.01.014

Sahoo, A., & Tripathy, A. K. (2023). On routing algorithms in the internet of vehicles: A survey. *Connection Science, 35*(1), 2272583. https://doi.org/10.1080/09540091.2023.2272583