Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

VANET TRAFFIC SIMULATION FOR BLACKHOLE ATTACK DETECTION USING AODV ROUTING PROTOCOL

Ahmad Yusri Dak[1*], Musfira Mohd Azmir[2], Rafiza Ruslan[3] , Nor Azira Mohd Radzi[4]

[1] College of Computing, Informatics and Mathematics, UiTM Cawangan Perlis, 02600, Arau, Perlis, Malaysia
Email: ahmadyusri@uitm.edu.my
[2] College of Computing, Informatics and Mathematics, UiTM Cawangan Perlis, 02600, Arau, Perlis, Malaysia
Department of Account, Universiti Malaysia Kelantan, Malaysia
Email: musfira@gmail.com
[3] College of Computing, Informatics and Mathematics, UiTM Cawangan Perlis, 02600, Arau, Perlis, Malaysia
Department of Account, Universiti Utara Malaysia, Malaysia
Email: rafiza.ruslan@uitm.edu.my
[4] Academy of Language Studies, UiTM Cawangan Perlis, 02600, Arau, Perlis, Malaysia
Email: norazira202@uitm.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 14.01.2025
Revised date: 23.01.2025
Accepted date: 27.02.2025
Published date: 20.03.2025

To cite this document:

Dak, A. Y., Azmir, M. M., Ruslan, R., & Radzi, N. A. M. (2025). Vanet Traffic Simulation For Blackhole Attack Detection Using AODV Routing Protocol. *Journal of Information System and Technology Management, 10* (38), 134-146.

DOI: 10.35631/JISTM.1038009

Abstract:

Vehicular Ad-hoc Networks (VANETs) play a pivotal role in modern intelligent transportation systems by enabling seamless Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. However, their dynamic and decentralized nature exposes them to security vulnerabilities, particularly Blackhole attacks, where malicious nodes disrupt network operations by advertising false routes and dropping packets. This study evaluates the impact of Blackhole attacks on VANET performance using the Ad-hoc On-Demand Distance Vector (AODV) routing protocol. Simulations were conducted in NS-2 with BonnMotion mobility models, varying node densities (20–60 nodes) within a 1000×1000 m² area over 140 seconds to emulate urban traffic congestion. Key metrics such as End-to-End Delay (EED), Packet Delivery Ratio (PDR), Throughput, Goodput, and Packet Loss Rate (PLR) were analysed under normal and attack scenarios. Results revealed severe network degradation during attacks: EED surged by 63.43% (from baseline 175.05 ms), PLR exceeded 80% consistently, and PDR plummeted drastically (e.g., from 99.78% to 10.01% for 60 nodes). Throughput declined by up to 85% (e.g., 46.94 Kbps to 6.84 Kbps for 60 nodes), while Goodput exhibited similar deterioration due to malicious packet drops. Notably, higher node density exacerbated congestion and attack impacts, underscoring the vulnerability of scalable VANETs. The findings highlight the Blackhole attack's crippling effects on data reliability and real-time communication, critical for safety applications like emergency messaging and traffic

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

management. This study underscores the urgent need for robust mitigation strategies, including trust-based protocols, intrusion detection systems, and adaptive routing algorithms, to safeguard VANETs against such threats. By addressing these vulnerabilities, this research advances secure, efficient vehicular communication frameworks, ensuring the operational integrity and safety of future intelligent transportation ecosystems.

Keywords:

VANET, Blackhole, AODV, Metric, Goodput, Attack

Introduction

The increasing popularity of wireless connectivity in personal devices has opened opportunities for developing numerous apps and services that rely on the Internet and interoperability (Lee. K et al., 2022). Moreover, advancements in wireless communication technologies have significantly impacted our quality of life. These advancements have improved the reliability, speed, and accessibility of wireless networks, enhancing our ability to stay connected, access information, and communicate effectively. To improve the operational effectiveness of our transportation systems, it is imperative to increase the use of information technology (Oladimeji et al., 2023). Intelligent Transportation Systems or Smart Transportation is defined as "The application of advanced sensor, computer, electronics, and communication technologies, and management strategies in an integrated manner to improve the safety and efficiency of the surface transportation system"

VANET is employed in various applications, including highway automation, traffic management, and intelligent transportation systems because they offer many advantages over traditional communication systems (Lee. M & Atkison, 2021). These include increased scalability, robustness, and flexibility. VANET also provides more accurate and up-to-date information (Khan et al., 2021), allowing vehicles to be aware of potential hazards on the road, traffic conditions, and alternative routes. VANET communications exchange Global Positioning System (GPS) coordinates, traffic route information, and emergency messages between automobiles and nodes (Mistareehi et al., 2022). Furthermore, VANET minimizes emissions by letting vehicles communicate with one another and coordinate their motions, resulting in more efficient driving and, as a result, lower emissions (M. Lee & Atkison, 2021). VANET comprises intelligent nodes representing vehicles that may communicate with surrounding nodes and Roadside Units (RSU), called roadside infrastructure (Aziz, A., Samad, F., & Siddiqui, 2002). As the VANET depends on wireless communication channels and does not depend on a fixed infrastructure, it will be vulnerable to threats such as the Blackhole, Wormhole, and Sybil attacks. This study has focused on the Blackhole attack, as it is a type of malicious attack where a rogue node can intercept data packets and cause disruption or manipulation of data. This can have devastating consequences, such as the potential to hijack vehicles, disrupt communication between vehicles, or cause a denial of service to the entire network (Alshammari, A., et al., 2020). A Blackhole attack launched against VANET could cause data interruptions and manipulation (Lee & Atkison, 2020). If a malicious node spoofs its identity to intercept and drop data packets, the data could become unavailable or be routed in the wrong direction. This would result in the data moving in a different direction. Blackhole-based attacks are risky since they can facilitate several criminal activities. This includes the potential for vehicles to be hijacked, communication between vehicles to be disrupted, a denial of service to be delivered to the entire network, and data manipulation.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

In addition, the AODV routing protocol is widely used in MANET to improve the behaviour of various applications in ad-hoc environments. The protocol only generates the path between nodes if the source nodes send the request to them. As a result, AODV is considered an on-demand technique because it generates no additional network traffic. However, there is limited study and implementation of AODV routing protocols in VANET.

Therefore, to protect against these attacks, it is critical to install suitable security measures and employ the most suitable routing protocol based on the traffic scenario. Performance metrics are also required for evaluating, comparing, optimizing, and troubleshooting systems or networks. By deploying routing protocol and acquiring insight through performance metric analysis such as EED, PDR and throughput, the network may strengthen its resilience to attacks and enable safe communication. The results demonstrated in this project show a significant decrease in throughput when Blackhole attacks were present, indicating the severe impact on the overall data transmission efficiency in VANET. Additionally, the experiments revealed a notable increase in EED and a decrease in PDR, highlighting the compromised network performance due to malicious nodes. Tourism is one of the fastest-growing development sectors in addition to other development strategic agendas such as energy, food, and infrastructure.

Literature Review

Referring to the statistics released by the Malaysian Computer Emergency Response Team, Cybersecurity Malaysia in the year 2023 showed a significant increase in cyber-attacks involving wireless communication by 150% from 2013 until 2022. Types of attacks that are often used by attackers to destroy the connection between a group of cars instead of communicating are wormhole, Blackhole and Sybil attacks located at the network layer of the OSI model. A Blackhole attack is rerouting the network traffic through a specific node controlled by the attacker (Dhanke et al.2024). Attackers may be able to control the car's communication and rerouting network traffic if there are no solutions where intelligent cars are rapidly developing. According to (Fenzl et al., 2021), Tesla's and BYD's smart cars can be controlled using a combination of black hole attack techniques and the experiments conducted in 2018 and 2021 proved a lack of the current security approach. The result showed that current intelligent cars like the Tesla Model S (P75 and P76) can be successfully manipulated using WIFI and cellular networks. Attackers have compromised in-vehicle systems such as the IC, CID, and Gateway, and then spread malicious CAN messages into Tesla's database system using Blackhole malicious attacks. Most attackers are detected using a technique like a watchdog (Krzysztoń & Marks, 2020; N. Premalatha, Manju Kumaresan, Shalini Devi Raja, 2020; Sharma et al., 2022), routing technique (Basomingera & Choi, 2020), profile databases (Arjoune et al., 2020) and cluster head (Chandravathi & Mahadevan, 2021) to improve detection rate.

Intrusion attack performance using techniques like watchdog, database and routing reached a less satisfactory level with a detection rate of less than 32% while cluster head was on the scale of 46%. Packet Delivery Ratio (PDR) and Signal Strength (SS) are two common metrics used to measure the performance of intrusion attack detection at a lower layer of the OSI model (Nabou et al., 2018). Therefore, inappropriate use of the techniques, metrics and layers model will result in inaccurate outcomes in determining the performance of each intrusion. Examining these works provides valuable insights into the progress made in securing VANET and

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

optimizing their performance. Table 1 shows the previous study conducted by researchers related to attack and methodology approaches.

(Kumar et al., 2021) focused on detecting Blackhole attacks in VANET using a secure AODV routing algorithm. The problem addressed was the presence of malicious nodes acting as routers and injecting spoofed routing tables, which disrupt the network's performance. The researchers measured metrics such as EED, PDR, and throughput to evaluate their proposed method. The results demonstrated a significant improvement, with only 238 packets dropped using the proposed method compared to 1532 packets with the previous approach.

(Bamhdi, 2020) proposed an efficient dynamic-power AODV routing protocol based on node density. The aim was to tackle the challenges of limited fixed infrastructure and low stability in VANET. The researcher evaluated the protocol's performance by analysing Control Overhead, EED, Jitter, Packet Delivery Fraction, PDR, and throughput metrics. The findings showed an increase in Packet Delivery Ratio from 12% to 31% and a decrease in End-to-End Delay to 51%, indicating improved performance compared to previous methods.

(Fatemidokht & Kuchaki Rafsanjani, 2022) proposed the QMM-VANET clustering algorithm, which considers QoS and monitoring malicious vehicles in VANET. The study tackled the challenges associated with the absence of fixed infrastructure and the need for an efficient routing protocol. The algorithm's performance was evaluated using EED, PDR, and throughput metrics. The findings revealed an increased PDR of 12% and a decreased EED of 45%, indicating improved performance compared to previous methods.

Table 1: Summary of Network Layer Attack and Methodology in Wireless Network

Author, Year	Title	Problem Statement	Methodology	Results & Findings
Kumar et al., 2021	• Blackhole attack detection in Vehicular ad-hoc network using secure AODV • routing algorithm	• Node acts as a router • Malicious • nodes inject spoofed routing table.	• EED • PDR • Throughput	• The total packet drop for the proposed method is only 238, compared to 1532 for the previous approach.
Bamhdi, 2020	• Efficient dynamic-power AODV routing protocol	• No fixed • infrastructure • Low stability	• Control Overhead • EED • Jitter • Packet • Delivery	• The PDR ratio increased from 12% to 31% EED

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

	based on node density		• Fraction • Throughput	decreased to 51%
(Fatemidokht & Kuchaki Rafsanjani, 2022)	• QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks	• No fixed infrastructure • Developing an efficient routing protocol is challenging	• EED • PDR • Throughput	• Increased PDR by 12%. • Decreased EED by 45%.

Methodology

In this project, NS-2 is used as a simulation tool to recreate a VANET network and study its behaviour under different scenarios. The simulations involve varying the number of nodes (10, 20, 30, 40, and 50) to represent traffic congestion in a network area of 1000 x 1000 square meters. The project's details and parameters are outlined in Table 2, providing a comprehensive overview of the setup, configurations, and simulation scenarios. Using NS-2, the project aims to gain insights into the performance and characteristics of VANET networks, especially in analysing Blackhole attacks. Table 2 also summarizes the simulation details, including the simulator, mobility model, number of nodes, simulation area, simulation time, routing protocols and performance metrics evaluated in the study.

Table 2: Network Parameter

`	Value
Simulator	**NS 2.35**
Mobility Model	BonnMotion
Number of Nodes	20,30,40,50,60
Simulation Area	1000 m^2
Simulation time	140 s
Routing Protocol	AODV
Performance Metric	EED, PDR, throughput, PLR and Goodput

Performance Metrics

There are five performance metrics used to evaluate the blackhole attack in VANET.

a) End-to-End Delay (EED)

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

EED measures the time it takes for a packet to travel from its source to its destination. In the presence of a Blackhole attack, the malicious node may intentionally delay or drop packets, resulting in abnormally high EED delays. Monitoring EED delays can help identify deviations from normal network behaviour and raise alarms when suspicious delays are detected (Kumar et al., 2021).

b) Packet Delivery Ratio

PDR represents the ratio of successfully received packets to the total packets sent. In a Blackhole attack, the malicious node intercepts and drops packets, leading to a lower PDR than expected. Monitoring PDR can reveal significant drops or inconsistencies in packet delivery, which can indicate the presence of a Blackhole attack (Kumar et al., 2021).

c) Throughput

Throughput measures the rate at which packets are successfully delivered. In a Blackhole attack, the throughput may be significantly reduced due to the malicious node dropping or manipulating packets. Monitoring changes in throughput can help identify abnormal network behaviour associated with a Blackhole attack (A. Kumar et al., 2021).

d) Goodput

Goodput is the measure of usable data transferred over a network, excluding protocol overhead and retransmitted data. Like bandwidth, it is measured in bits per second.

e) Packet Loss Rate (PLR)

PLR is the percentage of data packets that are lost during transmission. High PLR can indicate network congestion, issues with network reliability, or problems with the quality of the connection.

Figure 1 illustrates the process, which includes setting up the simulation environment, configuring parameters in a ".tcl" file, running the simulation, generating a trace file ".tr" with network activity data, using an AWK script ".awk" to extract relevant information from the trace file, analysing the data, and creating graphs using tools like Excel. The comprehensive process allows researchers to simulate and study network behaviour, extract data, and visualize results for analysis and interpretation.

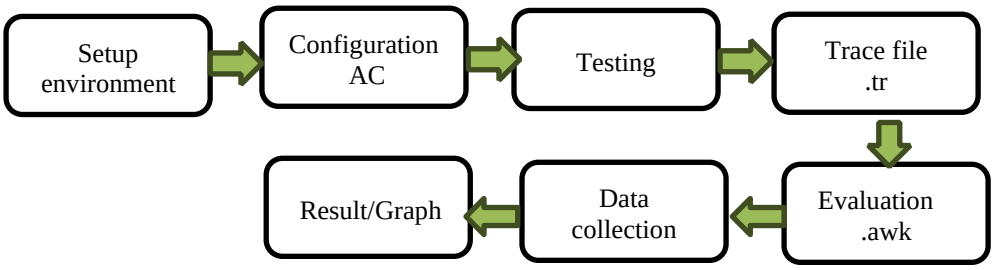

Figure 1: The Simulation Process

The EED measures the time it takes for packets to travel from the source node to the destination node in the network. By analysing the EED as part of the parameters, the project aims to understand how the presence of a Blackhole attack affects the time it takes for packets to reach their destination.

Figure 2 shows 20 nodes simulated on NS-2 and Bonn motion. The movement of the cars is generated using BonnMotion along with AODV routing protocol in a $1000m2$ within 140s duration.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

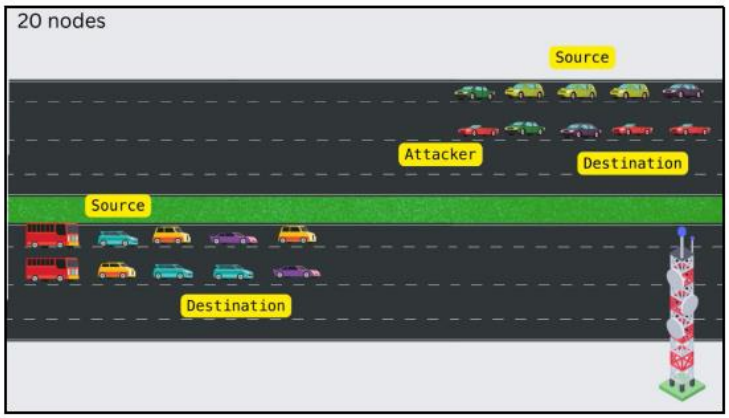

Figure 2: Simulation Scenarios with 20 Nodes

Result and Analysis

As more vehicles join Vehicular Ad Hoc Networks (VANETs), assessing the impact of Blackhole attacks depends on minimizing EED and PDR values. Increased vehicle density exacerbates the danger of Blackhole attacks by increasing delay in V2V and V2I communications. Communication disruptions are more likely due to lengthier delays in data transmission, along with the dropping or manipulation of information by malicious nodes. In larger networks, dealing with Blackhole attacks while maintaining reasonable EED becomes more intricate. Effective EED monitoring is crucial to detect and address these attacks, ensuring stability, reliability, and safety in VANETs amid growing vehicular participation.

As shown in Figure 3 comparison in VANET network without Blackhole attacks, where packets are delivered directly, the presence of Blackhole attacks leads to higher EED values. This impact damages throughput network performance, highlighting the negative consequences of Blackhole attacks on EED. The simulated VANET network analysis evidence that such attacks significantly affect EED, resulting in longer packet delivery times for most scenarios compared to those without these attacks.to scenarios without such attacks.

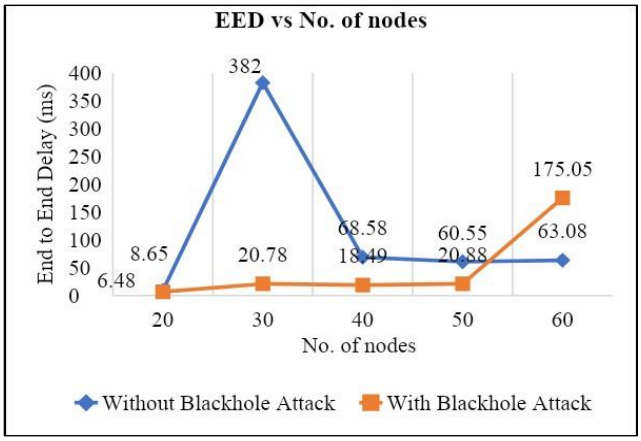

Figure 3: End-to-End Delay (EED) vs Number of Nodes

Figure 4 compares the PDR performance metric between without and with a Blackhole attack. The PDR indicates the percentage of successfully delivered packets out of the total sent. In the scenario without a Blackhole attack, packets are delivered as intended, establishing a baseline

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

PDR to evaluate typical delivery reliability. In the scenario with a Blackhole attack, a malicious node intentionally drops or manipulates packets, leading to a decreased PDR. Comparing the PDRs provides insights into the impact of Blackhole attacks on packet delivery, helping assess the effectiveness of countermeasures and detection mechanisms.

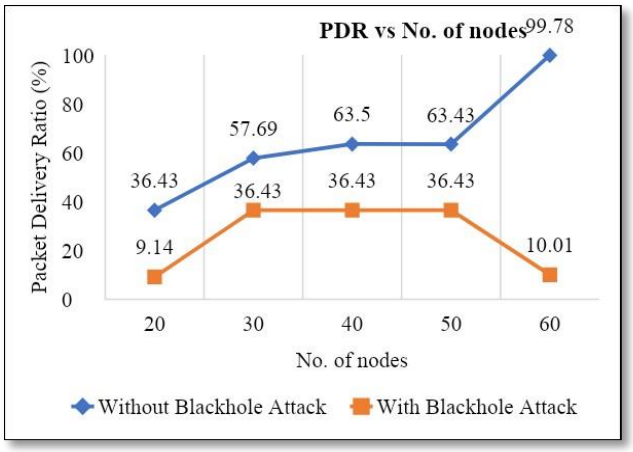

Figure 4: Packet Delivery Ratio vs Number of Nodes

For 20 nodes, the PDR without a Blackhole attack is 36.43%, indicating that approximately 36.43% of the packets were successfully delivered. However, in the presence of a Blackhole attack, the PDR drops significantly to 9.14%, indicating a substantial decrease in the successful delivery of packets. With 30 nodes, the PDR without a Blackhole attack is 57.69%, while the PDR with a Blackhole attack shows a slightly lower value of 36.43%. The difference between the two scenarios is relatively minimal, suggesting that the Blackhole attack has a limited impact on packet delivery in this configuration. In the case of 40 and 50 nodes, the PDR without a Blackhole attack remains EED higher between 63.43% and 63.50% respectively representing the impact of a Blackhole attack that interrupts communication between Vehicle to Vehicle(V2V) and Vehicle to Infrastructure(V2I).

However, with the introduction of a Blackhole attack, the performance of PDR decreases to 36.43% for an increasing number of nodes that represent traffic congestion. This signifies a significant reduction in the successful delivery of packets due to the presence of the Blackhole attack. With 60 nodes, the PDR without a Blackhole attack is considerably high at 99.78%, indicating a near-perfect packet delivery rate event during traffic congestion. However, when a Blackhole attack is introduced in the network, the PDR drops significantly to 10.01%, demonstrating a substantial decrease in the successful delivery of packets and this percentage rate keeps dropping with increasing number of nodes. The presence of a Blackhole attack significantly degrades the successful delivery of packets, leading to decreased PDR values.

Figure 5 compares the throughput performance metric without a Blackhole attack and another with a Blackhole attack. Throughput measures the amount of data transmitted over the network each time. The first scenario represents normal network conditions, where data transmission occurs without interference. In the second scenario with a Blackhole attack, a malicious node intentionally disrupts data transmission. By comparing the throughput in these scenarios, the project aims to evaluate the impact of a Blackhole attack on the network's data transmission efficiency.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

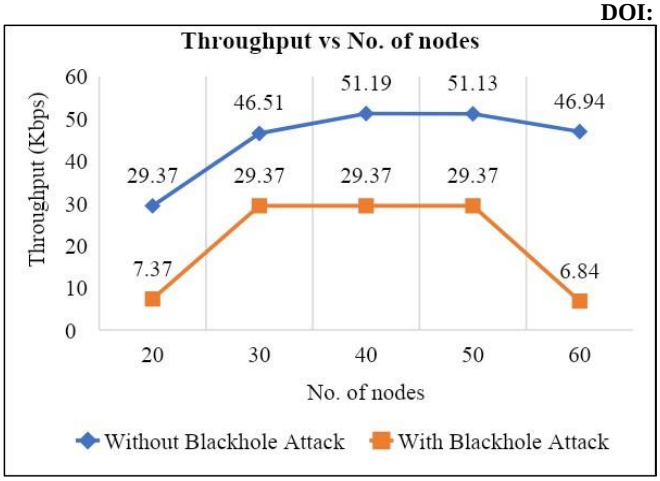

Figure 5: Throughput vs Number of Nodes

The results indicate that the presence of a Blackhole attack significantly impacts the network's throughput. In all cases, the throughput is notably lower when a Blackhole attack is present compared to scenarios without the attack. This highlights the disruptive effect of Blackhole attacks on data transmission, emphasizing the importance of implementing effective countermeasures to mitigate their impact and maintain higher network efficiency and throughput.

Figure 6 above shows the graph for comparison metric of percentage packet loss rate without and with a blackhole attack on the Random Waypoint mobility model in AODV routing protocol. The graph with blackhole attack shows a consistently high packet loss rate of around 80% across all node counts. This indicates that the blackhole attack is causing a significant and consistent disruption in the network, leading to a high rate of packet loss regardless of the number of nodes. Under a blackhole attack, the PLR is significantly higher, starting at 83.43% and peaking at 85.71%. This indicates that the blackhole attack exacerbates packet loss, making the network less reliable.

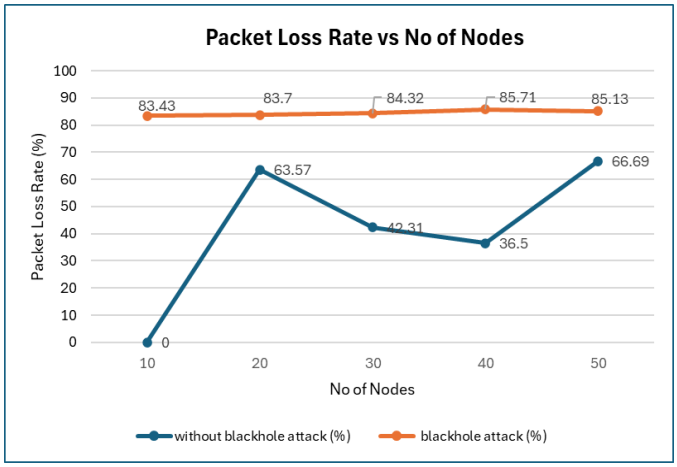

Figure 6: Packet Loss Rate vs Number of Nodes

In normal conditions (without blackhole attack), PLR starts at around 63.57% for a lower number of nodes and increases to 85.13% as the number of nodes increases the purple line shows a variable packet loss rate that changes with the number of nodes. As the number of

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

nodes increases, the network might experience congestion, leading to higher packet loss rates. The spike at 20 nodes could be a result of temporary congestion or suboptimal routing. The decrease in packet loss rate after 20 nodes suggests that the network might be optimizing itself or that the routing protocols are becoming more efficient as the number of nodes increases. In wireless networks, interference and packet collisions can lead to packet loss.

Figure 7 shows the outcome of goodput vs number of nodes. The increase in goodput due to the blackhole attack is substantial across all node counts, ranging from 188.291 kbps to 278.1215 kbps. The variations in the absolute change in goodput that the blackhole attack's effect on performance might depend on network size or configuration. Under Normal Conditions (without blackhole attack): The goodput decreases as the number of nodes increases, indicating that higher congestion (more vehicles/nodes) leads to reduced network efficiency and lower data delivery rates. This is expected as more nodes can lead to increased network congestion and collisions, slightly reducing the goodput.

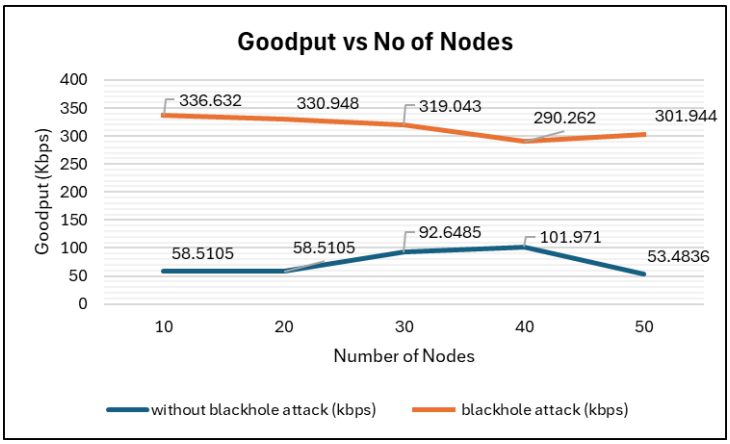

Figure 7: Goodput vs Number of Nodes

Under a blackhole attack, the goodput is significantly lower compared to normal conditions. This is because the malicious node drops packets, reducing the amount of useful data delivered to the destination. As the number of nodes increases, network congestion can increase, leading to more collisions and retransmissions, which can reduce the overall goodput. This effect is more pronounced in the presence of a blackhole attack. The efficiency of the routing protocol in handling increased nodes and mitigating the effects of a blackhole attack can influence the goodput. If the protocol is not efficient in detecting and avoiding the black hole, the goodput will be significantly lower. In Normal Conditions (without blackhole attack): The goodput decreases as the number of nodes increases, indicating that higher congestion (more vehicles/nodes) leads to reduced network efficiency and lower data delivery rates. Goodput is a key factor in determining the QoS in VANETs. Applications like emergency messaging, traffic management, and infotainment rely on high goodput to ensure timely and reliable data delivery. Ensuring high goodput is essential for maintaining the reliability and efficiency of VANETs, particularly in safety-critical applications. Effective security measures are necessary to mitigate the impact of attacks like blackhole and maintain optimal network performance.

Conclusion

This study investigated the detrimental impact of Blackhole attacks on Vehicular hoc networks (VANETs) using the AODV routing protocol, simulated under varying node densities (20–60 nodes) to emulate urban traffic scenarios. Through rigorous analysis of key metrics such as

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

End-to-End Delay (EED), Packet Delivery Ratio (PDR), Throughput, Goodput, and Packet Loss Rate (PLR), the research demonstrated severe network degradation during attacks. Results revealed a 63.43% surge in EED, PLR exceeding 80%, and drastic PDR reductions (e.g., from 99.78% to 10.01% for 60 nodes). Throughput and Goodput also declined significantly, highlighting the attack's disruptive effects on data transmission efficiency and reliability. Higher node density exacerbated congestion and attack impacts, underscoring the vulnerability of scalable VANETs to malicious interventions.

The findings emphasize the critical need for robust security mechanisms in VANETs, particularly for safety-critical applications like emergency messaging and traffic management. While existing detection techniques, such as watchdog systems and clustering algorithms, show promise, their limited detection rates (below 46%) necessitate further innovation. Future research should prioritize trust-based protocols, adaptive intrusion detection systems, and enhanced routing algorithms to mitigate Blackhole attacks effectively. Additionally, exploring hybrid approaches that combine machine learning with real-time monitoring could improve detection accuracy and resilience.

By addressing these vulnerabilities, this study advances secure VANET frameworks, ensuring operational integrity in intelligent transportation ecosystems. Implementing such measures will not only safeguard data transmission but also foster public trust in connected vehicle technologies, paving the way for safer and more efficient smart cities.

Acknowledegment
I would like to express my special thanks of gratitude to both of my students, Miss Siti Nurul Aina binti Mazlan and Raja Mohamad Arash bin Raja Azlan for their commitment and dedication to complete the research project based VANET. I also would like to thank my wife who helped me a lot in gathering information, collecting data and guiding me from time to time in making this project

References

Alshammari, A., Zohdy, M. A., Debnath, D., & Corser, G. (2020). Real-time vehicular traffic simulation for Blackhole Attack in the greater Detroit area. *Journal of Information Security, 11(01)*, 71–80.

Arjoune, Y., Salahdine, F., Islam, S., Ghribi, E., & Kaabouch, N. (2020). A novel jamming attack detection approach based on machine learning for wireless communication. *4th International Conference on Information Networking (ICOIN 2020)*.

Aziz, A., Samad, F., & Siddiqui, S. (2002). Optimizing privacy preservation in wireless VANETs. *International Conference on Emerging Trends in Smart Technologies (ICETST)*, 1–6.

Bamhdi, A. (2020). Efficient Dynamic-Power AODV Routing Protocol Based on Node Density. *Computer Standards & Interfaces*, *70*, 103406. https://doi.org/10.1016/j.csi.2019.103406

Basomingera, R., & Choi, Y. J. (2020). Learning from routing information for detecting routing misbehaviour in ad hoc networks. *Sensors (Switzerland)*, *20*(21), 1–22. https://doi.org/10.3390/s20216275

Chandravathi, C., & Mahadevan, K. (2021). Web-Based Cross-Layer Optimization Technique for Energy Efficient WSN. *Wireless Personal Communications*, *117*(4), 2781–2792. https://doi.org/10.1007/s11277-020-07047-1

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009
Dhanke, J., Rastogi, S., Singh, K., Saxena, K., Kumar, K., & Mishra, P. (2024). International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING An Efficient Approach for Prevention of Blackhole Attack in MANET 1. *Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE*, *2024*(12s). www.ijisae.org

Fatemidokht, H., & Kuchaki Rafsanjani, M. (2022). QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks.

Journal of Systems and Software, *165*, 110561. https://doi.org/https://doi.org/10.1016/j.jss.2020.110561

Fenzl, F., Rieke, R., & Dominik, A. (2021). *In-vehicle detection of targeted CAN bus attacks*. https://doi.org/10.1145/3465481.3465755

Khan, S., Sharma, I., Aslam, M., Khan, M. Z., & Khan, S. (2021). Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey. In *Future Internet* (Vol. 13, Issue 4). https://doi.org/10.3390/fi13040096

Krzysztoń, M., & Marks, M. (2020). Simulation of watchdog placement for cooperative anomaly detection in Bluetooth Mesh Intrusion Detection System. *Simulation Modelling Practice and Theory*, *101*, 102041. https://doi.org/https://doi.org/10.1016/j.simpat.2019.102041

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 Adhoc Network using secure AODV routing algorithm. *Microprocess Microsyst*, *80*(C), 1–7.

Lee, K., Yang, Y., Prabhune, O., Chithra, A. L., West, J., Fawaz, K., Klingensmith, N., Banerjee, S., & Kim, Y. (2022). AEROKEY: Using Ambient Electromagnetic Radiation for Secure and Usable Wireless Device Authentication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, *6*(1). https://doi.org/10.1145/3517254

Lee, M., & Atkison, T. (2021). VANET applications: Past, present, and future. *Vehicular Communications*, *28*, 100310. https://doi.org/https://doi.org/10.1016/j.vehcom.2020.100310

Mistareehi, H., Salameh, H. B., & Manivannan, D. (2022). An On-Board Hardware Implementation of AODV Routing Protocol in VANET: Design and Experimental Evaluation. *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 1–6. https://doi.org/10.1109/IOTSMS58070.2022.10062284

N. Premalatha, Manju Kumaresan, Shalini Devi Raja, Y. L. (2020). VANET-based Communication on Vehicles for Accident Prevention. *2020 International Journal of Engineering Research & Technology (IJERT), 8(12)*(12), 113–118.

Nabou, A., Laanaoui, M. D., & Ouzzif, M. (2018). Evaluation of MANET Routing Protocols under Black Hole Attack Using AODV and OLSR in NS3. *2018 6th International Conference on*

Wireless Networks and Mobile Communications (WINCOM), 1–6. https://doi.org/10.1109/WINCOM.2018.8629603

Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart Transportation: An Overview of Technologies and Applications. *Sensors*, *23*(8), 1–32. https://doi.org/10.3390/s23083880

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 134-146
DOI: 10.35631/JISTM.1038009

Sharma, P., Scholar, M. T., & Engineering, C. (2022). a Dynamic Self-Reconfiguration Protocol for Disaster Management. *Journal of Emerging Technologies and Innovative Research*, *9*(12), 50– 55.