JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 10 Number 2 | December 2025: 299-307
DOI: 10.15575/join.v10i2.1568

Performance Evaluation of Vehicular Ad Hoc Networks Considering Malicious Node Impact on Quality of Services Metrics

Naufal Faiz Alfarizi[1], Muhammad Taufiq Nuruzzaman[2], Shofwatul 'Uyun[3], Bambang Sugiantoro[4], Mohd. Fikri Azli bin Abdullah[5]
[1,2,3,4]Department of Informatics, UIN Sunan Kalijaga Yogyakarta, Indonesia
[5]Faculty of Information Science and Technology, Multimedia University (MMU), Malaka, Malaysia

Article Info

Article history:

Received February 09, 2025
Revised June 09, 2025
Accepted July 13, 2025
Published August 24, 2025

Keywords:

Blackhole
Malicious
TIPHON
VANETs
Wormhole

ABSTRACT

Vehicular Ad Hoc Networks (VANETs), a subset of mobile ad hoc networks (MANETs), is essential for enabling communication between vehicles in intelligent transportation systems. However, their dynamic and decentralized nature exposes them to significant security threats, particularly from malicious nodes. Attacks such as black holes and wormholes can severely degrade network performance by causing packet loss and increasing end-to-end delays. This paper aims to evaluate the impact of malicious node behavior on VANET performance using key Quality of Service (QoS) parameters, including throughput, end-to-end delay, jitter, packet delivery ratio (PDR), and packet loss ratio (PLR). The specific objective is to analyze how black hole and wormhole attacks affect communication efficiency in VANET environments. The main contribution of this work lies in the integration of Simulation of Urban Mobility (SUMO) for realistic traffic scenario generation with Network Simulator 3 (NS-3) for detailed network performance evaluation. This approach enables comprehensive simulation of VANET behavior under attack conditions. The findings provide valuable insights into the vulnerabilities of VANETs and form a basis for the design of more robust and secure vehicular communication systems.

Corresponding Author:

Muhammad Taufiq Nuruzzaman,
Department of Informatics, Faculty of Science & Technology, UIN Sunan Kalijaga Yogyakarta
Jl. Laksda Adisucipto No 1 Yogyakarta, 55281
Email: m.taufiq@uin-suka.ac.id

1. INTRODUCTION

An ad hoc network is a wireless mobile communication network composed of a group of mobile nodes with wireless transceivers [1]. The mobile nodes of the network use their own wireless transceivers to exchange information when the information is not within the communication range, other intermediate nodes can be used to relay to achieve communication. They can be widely used in environments that cannot be supported by wired networks, or which require temporary communication, such as military applications, sensor networks, rescue and disaster relief, and emergency response [2][3][4].

The network model used in this research is an ad hoc network with the type of Vehicular Ad Hoc Network (VANET), which is affected by Malicious Node attacks. A malicious node is a node that brings threats or disruptions to a network. The malicious node moves randomly and then attacks the existing

p-ISSN: 2528-1682
e-ISSN: 2527-9165

network. Routing within a VANET is a complex process involving successfully transferring data packets from a source vehicle to a destination vehicle while ensuring a secure and dependable communication framework [5]. One such dynamic routing protocol is Ad hoc On-demand Distance Vector (AODV) [6], which mainly focuses on coverage area and throughput data. The AODV protocol faces challenges in selecting the best relay nodes, which requires optimization to improve performance in VANETs [7].

VANET infrastructure is crucial for ensuring vehicular safety, mobility management, and vehicular applications. The transportation sector, constituting the legal means of moving goods or individuals between locations, has encountered various challenges over time. Issues such as elevated accidents, blockades, and carbon emissions have emerged. Given the intricate nature of these challenges, researchers have endeavored to integrate virtual technologies into transportation, leading to the development of what is known as Intelligent Transport Systems (ITS) [8]. The integration collects information on traffic and road conditions without relying on traditional internet connectivity. It also addresses applications such as early warnings in areas with limited coverage, safety and health emergency messages in highly congested zones, and air monitoring without depending on traditional TCP/IP internet connectivity [9]. In this Ad hoc network, it is highly vulnerable to threat attacks. This will be very dangerous if the packet being sent contains important information [10]. VANET establishes an ad hoc network in each vehicle with high node movement dynamics. Therefore, it is necessary to test the performance of VANET under the influence of Malicious Nodes such as Black hole Attacks, which can cause excessive packet drops, and Wormhole Attacks, which can increase delay.

The VANETs hold a crucial position within smart city applications as inter-vehicle communication is deemed indispensable for maintaining the technological efficiency of the city [11]. It is an emerging technology that has much potential for development ahead of it. VANETs seek to connect devices contained within vehicles together to create services that are particularly relevant to a vehicular environment. They attempt to do so without relying on infrastructure devices to assist in the process of network topology management [12]. A cooperative communication system is one of the key technologies in the framework of ITS. The term “cooperative” signals the collaboration between vehicles and transport infrastructure by using wireless networks. Normally, there are four types of communication in a cooperative intelligent transport system (C-ITS), namely, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-network (V2N) [13]. In VANET, each vehicle will be equipped with wireless connectivity to enable vehicles to communicate with each other, in addition to communication towers on both sides of the road to connect distant vehicles to each other or to the Internet, and even to connect trains and airplanes to this network, making the volume of information exchange very large as shown in Figure 1. VANETs and traffic accidents play an important role in reducing the number of fatalities, driving efforts in developed countries and among vehicle manufacturers to find solutions to ensure road safety [14].

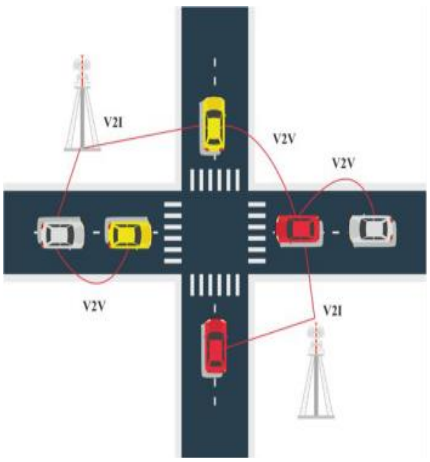

Figure 1. V2V Schema

V2V communication, vehicles directly exchange information. This can include data about speed, position, acceleration, and other relevant parameters. V2V communication enables real-time collaboration among vehicles, helping them react to changes in the road environment, such as sudden braking or the presence of obstacles [15]. In a network, the routing protocol significantly impacts its performance. Similarly, in VANET, there are many routing protocols that can be implemented. One of them is the AODV routing protocol [16]. In this research, the author uses Sumo as a generator for the VANET scheme, which will then be analyzed for node mobility using Network Simulator-3 (NS-3). The results obtained will be used to evaluate network performance using Quality of Services (QoS) techniques.

A Blackhole works by declaring itself to the source node that it has the shortest route to the destination node [17]. In a VANET, a Blackhole attack occurs when the routing protocol is used to declare itself to other intermediate nodes as the node with the shortest route to the destination node. After receiving a Route Request (RREQ) message from a node, the Blackhole node can forge a Route Reply (RREP) message as if it has a new route to the destination node. To suppress genuine RREP messages that might be received by the source node from other nodes, the attacker can forge a fake RREP message by increasing the destination's sequence number [18]. Like a Blackhole Attack, a Wormhole Attack is also a type of malicious node attack that can jeopardize the performance of an ad hoc network. A Wormhole is an attack on a network involving one or more wormhole nodes that are connected to each other and cooperate to disrupt network traffic [19]. These attacker nodes are located at a considerable distance from each other, and each attacker node sends the packets received from ordinary nodes to other attacker nodes using a wormhole tunnel. Through this tunnel, the distance between attacker nodes appears to be just one hop, even though they are quite far apart, creating the illusion of a shorter path compared to the actual route [20]. Consequently, the impact of a wormhole attack will affect the end-to-end delay of packet transmission from the source node to the destination node.

This research aims to simulate a VANET network model using the AODV routing protocol affected by Malicious Nodes, such as Black hole Attacks and Wormhole Attacks. The communication between vehicles takes place in an urban environment using IEEE 802.11p, which is part of Wireless Ad hoc Vehicular Environments (WAVE). WAVE is a protocol architecture developed by IEEE for vehicular ad hoc networks [21]. WAVE is also known as Dedicated Short-Range Communication (DSRC). This architecture includes two standards: IEEE 802.11p for the lower protocol layer and the IEEE 1609 group of standards for the higher protocol layers [22]. The testing metrics based on QoS parameters include performance measures. QoS is a critical mechanism in network management that ensures the efficient allocation of resources to meet specific performance metrics such as throughput, latency, jitter, and packet loss [23][24].

2. METHOD

This research examines VANET performance under malicious node influence through several stages: data generation using realistic traffic scenarios and network simulations, followed by performance analysis based on QoS metrics. The study leverages the potential of simulation-based data using two integrated tools: Simulation of Urban Mobility (SUMO) and Network Simulator 3 (NS-3). Figure 1 illustrates the proposed methodology for evaluating the impact of malicious nodes in VANET environments, and the explanation follows the outlined framework.

2.1. Data Collection

We collected primary simulation data through an integrated network and traffic simulation using NS-3 and SUMO. The simulations were conducted in an urban environment with wireless communication channels, emulating real-world vehicular scenarios. The simulation was set in an urban environment with a wireless communication channel, reflecting realistic traffic conditions. Traffic flows were modeled using File Transfer Protocol (FTP) over a simulation time of 100 seconds. Vehicle mobility was generated using the SUMO tool, with an average vehicle speed of 13.22 m/s and node distribution based on real urban movement patterns. For routing, the AODV protocol was utilized due to its reactive nature and suitability for dynamic environments. Each simulation involved the transmission of 100 data packets to evaluate performance metrics such as throughput, end-to-end delay, jitter, packet delivery ratio, and packet loss.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

2.2. *Simulation Processing*

For the simulation data preprocessing, we assigned labels to each simulation run based on scenario type under attack and ensured that each simulation file contained complete and valid QoS metric values. The tabular dataset extracted from NS-3 output includes five main variables: throughput, end-to-end delay, jitter, packet delivery ratio (PDR), and packet loss ratio. For multi-modal analysis, we associated each simulation with mobility trace data from SUMO, representing vehicle movement, speed, and position. Each simulation ID was mapped to its corresponding traffic trace to ensure consistency and prevent duplicate records. We isolated simulation results influenced by black hole and wormhole attacks. This allowed the classification model to learn behavioral patterns under malicious influence. Additionally, QoS features were normalized to ensure uniformity in scale, improving model convergence. The extracted features represent the core indicators for evaluating VANET performance and are critical in assessing the impact of routing attacks on vehicular communication networks. The performance evaluation was conducted by attack scenarios using QoS, the complete process and outcomes of these simulations are illustrated in Figure 2.

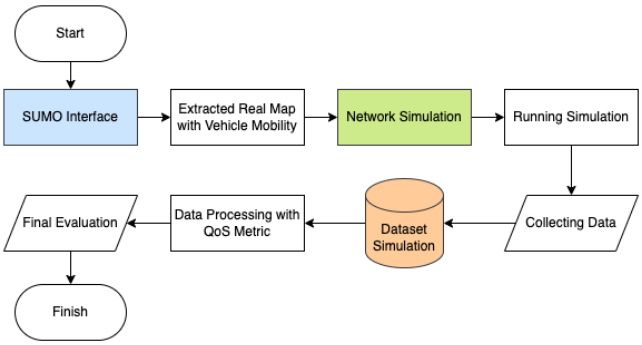

Figure 2. Flowchart Data Processing

2.3. *Mobility node with real map*

The Mobility node with real map obtained in this research are from the Urban Simulation Area in VANET, created using SUMO by adapting the movement map of nodes in the city of Yogyakarta. This map falls into the real map category, depicting a realistic traffic environment and sampling several nearby nodes that cover Kaliurang Road, Jalan Ring Road Utara, Road Pandega Marta, Road Pandega Sakti, and Jalan Timor Tim. The real map used as a test sample with indications of nearby nodes based on mobility can be seen in Figure 3.

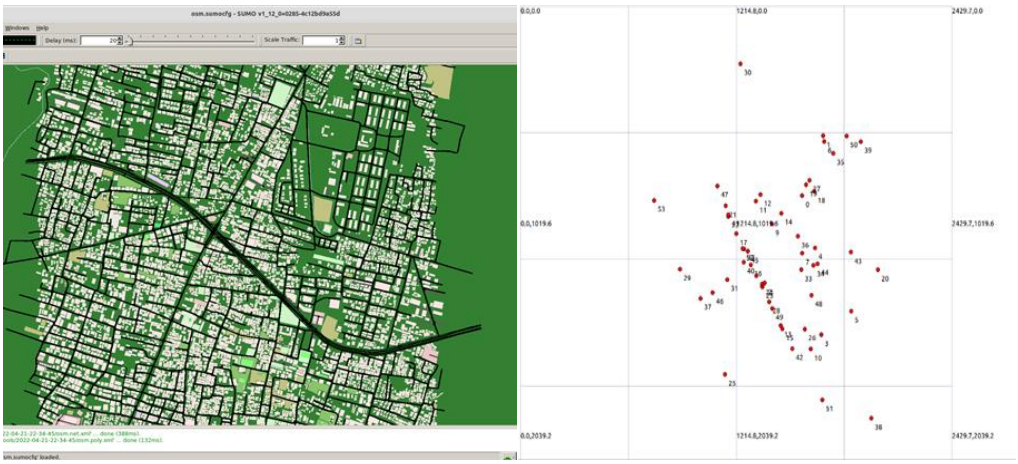

Figure 3. Real Maps SUMO with Mobility Node

The simulation design in this research aims to determine the values of the parameters used. Essentially, parameters serve as reference values for the computational process during the simulation. In the VANET simulation design, two new modules are introduced: Mac802.11Ext and WirelessPhy-Ext, based on the IEEE 802.11p standard. The IEEE 802.11p standard is represented as IEEE 802.11Ext during the VANET simulation. To implement WAVE, a new standard, IEEE 802.11p, was developed from the IEEE 802.11 standard. The principle of this standard is to support Intelligent Transportation Systems (ITS) applications. The design used in NS-3 for the VANET network can be seen in Table 1.

Table 1. VANET on IEEE 802.11p Standard

No	Simulation	
	Name	***Specification***
1	Network Simulation	3.35 All in One
2	Type Simulation Area Channel	Urban Simulation Area with Wireless Channel
3	Traffic Type and Simulation Time	FTP with 100 Seconds
4	Average Vehicle Speed and Number of Nodes	13.22 m/s with Base on Mobility SUMO
5	Nodes of Black hole	Nodes 5, 8, 15, 16, 19, 31, 37, 38 and 39
6	Nodes of Wormhole	Nodes 5, 8, 15, 16, 19, 31, 37, 38 and 39
7	MAC Layer / Network Interface	802_11p/WirelessPhyExt
8	Routing Protocol	AODV
9	Number of Packets	100 Packets

2.4. QoS Metrics

The QoS Metrics steps in this research are carried out to evaluate the performance of the VANET network simulation model design under the influence of Malicious Nodes with QoS parameters based on the Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) standard. According to the TIPHON standard concerning general aspects of QoS, several points can be used to evaluate the quality of a computer network, such as throughput, end-to-end delay, jitter, and packet loss ratio. The testing criteria values are shown in Table 2.

Table 2. Index QoS

Value	Percentage Index	
	%	***Index***
3,80 - 4,00	96 – 100	Very Good
3,00 - 3,79	75 – 95	Good
2,00 - 2,99	50 – 74	Medium
1,00 - 1,99	<= 49	Bad

3. RESULT AND DISCUSSION

This section presents the results of evaluating VANET performance under the threat of malicious nodes—specifically Blackhole and Wormhole attacks. The primary contribution of this paper is the comparative analysis of VANET QoS performance under these two types of attacks using TIPHON-based metrics: throughput, end-to-end delay, jitter, and packet loss ratio. The key problem addressed is the vulnerability of VANETs to these attacks and the extent to which they degrade network performance.

3.1. Throughput

Throughput refers to the rate of successful data transmission, expressed in bits per second (bps). The presence of Blackhole and Wormhole nodes in the VANET environment significantly affects this parameter. Blackhole attacks exhibit a sharper degradation in throughput as the number of malicious nodes increases, dropping from 57.75 bps (1 node) to 31.03 bps (8 nodes). Wormhole attacks, however, maintain relatively stable throughput performance, albeit slightly decreasing. Tables 3 and 4 indicate that the QoS index for throughput under Blackhole attacks drops from “Good” to “Medium” with the addition of more malicious nodes. For Wormhole attacks, the throughput QoS index remains “Good” to “Very Good” across all node scenarios.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Table 3. Throughput in Blackhole Attack

Nodes	Blackhole		
	Bps	***QoS***	***Index***
1	57,75	3	Good
2	58,16	3	Good
4	52,33	3	Good
6	32,36	2	Medium
8	31,03	2	Medium

Table 4. Throughput in Wormhole Attack

Nodes	Wormhole		
	Bps	***QoS***	***Index***
1	82,84	4	Very Good
2	58,16	3	Good
4	52,43	3	Good
6	51,10	3	Good
8	52,12	3	Good

3.2. End-to-End Delay

End-to-end delay measures the latency experienced by packets from source to destination. Blackhole attacks result in lower latency values since dropped packets reduce the number of successful deliveries, which can misrepresent actual performance. In contrast, Wormhole attacks introduce a significant delay, especially when multiple nodes collude to form private tunnels. Tables 5 and 6 show that Blackhole attacks yield "Very Good" QoS ratings in most cases due to packet dropping. Meanwhile, Wormhole attacks often result in "Medium" to "Good" latency values, reflecting a more realistic yet compromised delivery process. These findings reveal that while Blackhole attacks falsely lower delay metrics, Wormhole attacks visibly degrade performance through packet rerouting.

Table 5. End-to-End Delay in Blackhole

Nodes	Blackhole		
	ms	***QoS***	***Index***
1	90,88	4	Very Good
2	89,97	4	Very Good
4	169,52	3	Good
6	85,60	4	Very Good
8	35,59	4	Very Good

Table 6. End-to-End Delay in Wormhole Attack

Nodes	Wormhole		
	ms	***QoS***	***Index***
1	413,65	2	Medium
2	298,20	3	Good
4	296,38	3	Good
6	136,70	4	Very Good
8	305,93	2	Medium

3.3. Jitter

Jitter refers to the variability in packet arrival time. Jitter under Blackhole attacks remains consistently low, which is expected due to fewer packets reaching their destination. Wormhole attacks exhibit higher jitter values due to inconsistent routing paths and delays caused by tunneling. Tables 7 and 8 show that Blackhole attacks maintain a consistently good jitter QoS, while Wormhole attacks fluctuate between "Good" and "Medium."

Table 7. Jitter in Blackhole Attack

Nodes	Blackhole		
	ms	***QoS***	***Index***
1	60,06	3	Good
2	32,95	3	Good
4	45,80	3	Good
6	32,33	3	Good
8	4,05	3	Good

Table 8. Jitter in Wormhole Attack

Nodes	Wormhole		
	ms	***QoS***	***Index***
1	91,67	2	Medium
2	59,90	3	Good
4	72,72	3	Good
6	52,24	3	Good
8	87,03	2	Medium

3.4. Packet Loss Ratio

Packet loss ratio indicates the percentage of packets lost during transmission. Blackhole attacks lead to significant packet drops, with loss ratios increasing from 29% to 59% as more malicious nodes are introduced. In contrast, Wormhole attacks exhibit more moderate losses. Tables 9 and 10 confirm these observations. Under Blackhole attacks, the QoS rating for packet loss remains "Bad" across all node counts. Wormhole attacks, however, maintain a "Medium" rating, indicating that although they increase delay and jitter, they do not cause as many outright losses as Blackhole attacks.

Table 9. Packet Loss Ratio in Blackhole Attack

Nodes	Blackhole		
	%	***QoS***	***Index***
1	29	1	Bad
2	31	1	Bad
4	46	1	Bad
6	51	1	Bad
8	59	1	Bad

Table 10. Packet Loss Ratio in Wormhole Attack

Nodes	Wormhole		
	%	***QoS***	***Index***
1	18	2	Medium
2	21	2	Medium
4	24	2	Medium
6	25	2	Medium
8	24	2	Medium

3.5. Overall Analysis

Tables 11 and 12 summarize the average QoS values across all parameters. The Blackhole attack scenario yields an overall QoS average of 2.6 (Medium), with the lowest score in packet loss. The Wormhole attack scenario shows a slightly higher average of 2.65 (Medium), with the lowest score in packet loss and jitter

Table 11. Average Result in Blackhole Attack

No	***Test Parameters***	***Average Value QoS***
1	Throughput	2,6
2	End to End Delay	3,8
3	Jitter	3
4	Packet Loss Ratio	1
5	Average	2,6 (Medium)

Table 12. Average Result in Wormhole Attack

No	*Test Parameters*	*Average Value QoS*
1	Throughput	3,2
2	End to End Delay	2,8
3	Jitter	2,6
4	Packet Loss Ratio	2
5	Average	2,65 (Medium)

These results highlight the different characteristics of each attack. Blackhole Attacks are more destructive in terms of throughput and packet loss, but misleadingly favorable in delay and jitter due to packet dropping. Wormhole Attacks introduce greater instability in delay and jitter but retain higher throughput and lower loss ratios. The analysis emphasizes the importance of detecting both attack types, as each compromises VANET performance in unique ways. These findings also support the need for multi-metric QoS evaluation when assessing network resilience in hostile environments

4. CONCLUSION

This study addresses a critical problem in VANET environments: the degradation of QoS due to malicious node behavior. Specifically, it evaluates the impact of two well-known attack models, Blackhole and Wormhole attacks, on key TIPHON-based QoS parameters: throughput, end-to-end delay, jitter, and packet loss ratio. The main contribution of this research lies in its comparative analysis of these two attack types using real-world traffic scenarios generated via SUMO and simulated through NS-3.

The experimental results show that Blackhole attacks have the most severe effect on the packet loss ratio, with an average QoS score of 1.0, categorized as "Bad." This is due to the nature of Blackhole nodes that absorb all packets, preventing them from reaching their destination. On the other hand, Wormhole attacks significantly increase end-to-end delay, achieving a QoS score of 2.8 ("Medium") as they manipulate routing paths by establishing private tunnels between colluding nodes.

Overall, both types of attacks degrade VANET performance, each affecting different QoS parameters. The average QoS score under Blackhole influence is 2.6, while under Wormhole influence, it is 2.65, both falling under the "Medium" category. These findings confirm that VANETs are vulnerable to multiple forms of attack and require comprehensive detection and mitigation strategies.

The key contribution of this research lies in its clear demonstration of how different malicious node behaviors affect specific QoS parameters differently, supported by simulation data grounded in real-world traffic modeling. However, this study is limited to only two types of malicious attacks. Future research is encouraged to broaden the scope by incorporating additional attack models, such as Flooding Attacks, Jellyfish Attacks, and Replay Attacks, which possess different behavioral patterns and impacts. Furthermore, future work could also explore the implementation of detection and mitigation strategies, such as machine learning-based intrusion detection systems or anomaly-based detection techniques. Investigating VANET performance under hybrid attack scenarios involving multiple attack types simultaneously would also contribute to a more comprehensive understanding of VANET security resilience.

REFERENCES

[1] K. Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," Aug. 01, 2022, *Elsevier B.V.* doi: 10.1016/j.adhoc.2022.102894.

[2] M. T. Nuruzzaman and H.-W. Ferng, "Routing Protocol for a Heterogeneous MSN With an Intermittent Mobile Sink," *IEEE Sens J*, vol. 22, no. 22, pp. 22255–22263, 2022, doi: 10.1109/JSEN.2022.3212197.

[3] M. T. Nuruzzaman and H.-W. Ferng, "Beaconless Geographical Routing Protocol for a Heterogeneous MSN," *IEEE Trans Mob Comput*, vol. 21, no. 7, pp. 2332–2343, 2022, doi: 10.1109/TMC.2020.3038628.

[4] M. T. Nuruzzaman and H.-W. Ferng, "Design and evaluation of an LQI-based beaconless routing protocol for a heterogeneous MSN," *Wireless Networks*, vol. 26, no. 1, pp. 699–721, 2020, doi: 10.1007/s11276-019-02177-2.

[5] M. ul Hassan *et al.*, "ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV," *Sensors*, vol. 24, no. 3, Feb. 2024, doi: 10.3390/s24030818.
[6] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, "Moving ad hoc networks—a comparative study," *Sustainability (Switzerland)*, vol. 13, no. 11, Jun. 2021, doi: 10.3390/su13116187.
[7] V. Chandrasekar *et al.*, "Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-57480-6.
[8] A. Sarwar, S. Anwar, G. Husnain, and M. Akmal, "Crayfish-Inspired Cluster Optimization for Efficient Routing in Vehicular Ad Hoc Networks (COANET)," 2024. [Online]. Available: http://xisdxjxsu.asia
[9] A. Dutta, L. M. Samaniego Campoverde, M. Tropea, and F. De Rango, "A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications," *Journal of Network and Systems Management*, vol. 32, no. 4, Oct. 2024, doi: 10.1007/s10922-024-09853-5.
[10] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Mar. 01, 2023, *MDPI*. doi: 10.3390/electronics12061333.
[11] N. G. Praveena, K. Selvaraj, T. Kalaiselvi, S. S. Nath, and D. Prabakaran, "A fuzzy based efficient and blockchain oriented secured routing vehicular Ad-Hoc networks," *Iranian Journal of Fuzzy Systems*, vol. 21, no. 6, pp. 15–31, Nov. 2024, doi: 10.22111/ijfs.2024.48069.8461.
[12] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, vol. 28, p. 100310, Apr. 2021, doi: 10.1016/J.VEHCOM.2020.100310.
[13] M. N. Tahir, P. Leviäkangas, and M. Katz, "Connected Vehicles: V2V and V2I Road Weather and Traffic Communication Using Cellular Technologies," *Sensors*, vol. 22, no. 3, Feb. 2022, doi: 10.3390/s22031142.
[14] M. A. Al-Shabi and M. A. Al-Shabi, "Evaluation The Performance of MAODV and AODV Protocols In VANETs Models," 2020. [Online]. Available: https://www.researchgate.net/publication/343473429
[15] A. Sheela Rini and C. Meena, "Dynamic Integration of Fast Furious Cheetah Optimization for Efficient and Secure Routing in Vehicular Ad Hoc Networks," *International Journal of Computer Networks and Applications*, vol. 11, no. 2, pp. 248–273, Mar. 2024, doi: 10.22247/ijcna/2024/224449.
[16] M. ul Hassan *et al.*, "ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV," *Sensors*, vol. 24, no. 3, Feb. 2024, doi: 10.3390/s24030818.
[17] G. Farahani, "Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/8814141.
[18] M. T. Ahmed, A. A. Rubi, M. S. Rahman, and M. Rahman, "Red-aodv: A prevention model of black hole attack for vanet protocols and identification of malicious nodes in vanet," *International Journal of Computer Networks and Applications*, vol. 8, no. 5, pp. 524–537, 2021, doi: 10.22247/ijcna/2021/209985.
[19] D. S. Bhatti, S. Saleem, A. Imran, H. J. Kim, K. Il Kim, and K. C. Lee, "Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-53938-9.
[20] F. Alifo, D. Martin, and M. Awinsongya Yakubu, "Wormhole Attack Vulnerability Assessment of MANETs: Effects on Routing Protocols and Network Performance," 2023.
[21] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3060046.
[22] N. Torabi and B. S. Ghahfarokhi, "Implementation of the IEEE 802.11p/1609.4 DSRC/WAVE in NS-2," in *Proceedings of the 4th International Conference on Computer and Knowledge Engineering, ICCKE 2014*, Institute of Electrical and Electronics Engineers Inc., Dec. 2014, pp. 519–524. doi: 10.1109/ICCKE.2014.6993388.
[23] R. Dong, C. She, W. Hardjawana, Y. Li, and B. Vucetic, "Deep Learning for Radio Resource Allocation with Diverse Quality-of-Service Requirements in 5G," Mar. 2020, [Online]. Available: http://arxiv.org/abs/2004.00507
[24] M. Taufiq, M. F. A. bin Abdullah, and D. Choi, "Wireless LAN Access Point Placement Based on User Mobility," *Wirel Pers Commun*, vol. 60, no. 3, pp. 431–440, 2011, doi: 10.1007/s11277-011-0300-0.