Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.031342

ARTICLE

Secure and Reliable Routing in the Internet of Vehicles Network: AODV-RL with BHA Attack Defense

Nadeem Ahmed[1,*], **Khalid Mohammadani**[2], **Ali Kashif Bashir**[3,4,5], **Marwan Omar**[6], **Angel Jones**[7] **and Fayaz Hassan**[1]

[1]School of Electronic Science, Beijing University of Post and Telecommunication, Beijing, 100086, China

[2]Department of Computer Science, Huanggang Normal University, Huanggang, China

[3]Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK

[4]Woxsen School of Business, Woxsen University, Hyderabad, 502345, India

[5]Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon

[6]Information Technology and Management, Illinois Institute of Technology, Chicago, USA

[7]College of Computing, Capital Technology University, Laurel, USA

*Corresponding Author: Nadeem Ahmed. Email: nadeem.ahmed@bupt.edu.cn

Received: 05 June 2023 Accepted: 18 September 2023 Published: 30 December 2023

ABSTRACT

Wireless technology is transforming the future of transportation through the development of the Internet of Vehicles (IoV). However, intricate security challenges are intertwined with technological progress: Vehicular ad hoc Networks (VANETs), a core component of IoV, face security issues, particularly the Black Hole Attack (BHA). This malicious attack disrupts the seamless flow of data and threatens the network's overall reliability; also, BHA strategically disrupts communication pathways by dropping data packets from legitimate nodes altogether. Recognizing the importance of this challenge, we have introduced a new solution called ad hoc On-Demand Distance Vector-Reputation-based mechanism Local Outlier Factor (AODV-RL). The significance of AODV-RL lies in its unique approach: it verifies and confirms the trustworthiness of network components, providing robust protection against BHA. An additional safety layer is established by implementing the Local Outlier Factor (LOF), which detects and addresses abnormal network behaviors. Rigorous testing of our solution has revealed its remarkable ability to enhance communication in VANETs. Specifically, Our experimental results achieve message delivery ratios of up to 94.25% and minimal packet loss ratios of just 0.297%. Based on our experimental results, the proposed mechanism significantly improves VANET communication reliability and security. These results promise a more secure and dependable future for IoV, capable of transforming transportation safety and efficiency.

KEYWORDS

Black hole attack; IoV; vehicular ad hoc network; AODV routing protocol

1 Introduction

The rapidly evolving Internet of Vehicles (IoV) field encompasses a transformative paradigm that has revolutionized vehicular communication and connectivity. IoV integrates many technologies, enabling vehicles to interact seamlessly with each other and the surrounding environment [1]. This interconnected ecosystem involves VANETs and extends its connectivity to sensor networks, cloud computing, and other emerging technologies. IoV is built upon leveraging advanced sensing capabilities, where sensors [2] in vehicles capture real-time data about their surroundings. These sensors enable vehicles to gather information regarding traffic conditions, road hazards, and other relevant parameters, fostering a comprehensive understanding of the transportation ecosystem. This rich sensory data is then processed and analyzed using cloud computing infrastructure, which enables intelligent decision-making and efficient resource allocation [3]. Fig. 1 provides a a holistic view of the inter-connectivity within the IoV framework.

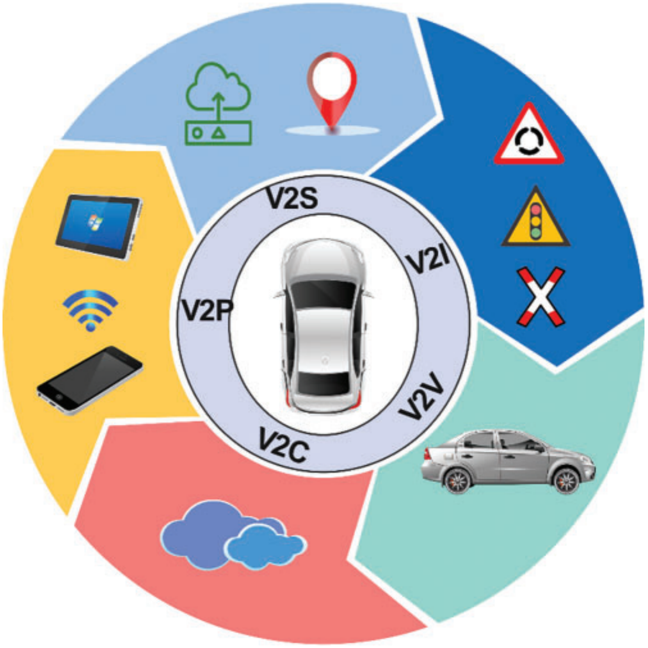


Figure 1: Typical diagram of IoV

It illustrates the intricate network of communication links, each representing a distinct interaction between vehicle to sensors, vehicles to infrastructure, vehicle to vehicle, vehicle to internet clouds, and vehicle to personal devices [4]. These links exemplify the seamless flow of information within the IoV ecosystem, demonstrating the collaborative efforts of sensors, cloud infrastructure, VANETs, and other technologies. Vehicular ad hoc Networks (VANETs) are a crucial component of the Internet of Vehicles (IoV) [5], enabling dynamic communication links between vehicles and infrastructure. VANETs facilitate two modes of communication: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), utilizing the IEEE 802.11p standard for wireless connectivity [6]. V2V communication involves the real-time exchange of information between nearby vehicles, enhancing safety and efficiency through collective awareness. V2I communication connects vehicles with Roadside Units (RSUs), forming the VANET infrastructure. RSUs provide access to traffic management information, signals, and navigation services, empowering vehicles to make informed decisions [7].

Fig. 2 illustrates the interconnectedness between vehicles and infrastructure, demonstrating the seamless flow of information within the VANET infrastructure. This visual representation highlights the collaborative efforts between vehicles and the infrastructure to optimize transportation systems within the IoV framework By leveraging V2V and V2I communication, enabled by technologies like IEEE 802.11p, VANETs enhance collective awareness, improve road safety, optimize traffic flow, and deliver intelligent transportation services [8]. As depicted in Fig. 2, these communication links foster a connected and intelligent transportation ecosystem by facilitating the exchange of critical information between vehicles and the infrastructure.

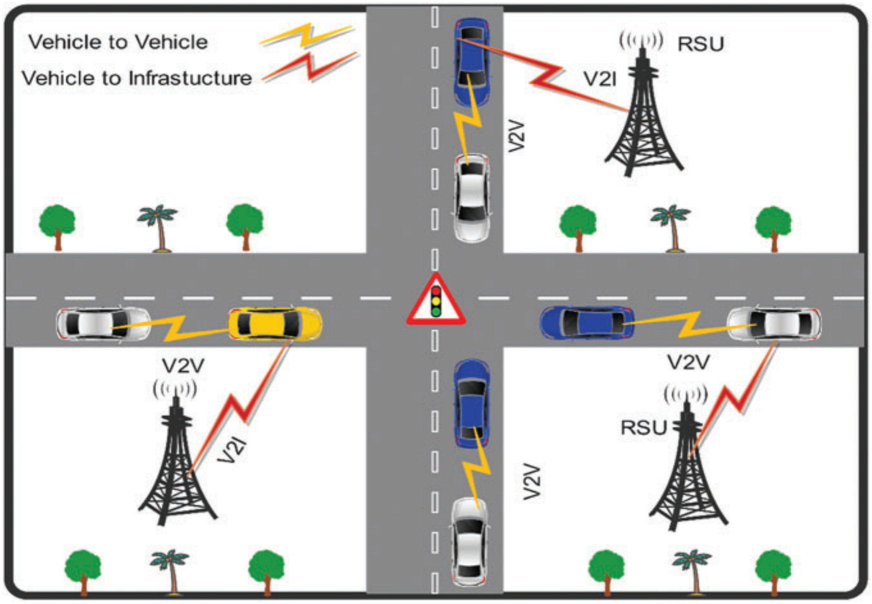


Figure 2: VANET diagram and its components

1.1 Challenges in Maintaining Reliable Message Transmission Quality in VANETs and Mitigation Strategies

Maintaining reliable message transmission in VANETs is critical for supporting various applications [9]. Specialized routing protocols [10] and security procedures are necessary for VANETs to enable reliable and secure communication because of the rapid mobility of vehicles, frequent topology changes, and security threats [11]. However, several other challenges affect message transmission quality [12], including high mobility [13], limited communication range, interference from other wireless systems, channel fading and shadowing, network congestion [14,15], and security and privacy threats [16]. Addressing these challenges requires the development of efficient communication protocols, resource management strategies, security, and privacy mechanisms, and Quality of Service (QoS) mechanisms tailored to the unique characteristics of VANETs [17]. Techniques such as adaptive modulation and coding, channel scheduling, and cooperative communication can also improve message transmission quality in VANETs [18]. Message accuracy refers to the degree to which a message conveys the intended information without errors or distortions. However, maintaining message accuracy in VANETs is a challenging task due to numerous factors such as noise, signal interference, errors or distortions in the message, spoofing [19], jamming [20], relay attacks [21], and BHA [22], which can be caused by malicious attackers. Such factors can lead to inaccuracies in the message content, resulting in incorrect routing decisions, traffic congestion, and unsafe driving situations. To address these challenges, it is crucial to develop efficient communication protocols, error detection and correction mechanisms, and quality of service mechanisms tailored to the unique characteristics of VANETs. Additionally, it is essential to consider potential attackers and develop solutions to mitigate their impacts, such as intrusion detection systems [23], reputation-based trust management systems [24], and secure routing protocols. By implementing measures to ensure message accuracy and security, VANETs can provide a secure and reliable communication framework for various applications, such as traffic management, emergency response, and autonomous driving. Consistency of behavior is a significant challenge in dynamic environments such as VANETs. Nodes in VANETs can move in and out of the communication range [18], affecting their behavior over time. Additionally, nodes may have limited resources, such as battery power or processing capabilities, which can affect their behavior. Inconsistent behavior can lead to a lack of trust and affect the overall reliability of the network. In addition, inconsistent behavior can also lead to routing loops, incorrect routing decisions, and security threats [25]. Therefore, it is essential to develop mechanisms to monitor and evaluate behavior consistency in VANETs and incorporate this factor into the trust score equation. By doing so, nodes that exhibit consistent behavior can be given a higher trust score, contributing towards the development of a secure and reliable communication framework in VANETs. The Table 1 contains the list of abbreviation.

Table 1: List of abbreviation

Abbreviation	Meaning
AODV	ad hoc on-demand distance vector
AODV-RL	ad hoc on demand distance vector-reputation-based mechanism local outlier factor (AODV-RL)
BHA	Black hole attack
DSDV	Destination-sequenced distance vector
IDS	Intrusion detection system
IoV	Internet of vehicles
ITS	Intelligent transportation systems
LOF	Local outlier factor
MAC	Media access control
MANET	Mobile ad hoc network
ML	Machine learning
NRL	Normalized routing load
OBU	On-board unit
PDR	Packet delivery ratio
PLR	Packet loss ratio
PHY	Physical layer
PFR	Packet forwarding ratio
QoS	Quality of service
RSU	Roadside unit
TCP	Transmission control protocol
V2C	Vehicle-to-cloud
V2I	Vehicle-to-infrastructure

(Continued)

Table 1 (continued)

Abbreviation	Meaning
V2P	Vehicle-to-pedestrian
V2S	Vehicle-to-sensor
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
VANET	Vehicular ad hoc network

1.1.1 Challenges and Vulnerabilities Addressed by AODV-RL

ad hoc On Demand Distance Vector-Reputation-based mechanism Local outlier factor (AODV-RL) addresses the challenges and vulnerabilities associated with securing communication in VANETs [8], which are related to the presence of malicious nodes that can launch attacks such as BHA [17], causing communication disruptions in the entire network [17]. To mitigate these risks, AODV-RL uses a reputation-based mechanism that assigns reputation scores to nodes based on their past behavior. Nodes with low reputation scores or flagged as potential outliers by the LOF algorithm are avoided as potentially malicious. This mechanism enhances the security of communication in VANETs by identifying and avoiding potentially malicious nodes. AODV-RL effectively mitigates the risks associated with BHA attacks and other malicious activities in VANETs by using a reputation-based mechanism and LOF algorithm, ensuring the security and reliability of communication in the network.

1.2 Unique Contributions and Implications

Different from traditional routing protocols, our research is novel that enhances the security and reliability in VANET using reputation-based and Local Outlier Factor (LOF) based mechanism. The key contribution of our proposed research are given below:

a) The study proposes a new secure and modified version of the AODV routing protocol for VANET secure communication. The proposed protocol, called AODV-RL, enhances the existing AODV protocol with reputation and Local Outlier Factor (LOF)-based mechanisms to improve the reliability and security of communication in VANETs.

b) The novelty of AODV-RL lies in its ability to address the limitations of existing routing protocols in VANETs. By considering the dynamic topology changes and trustworthiness of nodes (Node Trust Score), AODV-RL provides a more effective and efficient routing solution for detecting malicious nodes in VANET applications. Additionally, the integration of reputation and LOF-based mechanisms allows AODV-RL to identify and isolate malicious nodes in the network, enhancing the security and reliability of communication in VANETs.

c) The significance of AODV-RL is in its potential to enable reliable and secure communication in VANETs for various safety-critical applications. The protocol has been evaluated using simulation experiments under dynamic traffic load scenarios.

d) We compare different AODV-based routing protocols; results are analyzed with our designed routing protocol. The results show that AODV-RL outperforms existing routing protocols regarding Packet Delivery ratio, packet loss ratio, network routing load, and throughput, demonstrating its effectiveness in improving the reliability and security of communication in VANETs.

1.3 Background of Routing Protocols Used in VANETs

Routing protocols are a crucial aspect of wireless networks [6], as they allow for efficient data communication across the network. These protocols determine the optimal path for data to travel across the network based on network topology, link quality, and traffic congestion. Routing protocols intended for VANETs, such as AODV (ad hoc On-Demand Distance Vector) and OLSR (Optimized Link State Routing), are specifically designed to address challenges such as high mobility and frequent changes in network topology such as VANETs and Mobile ad hoc Networks (MANETs) [26], with distinctive features and requirements reflected in their routing protocols [27,28]. Below are the two main types of routing protocols; there are two types of routing protocols, one is proactive routing protocol, and other is the reactive routing protocol.

1.4 AODV Routing Protocol

AODV is a reactive routing protocol for wireless ad hoc networks with no fixed infrastructure or centralized control [29,30]. AODV is designed to establish and maintain routes on demand, as needed, in response to specific requests from source nodes. AODV establishes the communication links by using route discovery procedures. The route discovery steps of AODV are as follows, when a source node needs to send data to a destination node, it first broadcasts a Route Request (RREQ) packet, which contains the address of the destination node [31]. Each node that receives the RREQ packet forwards it to its neighbors until the packet reaches the destination node or a node that has a route to the destination node in its routing table. When the destination node receives the RREQ packet, it sends a Route Reply (RREP) packet back to the source node, containing the address of the next-hop node on the route to the destination. Once the source node receives the RREP packet, it sends data packets to the destination node using the route specified in the RREP packet [26]. The nodes along the route update their routing tables to reflect the new route, and the route is maintained if data packets are sent. If the route is not used for a certain period, it is removed from the routing tables. In the context of VANET, the traditional AODV routing protocol is considered unsecured due to its lack of a monitoring mechanism for security [31]. While AODV has a route-maintained procedure that identifies broken links, it does not monitor the behavior of nodes, leaving the network vulnerable to attacks. Therefore, new novel secure techniques are required to ensure secure communication in VANETs, such as the use of cryptographic methods to authenticate and encrypt messages, intrusion detection systems, an anomaly detection method, e.g., Local Outlier Factor (LOF), and trust management systems to monitor the behavior of nodes and ensure the reliability of the network. By employing these new techniques, VANETs can become more secure and reliable for their intended applications.

The rest of this paper is organized as follows: Section 2 introduces the related work, providing an overview of existing research in the field. Section 3 presents the materials and methods employed in this study, including a detailed explanation of the system model. Section 4 describes the experimental design and simulation setup used to validate our approach. Subsequently, Section 5 presents the results obtained from our experiments, offering comprehensive data analysis. Finally, in Section 6, we draw conclusions based on our findings and discuss future directions for research.

2 Related Work

This section consists of two subsections. The first subsection includes background information on routing protocols in VANETs, focusing on the AODV protocol. The AODV protocol is frequently used in VANETs [32]; however, its drawbacks render it susceptible to assaults and lower its dependability in dynamic network situations. The second part examines the current research on secure routing techniques for VANETs. The literature study underlines the problems of building safe and reliable routing protocols for VANETs and explores many ways to meet these issues. These methods include reputation-based processes, trust management systems, and machine learning strategies [33]. The literature study offers valuable context for the proposed AODV-RL protocol, which upgrades the current AODV protocol with reputation and Local Outlier Factor (LOF)-based methods to increase the reliability and security of communication in VANETs.

2.1 Literature Review on Secure Routing Protocols for VANETs

VANETs, including BHA, are highly vulnerable to attacks due to their dynamic and open nature. BHA are particularly severe as they can cause significant disruption to the network's communication and routing protocols [34,35]. Several studies have been conducted to detect and prevent BHA in VANETs, focusing on the widely used AODV routing protocol. Proposed detection mechanisms rely on detecting inconsistencies in the nodes' routing tables or using cryptographic mechanisms to prevent the insertion of false routing information [36]. However, these mechanisms often suffer from high overhead and reduced network performance [37]. Therefore, there is a need for more efficient and effective detection and prevention mechanisms that can be integrated with the AODV routing protocol to mitigate the impact of BHA in VANETs. In [38], the authors proposed a secure AODV routing protocol to detect and prevent single and cooperative BHA in VANETs. To achieve this, they added a validity value to the RREP without altering the fundamental mechanism of AODV. Simulation results showed that the proposed protocol outperformed the original AODV against BHA. However, the method was ineffective against intelligent adaptive black hole nodes that could falsely claim to have the shortest route by setting the validity value similarly. The authors in [39] proposed modifying the AODV routing protocol for VANETs to enhance its security against BHA. Their modification involved adding a neighbor credit table to each node in the network.

This table records the credit value of a neighbor node each time it sends or forwards a data packet, with genuine nodes receiving higher credit values than untrustworthy ones. Before utilizing a neighbor node for message transmission, a node checks its credit value in the table; if it lacks sufficient credit, the neighbor node is considered untrustworthy, and an alternative hop is used. This approach aims to increase the security of AODV in VANETs. This study introduces the Neighbor Credit Value-based AODV (NCV-AODV) algorithm to mitigate selfish behavior. It accurately detects misbehavior in active networks using neighbor credit values. False positives are prevented by simulating dummy traffic black. In [40], the authors proposed an extension to the acknowledgment-based approach for securing communication in VANETs. The proposed method includes selecting energy-efficient intermediate nodes for communication, establishing session key agreements, implementing a counter-based end-to-end acknowledgment cycle, and authenticating acknowledgment packets using message digest. The approach offers the benefit of differentiating between malicious, selfish, and low-energy nodes. However, the increased network load due to additional acknowledgment packets is a disadvantage that may lead to network congestion black. In [41], the authors introduced a new routing protocol based on TOR for VANETs. This protocol dynamically creates groups of vehicles around specific locations to act as cryptographic onion relays. Its primary objective is to maintain source, destination, and route anonymity. However, the efficacy of this approach relies on the existence of a trusted entity responsible for generating and distributing asymmetric keys in the form of certificates. The study presents a novel anonymous onion-based routing protocol. A new concept of dynamic relay groups that form around specific locations to enhance privacy and anonymity. Vehicle anonymity is maintained through the anonymity of source, destination, and route. black The authors in [42] proposed a technique for detecting black hole nodes in VANETs using bait timers in all nodes. This technique involves setting a random timer, called a baiting timer, which launches broadcasts with fake IDs once it reaches the set time. The black hole node responds to all requests regardless of authenticity and will reply to these fake requests. The sending node can then identify the black hole and record its information in a specific table. Subsequently, when legitimate requests are launched, malicious nodes can be identified and disregarded based on the information in the black hole node table. This paper introduces an enhanced AODV routing protocol with timers and baiting techniques for detecting and isolating black hole attacks. Black hole nodes can be countered through dynamic integration, maintaining network functionality. Effective detection is demonstrated while Maintaining throughput, Delay, and PDRblack. Table 2 provides a summary of the pertinent literature contributed by different researchers. Moreover, it offers a comparison of our research findings with those of various researchers, highlighting the advantages and limitations.

Table 2: Comparison of our work with related studies

Reference	Technique	Advantage	Limitations	Routing protocol	Simulator
[43]	Detect IDS	Anomaly-based methods are highly effective in detecting BHA.	Nodes can operate promiscuously; promiscuous mode can compromise system security.	AODV	NS 2.35
[44]	Dynamic threshold	Detecting BHA during route discovery can isolate clever BHA.	During BHA detection, sending extra packets to identify malicious nodes can increase overhead and network traffic.	AODV	Simulator NS2
[45]	Feature selection for BHA	Anomaly-based techniques exhibit high precision in detecting BHA.	Enabling nodes to monitor network traffic for analysis passively can make the system vulnerable to attacks and undesirable for the nodes.		Glomosim
[46]	(ACK)-based	Detection method is efficient.	The network may experience increased congestion due to additional acknowledgment packets.	AODV	NS2
[47]	Frame-checking sequence	Can identify black and gray hole attacks.	The procedure is time-consuming and involves high computational complexity	invincible AODV	NS 2.35

(Continued)

Table 2 (continued)

Reference	Technique	Advantage	Limitations	Routing protocol	Simulator
[48]	BHA IDS using SVM ML	High accuracy of detection.	The simulation was conducted on a network with only seven nodes,only with one attacker. In real-word network it may not demonstrate the same results.	AODV	OMNET++
[49]	Machine Learning based IDS	Analyzes intrusion detection mechanisms and provides a comparison with an approximation of their performance.	During BHA detection, sending extra packets to identify malicious nodes can increase overhead and network traffic.	AODV	NS-3.25
This study	Reputation-based mechanism LOF	Combines reputation assessment and LOF for enhanced security, offering robust defense against BHA and ensuring reliable data transmission.	Not tested in real-world scenarios.	AODV	NS-2.33

3 Material and Methods

This section discusses the proposed research methodology and background of VANET-based routing protocols, including AODV routing protocols and their types. Also, we discuss the BHA. The AODV protocol faces several security weaknesses and difficulties, mainly due to the source node's lack of knowledge about the intended destination. This feature makes VANETs more vulnerable to different security attacks, including the specific type known as BHA. BHA is categorized as a Denial of Service (DoS) attack aiming to disrupt network services [50,51]. A BHA stands out as a highly aggressive cyber attack. Within VANETs, it is recognized as a complete packet drop attack. In the context of a BHA, routing protocols are exploited to steer data toward the malicious node. Regardless of whether the routing table is scrutinized, active nodes expose the presence of alternative routes [52]. In this situation, a malicious node can constantly intercept a routing request. Consequently, there is a need to either alter or discard the data packets. Moreover, flood-dependent protocols introduce a vulnerability where the requesting node receives deceitful responses from malicious nodes before receiving legitimate replies from actual nodes. This leads to the creation of fabricated and harmful routes. Once a route is established, the node must decide whether to transmit the packet to an unfamiliar destination or discard it [53,54]. Despite lacking a legitimate route to the destination, the black hole node successfully deceives the source node by falsely claiming to possess a valid, efficient, and recently updated route to the intended destination node [55]. As shown in Fig. 3, when the black hole node assumes the identity of the source node, it positions itself along the path connecting the actual source node and its intended target.To determine whether a path has been established, the source node begins transmitting data packets to the black hole node [56,57], eventually dropping all data packets without forwarding them to the destination node.

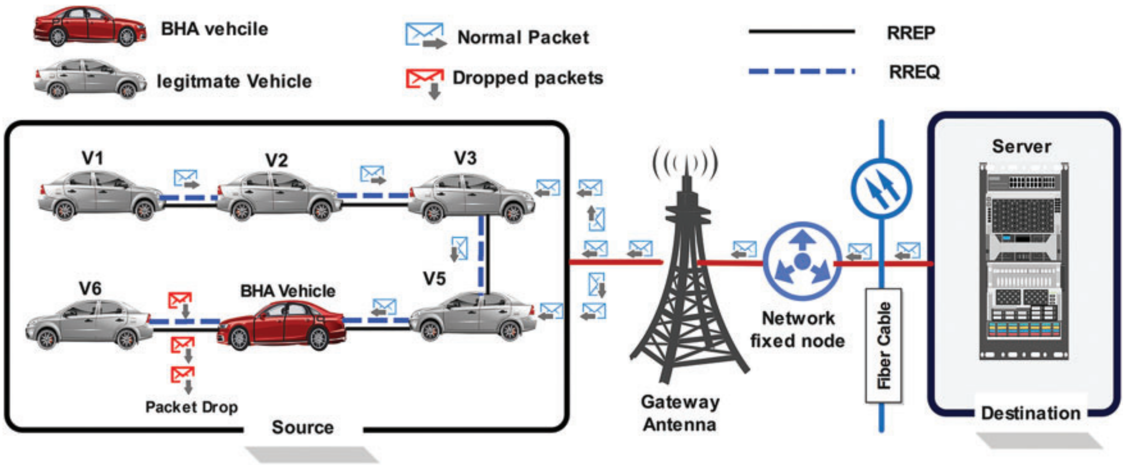


Figure 3: Black hole node attack in VANET

3.1 Node Trust Score Calculation and Proposed Reputation-Based Routing Protocol

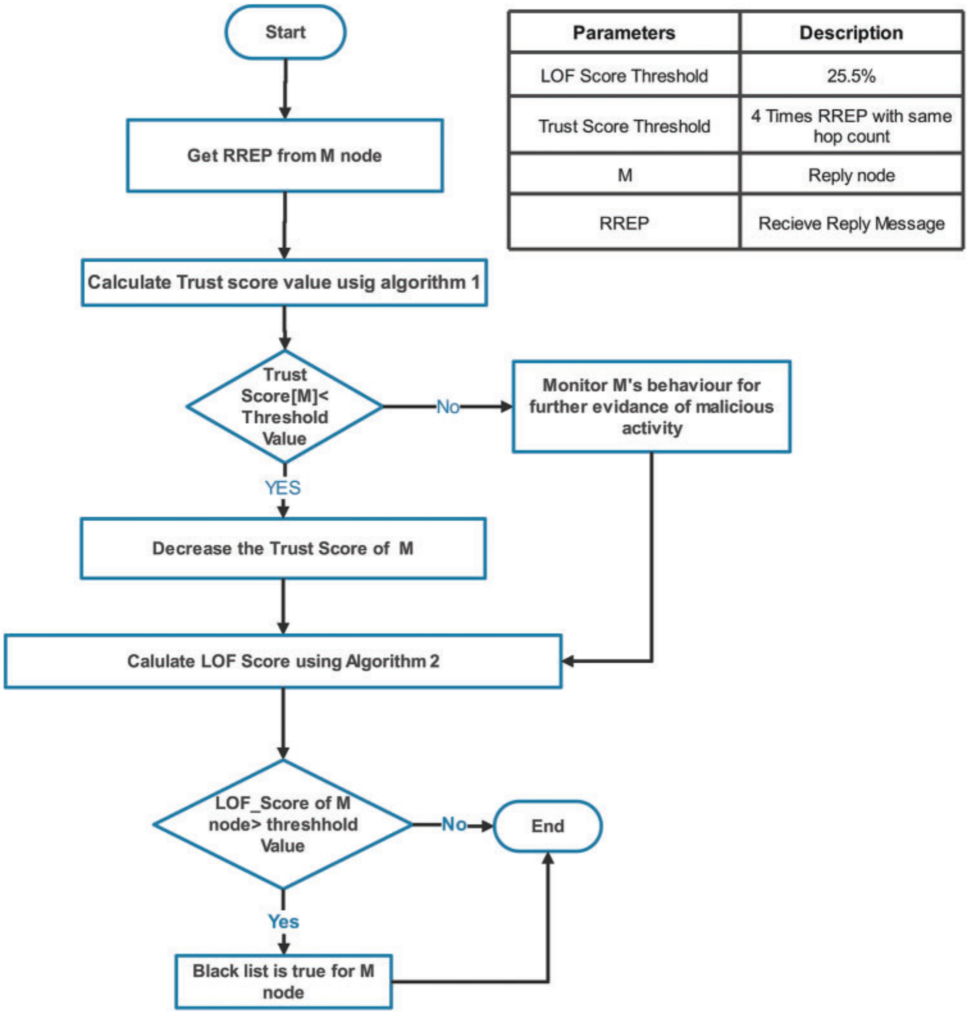
The trust score of a node is calculated based on three factors: message transmission quality, message accuracy, and consistency of the node's behavior in the network. (a) Message transmission quality: This factor reflects the ability of a node to transmit messages accurately and reliably in the network. The weight assigned to this factor should reflect its importance in achieving the goals of the trust-based routing algorithm. (b) Message accuracy: This factor reflects the accuracy of the information in messages transmitted by a node. The weight assigned to this factor should reflect the importance of message accuracy in achieving the goals of the trust-based routing algorithm. (c) Consistency of behavior: This factor reflects the consistency of a node's behavior in the network over time. The weight assigned to this factor should reflect the importance of consistency in achieving the goals of the trust-based routing algorithm. The trust score is typically calculated as the product of these three factors, with an additional weighting factor applied to each factor to reflect its relative importance. As Eq. (1) shows, where w1, w2, and w3 are weighting factors that reflect the relative importance of each factor. These factors can be adjusted to give weight to each factor based on the network's requirements.

$$\text{Trust\_score} = w_1 \times \text{message\_transmission\_quality} + w_2 \times \text{message\_accuracy} + w_3 \times \text{consistency\_score} \tag{1}$$

Each weighting factor should be a value between 0 and 1, and the sum of all weighting factors should be equal to 1. The exact values assigned to each weighting factor will depend on the specific requirements of the network and the goals of the trust-based routing algorithm.

3.2 Integrated Flowchart: Detecting Malicious Nodes through Combined Algorithmic Approaches

Fig. 4 presents a table and a flowchart that describe the working principle of the proposed AODV-RL routing protocol. As AODV-RL is a modified version of the traditional version of AODV, we skipped all other working procedures and only focused on the main part of the modified AODV for our proposed work in Fig. 4. The table lists the parameters and their descriptions used in the protocol and their descriptions used in the protocol.


Start
Get RREP from M node
Calculate Trust score value usig algorithm 1
Trust Score[M]< Threshold Value
No
Monitor M's behaviour for further evidance of malicious activity
YES
Decrease the Trust Score of M
Calulate LOF Score using Algorithm 2
LOF_Score of M node> threshhold Value
No
End
Yes
Black list is true for M node

Parameters	Description
LOF Score Threshold	25.5%
Trust Score Threshold	4 Times RREP with same hop count
M	Reply node
RREP	Recieve Reply Message

Figure 4: Visual representation of algorithmic workflows

The M node is assumed to be a Reply Node, and the source node is supposed to receive a route reply message (RREP) from the M node. The Trust Score Threshold is assumed to 4 times the RREP with the same hop count. The AODV-RL employs a double check by utilizing the Local Outlier Factor (LOF) algorithm to calculate a score threshold of 25.5% to identify potentially malicious nodes. The flowchart shows the working principle of the proposed algorithms used in the AODV-RL routing protocol. Algorithm 1 is used to calculate the Trust Score Value, which is used to evaluate the trustworthiness of nodes based on their historical behavior. The protocol monitors the behavior of the M node for further evidence of malicious activity and decreases its Trust Score if necessary. Algorithm 2 calculates the LOF Score, which is used to double-check the behavior of nodes flagged as potentially malicious by the reputation-based mechanism. Overall, the proposed AODV-RL protocol enhances the security and reliability of communication in VANETs by identifying and avoiding malicious nodes and providing a secure and reliable communication framework for various applications, such as network traffic management, emergency response, and autonomous driving scenario.

3.3 Algorithms of Reputation-Based Routing Protocol

The use of the trust score in VANETs can provide several potential benefits, including improved routing efficiency, reduced vulnerability to attacks, and increased resilience to network failures. By identifying the network's most reliable and trustworthy nodes, routing algorithms can be optimized to select the most efficient and secure paths between nodes, improving overall routing efficiency. By blacklisting nodes with low trust scores, the network can be protected against potential attacks or malicious nodes, reducing vulnerability to security threats. Finally, by using the trust score to identify the most reliable nodes, the network can be more resilient to node failures or other types of network failures, ensuring that the network continues functioning even if some nodes are unavailable.

The efficiency of Algorithm 1 (see Appendix A) in big O notation is analyzed as follows: Lines 2–5 initialize the reputation and routing table for each node, resulting in a time complexity of O(n). The RREQ function (Lines 6–17) broadcasts a message to all neighbors, and its time complexity depends on the number of neighbors. Assuming a fully connected network, this function's time complexity is O(n2). The RREP function (Lines 18–36) involves updating the routing table and reputation scores, and its time complexity is also dependent on the number of neighbors. Assuming a fully connected network, this function's time complexity is also O(n2). The RRSE function (Lines 37–45) involves selecting the best route based on reputation score and distance, resulting in a time complexity of O(nLogn) due to the use of sorting algorithms. Therefore, the computational time complexity of the proposed algorithm is O(n)+O(n2) + O(n2) + O(nLogn), which simplifies to O(n2).

3.4 Local Outlier Factor (LOF): A Machine Learning-Based Algorithm for VANET Security

In VANETs, identifying nodes that exhibit abnormal behavior or may be potentially malicious is crucial for enhancing network security and reliability. Local Outlier Factor (LOF) is a widely used machine learning algorithm that can effectively detect such nodes. LOF evaluates the local density of each node by comparing it to the local densities of its k-nearest neighbors. The algorithm 2 (see Appendix B) can be divided into two primary steps: calculating the local reachability density of each data point and calculating the local outlier factor of each data point. To accomplish these steps, LOF relies on four equations. Eq. (1) calculates the Euclidean distance between two data points(Nodes), which is used to determine the k-nearest neighbors of a data point x. Eq. (2) increments the hop count variable by 1 each time the Euclidean distance function recursively calls itself to search for the k-nearest neighbors within a certain hop count h. Eq. (3) calculates the local reach-ability density of a data point, which is used to measure the local density around the point. Eq. (4) calculates the local outlier factor of a data point, which is used to identify potential anomalies or malicious nodes in the dataset.

The integration of LOF in AODV-RL enhances the security of VANETs by providing an additional layer of detection for potentially malicious nodes beyond the reputation-based mechanism. LOF evaluates the local density of each node and can identify nodes that exhibit abnormal behavior or deviate significantly from their neighbors in terms of their network behavior. LOF plays a specific role in detecting previously unknown or undetected malicious nodes that may have been missed by the reputation-based mechanism. By calculating the local outlier factor of each data point, LOF can identify nodes with high LOF values as potential outliers or malicious nodes that require further investigation or isolation from the network. Therefore, the integration of LOF in AODV-RL provides an effective way to enhance the overall security and reliability of VANETs.

$$\text{distance} = \sqrt{\sum (x_1(i) - x_2(i))^2} \tag{2}$$

$$\text{hop\_count} = \text{hop\_count} + 1 \tag{3}$$

$$\text{LRD}(x) = \frac{k}{\sum \frac{\text{dist\_}k(x,h)}{\text{dist}(x,p,h)}} \tag{4}$$

$$\text{LOF}(x) = \frac{\sum \frac{\text{lrd}(p,h)}{\text{lrd}(x,h)}}{k} \tag{5}$$

The Euclidean distance function has a time complexity of $O(d)$, where d is the number of dimensions of the data points being compared. The LRD function loops through all data points, which results in a time complexity of $O(n^2)$, where n is the number of data points. However, since it only considers the k nearest neighbors, the actual time complexity can be lower, roughly $O(nk\log(k))$. The LOF function also loops through all data points, resulting in a time complexity of $O(n^2)$. Similar to the LRD function, the actual time complexity can be lower, roughly $O(nk\log(k))$. Overall, the time complexity of the algorithm can be estimated as $O(n^2 \cdot k \cdot \log(k) \cdot d)$, where n is the number of data points, k is the number of nearest neighbors to consider, and d is the number of dimensions of the data points.

4 Experimental Design and Simulation Setup

In this section, we have discussed the experimental design and simulation methodology.

4.1 Simulation Tools Description

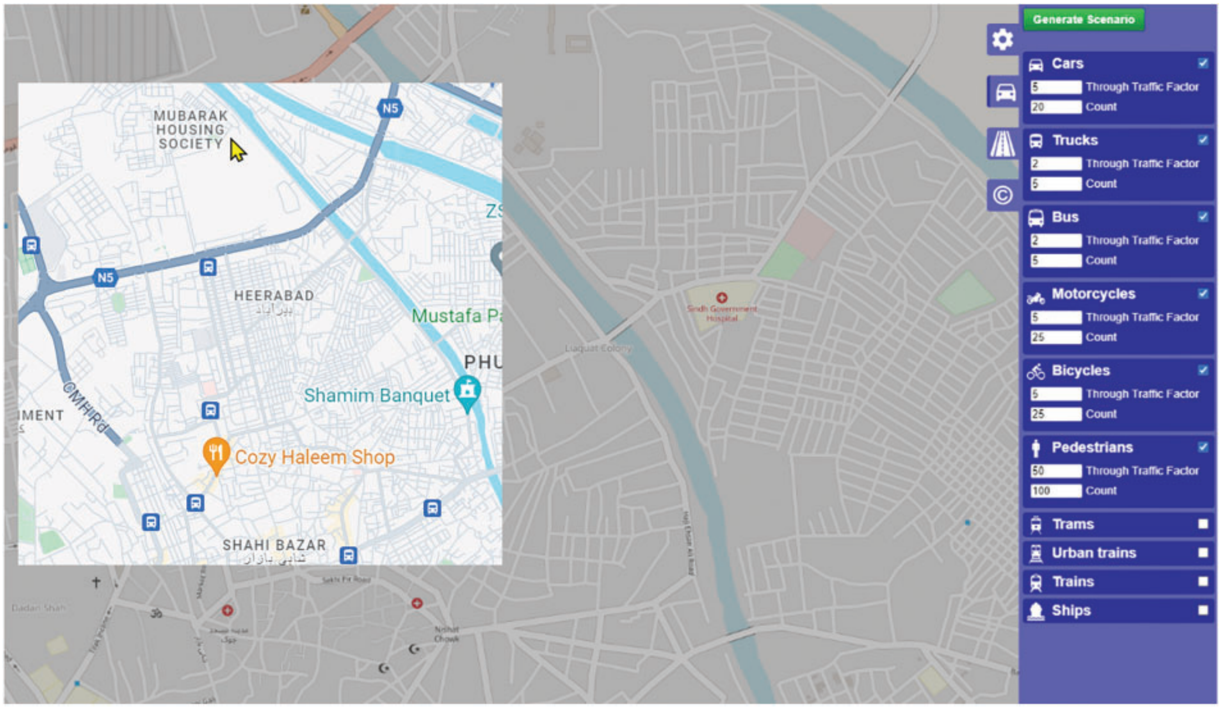
The simulation setup section describes the experimental environment and the tool used to evaluate the performance of the VANET scenario [58]. In this study, we used Network Simulator Tool version 2.33 [59] to simulate the VANET scenario. NS-2.33 is a widely used open-source network simulator that allows researchers to evaluate the performance of various network protocols and algorithms in different network scenarios. We configured NS-2.33 with the appropriate protocols and parameters for the VANET scenario to ensure our simulation was accurate, specifically, the AODV-RL routing protocol for packet forwarding and the network interface type WirelessPhyExt with 5.9 GHz frequency. We also set the simulation parameters based on the characteristics of the VANET scenario. For example, we set the simulation time to 1000 s to allow for a sufficient amount of data to be collected, and we set the packet size to 1000 bytes to simulate realistic network traffic. Table 3 shows Simulation Parameters for the proposed work. The simulation parameters table summarizes the key parameters used in the VANET scenario simulation. These parameters include the network simulator version, routing protocols, MAC protocol, network topology, number of nodes, simulation time, signal bandwidth, packet size, and QoS metrics.

Table 3: Simulation parameters

Parameter	Values
NS2	2.33
Routing protocols	Normal AODV, AODV-RL, D_BH_AODV [55], FA-AODV [54], OEAODV [57]
MAC protocol	802.11 p
Frequency	5.9 GHz
Network interface type	Phy/WirelessPhyExt
Number of nodes	375
Number of RSU	1
Number of internet servers	2
Simulation time	750 s
Topology area	3000 × 3000 (m^2)
Signal bandwidth	10 MHz
SIFS	32 μs
SlotTime	13 μs
CWMax	1023
CWMin	15
ShortRetryLimit	7
LongRetryLimit	4
Gain/loss factor	1
Noise	−99 dBm
CSThresh	−94 dBm
Power transmission	20 dBm
Packet size	512 bytes
CBR rate	1 Mbps
Average call duration of one pair	Varying from 40 to 200 s
Average mobility	Varying from 0.5 to 20 m/s
Type of vehicles	Various
Attacker node assumed	Bicycle node

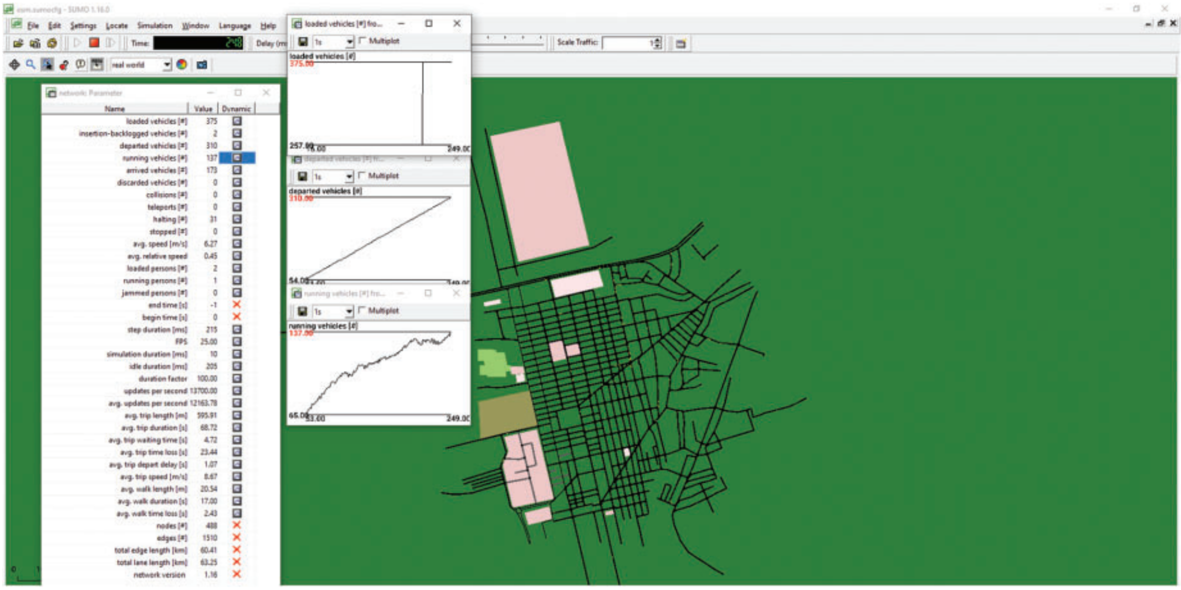
The VANET scenario used five routing protocols: Normal AODV, AODV-RL, D_BH_AODV, FAAODV, and OEAODV. The MAC protocol used in the simulation was 802.11p, designed for vehicular networks. The simulation was conducted with 375 nodes and one roadside unit (RSU), with a topology area of 3000 × 3000 square meters. The simulation time was set to 750 s, and the signal bandwidth was set to 10 MHz. The simulation used a noise level of –99 dBm, a carrier sense threshold (CSThresh) of –94 dBm, and power transmission of 20 dBm. For traffic patterns, Pascal language developed a traffic generator [60], and the following are employed; it has been used in several previous studies [61,62]. This traffic generator can create a traffic pattern in TCL format, supporting end-user coding in NS2. Furthermore, we have used SUMO [63] and open-street MAP [64] for mobility generating of VANET, as shown in their capturing images. Different vehicles were simulated in the

VANET scenario, as shown in the OpenStreetMap Fig. 5. A move-able attacker node was also assumed in the simulation, represented by a bicycle node Fig. 6. SUMO simulation scenario of 375 Loaded vehicles and other parameters.



		Through Traffic Factor	Count
Cars	☑	5	20
Trucks	☑	2	5
Bus	☑	2	5
Motorcycles	☑	5	25
Bicycles	☑	5	25
Pedestrians	☑	50	100
Trams	□		
Urban trains	□		
Trains	□		
Ships	□		

Figure 5: OpenStreetMap scenario of Heerabad, Hyderabad area with number of vehicles



Name	Value	Dynamic
loaded vehicles [#]	375	▣
insertion-backlogged vehicles [#]	2	▣
departed vehicles [#]	310	▣
running vehicles [#]	137	▣
arrived vehicles [#]	173	▣
discarded vehicles [#]	0	▣
collisions [#]	0	▣
teleports [#]	0	▣
halting [#]	31	▣
stopped [#]	0	▣
avg. speed [m/s]	6.27	▣
avg. relative speed	0.45	▣
loaded persons [#]	2	▣
running persons [#]	1	▣
jammed persons [#]	0	▣
end time [s]	-1	✗
begin time [s]	0	✗
step duration [ms]	215	▣
FPS	25.00	▣
simulation duration [ms]	10	▣
idle duration [ms]	205	▣
duration factor	100.00	▣
updates per second	13700.00	▣
avg. updates per second	12163.78	▣
avg. trip length [m]	595.91	▣
avg. trip duration [s]	68.72	▣
avg. trip waiting time [s]	4.72	▣
avg. trip time loss [s]	23.44	▣
avg. trip depart delay [s]	1.07	▣
avg. trip speed [m/s]	8.67	▣
avg. walk length [m]	20.54	▣
avg. walk duration [s]	17.00	▣
avg. walk time loss [s]	2.43	▣
nodes [#]	488	✗
edges [#]	1510	✗
total edge length [km]	60.41	✗
total lane length [km]	63.25	✗
network version	1.16	✗

Figure 6: SUMO simulation scenario of 375 vehicles and other parameters

4.2 Performance Metrics

To thoroughly evaluate the performance of the VANET scenario and compare the effectiveness of different routing protocols, we conducted 200 simulation runs. During each simulation run, we varied the quality of service (QoS) metrics, other routing protocols, and traffic load to ensure comprehensive coverage of the simulation space. The quality of service metrics used in this study included throughput, Packet Delivery Ratio (PDR%), Normalized Routing Load (NRL%), and packet loss ratio (PLR%).

Throughput: Throughput is the measure of the amount of data that can be transmitted or processed within a given time, and it is commonly expressed in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps). It can be calculated using the following equation:

$$\text{Throughput (bps)} = \frac{\text{Amount of data (bits)}}{\text{Time (s) taken for transfer}} \tag{6}$$

Packet Delivery Ratio%: PDR% is a key performance metric used to assess the reliability of a communication system in terms of packet transmission [65]. In the context of our research work based on AODV-RL, PDR% refers to the percentage of successfully transmitted packets out of the total number of packets sent. Eq. (7) presents the calculation of PDR in percentile (%) because it is a ratio.

$$\text{PDR\%} = \left(\frac{\text{Number of successfully received packets}}{\text{Total number of transmitted Packets}}\right) \times 100 \tag{7}$$

Normalized Routing Load: NRL% measures the network's ability to maintain connectivity and ensure reliable communication. NRL is evaluated to assess the impact of routing protocols overhead on the overall network performance. NRL% is calculated as in Eq. (8):

$$\text{NRL\%} = \frac{\text{No. of Routing Packets generated}}{\text{No. of data packets transmission}} \times 100 \tag{8}$$

Packet Loss Ratio%: PLR % is a metric used to evaluate the reliability of a communication system, and it represents the percentage of packets lost during transmission. PLR measures the percentage of packets lost during transmission, calculated by Eq. (9).

$$\text{Packet loss rate \%} = \left(\frac{\text{No. of Sent packets} - \text{No. of Received packets}}{\text{Total number of transmitted Packets}}\right) \times 100 \tag{9}$$

5 Results

The simulation experiments revealed essential insights into the performance of different routing protocols in the VANET scenario and compared their effectiveness in achieving reliable and efficient communication among vehicles and internet servers. We evaluated the performance of five routing protocols for different traffic loads and QoS metrics, including Normal AODV, AODV-RL, D_BH_AODV, FA-AODV, and OEAODV. The simulation results show that the choice of routing protocol significantly impacts the performance of the VANET scenario, with some protocols consistently outperforming others across all QoS metrics. In this section, we present the detailed results of our simulation experiments, and we also compare our results with those of existing protocols in the literature to provide a comprehensive evaluation of the effectiveness of protocols in the VANET scenario.

5.1 Throughput vs. Traffic Load in Pair

Fig. 7 shows the results of throughput for five different routing protocols, AODV-RL, D_BH_AODV, FA-AODV, Normal AODV, and OEAODV, under different traffic loads. The throughput values represent the total data transmitted over the network per unit of time (per second) in kbps. The graph shows that the highest throughput values are achieved by AODV-RL, and OEAODV achieves the lowest values. As the traffic load increases, the throughput values increase for all routing protocols. However, the rate of increase varies between the different protocols. Under a traffic load of 1 pair, Normal AODV has the highest throughput value of 338.96 kbps, while OEAODV has the lowest value of 40.933 kbps. However, as the traffic load increases, our proposed AODV-RL consistently outperforms the other routing protocols, achieving the highest throughput across all traffic loads. When we look under a traffic load of 50 pairs (i.e., 100 vehicles connected simultaneously), AODV-RL has a throughput is 36.18% higher than OEAODV (5,321.56 kbps *vs*. 3,907.815 kbps). The study's results demonstrate that the performance of routing protocols varies significantly across different traffic loads. D_BH_AODV exhibits strong performance under low traffic loads but deteriorates considerably under high traffic loads. Conversely, FA-AODV performs well under moderate to high traffic loads but experiences poor performance levels under low traffic loads. A comparison of the performance of these protocols to the proposed AODV-RL, under a traffic load of 50 pairs, indicates that AODV-RL attains the highest throughput value among all protocols. Specifically, D_BH_AODV and FA-AODV achieve 6.03% and 26.86% lower total throughput values than AODV-RL, respectively. Notably, under the same traffic load, Normal AODV achieves a total throughput of 5,524.13 kbps, 3.77% higher than the total throughput achieved by AODV-RL. Two main reasons for lower throughput in VANET networks are congestion and attacks, which can block or drop data, preventing it from reaching its destination [66]. In this study, a traffic load of 50 pairs is insufficient to fully congest the network, as only 100 nodes were communicating, and the remaining nodes were forwarding data due to the open nature of VANET networks. However, attacks can significantly impact network performance, leading to lower throughput. A more secure routing protocol, such as the proposed AODV-RL, can prevent attacks and enable successful data transmission, resulting in higher throughput. The proposed AODV-RL is more robust than other existing protocols due to its double-check mechanism for identifying and preventing attackers, as evidenced by the lower packet loss ratio in Fig. 7.

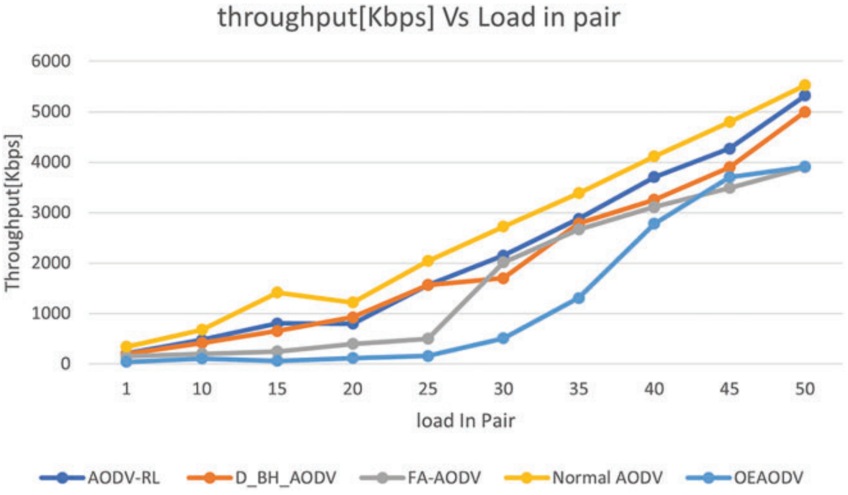


Figure 7: Throughput *vs.* load in pair

5.2 PDR % vs. Traffic Load in Pair

Fig. 8 shows the PDR% results of packets successfully delivered to their intended destination for each routing protocol under different traffic loads. Fig. 8 shows that AODV-RL achieves the highest PDR% across all traffic loads, with the lowest value achieved by OEAODV. As the traffic load increases, the PDR% values for all routing protocols tend to decrease. Under a traffic load of 1 pair, Normal AODV has the highest PDR% value of 96.22%, while OEAODV has the lowest value of 68.37%. However, as the traffic load increases, our proposed AODV-RL consistently outperforms the other routing protocols, achieving the highest PDR% across all traffic loads. When we look under the highest traffic load of 50 pairs, AODV-RL has a PDR% of 94.25%, which is 4.75% higher than OEAODV (89.5%). The PDR% results of the study demonstrate that the performance of routing protocols varies significantly across different traffic loads. D_BH_AODV exhibits strong performance under low traffic loads but deteriorates considerably under high traffic loads. Conversely, FA-AODV performs well under moderate traffic loads but experiences poor performance levels under low and high traffic loads. Comparison of the performance of these protocols to the proposed AODV-RL, under a traffic load of 50 pairs, indicates that AODV-RL attains the highest PDR% among all protocols. Specifically, D_BH_AODV and FA-AODV achieve 2.94% and 5.29% lower PDR% values than AODV-RL, respectively. The reasons for the higher and lower PDR% values are related to the mechanisms used by each routing protocol to ensure reliable data transmission in VANET networks. A more robust and secure routing protocol, such as AODV-RL, can prevent attacks and enable successful data transmission, resulting in higher PDR%. In contrast, less secure protocols, such as OEAODV, may experience packet loss due to not preventing attacks in the network, resulting in lower PDR%.

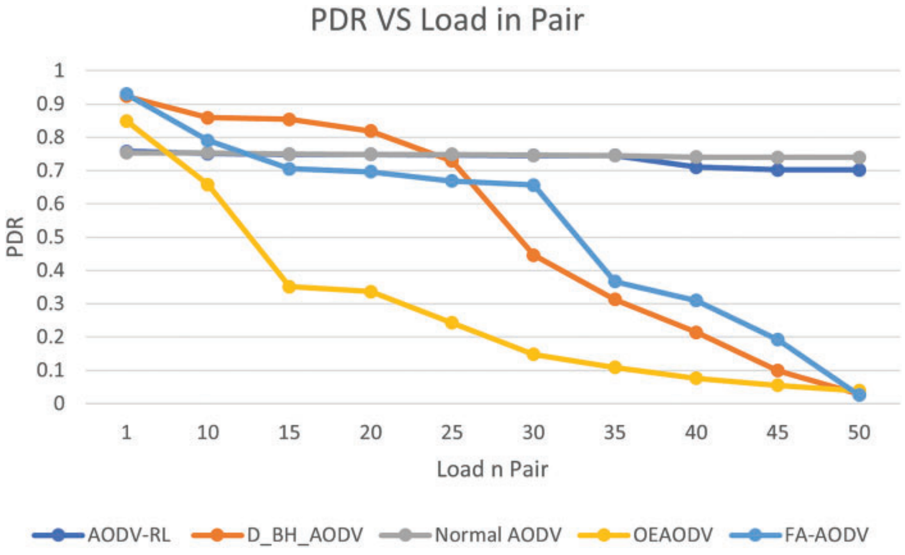


Figure 8: PDR *vs*. load in pair

5.3 NRL% vs. Traffic Load in Pair

Fig. 9 shows the normalized routing load generated by each routing protocol under different traffic loads. Based on the results of Fig. 9, we observe that AODV-RL consistently achieves the lowest NRL% across all traffic loads, indicating that it is more efficient in routing protocol overhead than other routing protocols. Under a traffic load of 1 pair, Normal AODV has the lowest NRL% value of 0.070%, while OEAODV has the highest value of 0.067%. However, as the traffic load increases, our proposed AODV-RL consistently outperforms the other routing protocols, achieving the lowest NRL% across all traffic loads. When we look under a traffic load of 50 pairs, AODV-RL has an NRL% of 0.333%, which is 1.46% lower than D_BH_AODV (0.338%) and 4.99% lower than OEAODV (0.352%). The NRL% results of the study demonstrate that the performance of routing protocols varies significantly across different traffic loads. D_BH_AODV exhibits strong performance under low traffic loads but deteriorates considerably under high traffic loads. Conversely, FA-AODV performs well under moderate to high traffic loads but experiences poor performance under very low traffic loads. Comparison of the performance of these protocols to the proposed AODV-RL, under a traffic load of 50 pairs, indicates that AODV-RL attains the lowest NRL% among all protocols. Specifically, D_BH_AODV and FA-AODV achieve 1.51% and 2.59% higher NRL% values than AODV-RL, respectively. Notably, under the same traffic load, Normal AODV performs an NRL% of 0.834%, which is 0.501% higher than the NRL% achieved by AODV-RL. The reasons for the lower NRL% values in the table are related to the mechanisms used by each routing protocol to minimize the routing protocol overhead in VANET networks. A more efficient and optimized routing protocol, such as AODV-RL, can reduce the number of control packets generated and transmitted, resulting in lower NRL%. The lower NRL% achieved by AODV-RL compared to other existing protocols demonstrates its ability to minimize routing protocol overhead, resulting in a more efficient and optimized communication system.

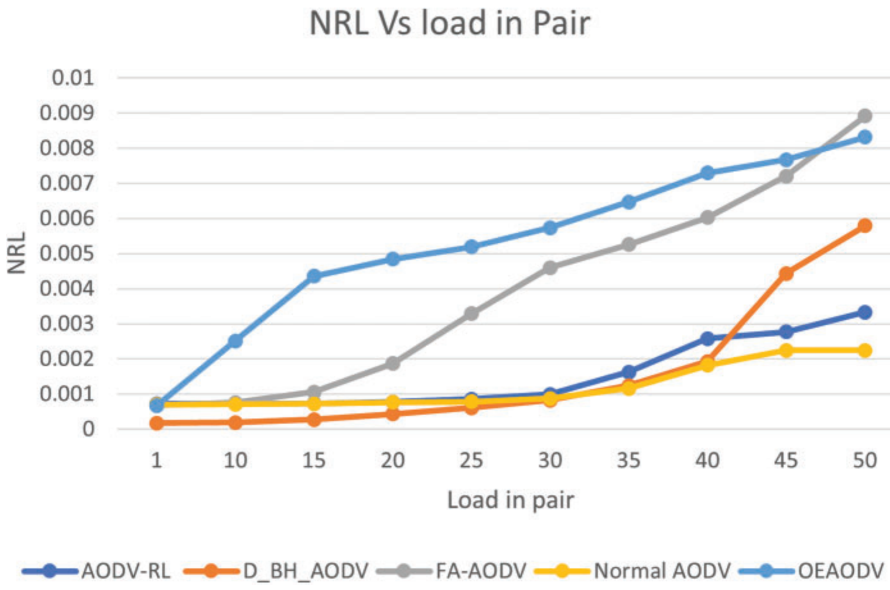


Figure 9: NRL% PDR *vs*. load in pair

5.4 PLR % vs. Traffic Load in Pair

A lower PLR % indicates that a routing protocol is more efficient in delivering data packets with lower packet loss rates. Fig. 10 compares the five routing protocols regarding the Packet Loss ratio, which is in percentile value (%) of data packets lost during transmission by each routing protocol under different traffic loads. Furthermore, in Fig. 10, we also observe that AODV-RL consistently achieves the lowest Packet Loss ratio % across all traffic loads, indicating that it is more efficient regarding data packet delivery than other routing protocols. In contrast, different routing protocols FA-AODV, D_BH_AODV, and OEAODV, generate the highest Packet Loss ratio % values, indicating they have the highest data packet loss rates. Under a traffic load of 1 pair, Normal AODV has the highest Packet Loss ratio % value of 24.65%, while D_BH_AODV has the lowest value of 7.6%. However, as the traffic load increases, our proposed AODV-RL consistently outperforms the other routing protocols, achieving the lowest Packet Loss ratio % across all traffic loads. AODV-RL has a Packet Loss ratio % of 0.297%, which is 69.16% lower than OEAODV (0.961%) and 69.42% lower than FA-AODV (0.974%) at the highest traffic load. The study's Packet Loss ratio % results demonstrate that the performance of routing protocols varies significantly across different traffic loads. D_BH_AODV exhibits strong performance under low traffic loads but deteriorates considerably under high traffic loads. Conversely, FA-AODV performs well under moderate to high traffic loads but experiences poor performance under low traffic loads. A comparison of the performance of existing routing protocols to the proposed AODV-RL, under a traffic load of 50 pairs, indicates that AODV-RL attains the lowest Packet Loss ratio % among all protocols. Specifically, D_BH_AODV and FA-AODV achieve 61.40% and 69.25% higher Packet Loss ratio % values than AODV-RL, respectively. Notably, under the same traffic load, Normal AODV reaches a Packet Loss ratio % of 25.98%, which is also lower than others. The reasons for the lower Packet Loss ratio % are related to the mechanisms used by each routing protocol to minimize the data packet loss rates in VANET networks. A more secure, efficient, and optimized routing protocol, such as AODV-RL, can reduce the data packet loss rates by selecting more reliable and secure routes. The lower Packet Loss ratio % achieved by AODV-RL compared to other existing protocols demonstrates its ability to minimize data packet loss rates, resulting in a more reliable and efficient communication system.

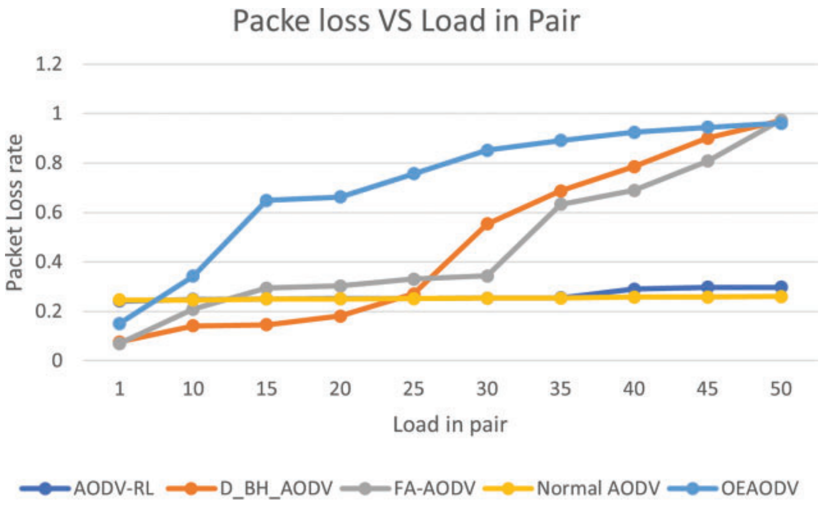


Figure 10: Packet loss rate *vs*. load in pairs

6 Conclusion, Limitations, and Future Directions

This article aims to introduce AODV-RL, a novel routing protocol designed to enhance the reliability and security of communication in VANET. By incorporating reputation and Local Outlier Factor (LOF)-based mechanisms, AODV-RL addresses the challenges posed by dynamic VANET environments, ensuring seamless and efficient communication between vehicles, infrastructure, and other entities involved in transportation. By evaluating AODV-RL under various scenarios, including different traffic loads and mobility speeds, extensive simulation experiments have yielded notable findings. According to our results, the message delivery ratio of AODV-RL is superior to existing routing protocols by as much as 94.25%, with a packet loss ratio of only 0.297%. AODV-RL demonstrates improved message delivery ratios compared to existing routing protocols, signifying its ability to facilitate reliable data transmission across the network. This enhancement in message delivery ratios contributes to the overall robustness and effectiveness of AODV-RL in VANETs. A further benefit of AODV-RL is its ability to identify malicious nodes and isolate them from the network, enhancing security. AODV-RL minimizes potential threats by evaluating the trustworthiness of nodes based on their historical behavior. AODV-RL routing protocol ensures the integrity of communication in VANETs. This contributes to the overall security and reliability of the protocol, making it suitable for various applications such as traffic management, emergency response, and autonomous vehicles. There are several limitations and practical considerations of AODV-RL to be considered. For instance, AODV-RL requires significant training data to optimize its routing decisions, which can be impractical in some scenarios. In addition, the training process for AODV-RL can be time-consuming, resulting in slower convergence times for routes than for traditional routing protocols. The AODV-RL is nevertheless configured to handle varying VANET traffic loads. The scalability of a network depends on several factors, such as its size and density, nodes' mobility, and computing resources. The AODV-RL has shown promising results in simulation studies, but its practical implementation in real-world deployment environments requires careful consideration of these limitations and scalability concerns.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the presentation of this paper.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Nadeem Ahmed, Khalid Mehmodani, Ali Kashif Bashir, Marwan Omar, Angel Jones, and Fayaz; data collection: Khalid Mehmodani; analysis and interpretation of results: Nadeem Ahmed, Khalid Mehmodani, and Ali Kashif Bashir; draft manuscript preparation: Khalid Mehmodani, and Ali Kashif Bashir. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. El Madani, S., Motahhir, S., El Ghzizal, A. (2022). Internet of Vehicles: Concept, process, security aspects and solutions. *Multimedia Tools and Applications, 81(12),* 16563–16587.
2. Smida, K., Tounsi, H., Frikha, M., Song, Y. Q. (2019). Software defined Internet of Vehicles: A survey from QoS and scalability perspectives. *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. Tangier, Morocco, IEEE.
3. Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S. et al. (2022). A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography. *Computers and Electrical Engineering, 102,* 108205.
4. Shafiq, M., Tian, Z., Bashir, A. K., Du, X., Guizani, M. (2021). CorrAUC: A malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet of Things Journal, 8(5),* 3242–3254.
5. Mchergui, A., Moulahi, T., Zeadally, S. (2022). Survey on artificial intelligence (AI) techniques for Vehicular ad hoc NETworks (VANETs). *Vehicular Communications, 34,* 100403.
6. Ahmed, N., Deng, Z., Memon, I., Hassan, F., Mohammadani, K. H. et al. (2022). A survey on location privacy attacks and prevention deployed with IoT in vehicular networks. *Wireless Communications and Mobile Computing, 2022,* 6503299.

7. Yu, H., Liu, R., Li, Z., Ren, Y., Jiang, H. (2021). An RSU deployment strategy based on traffic demand in vehicular ad hoc networks (VANETs). *IEEE Internet of Things Journal, 9(9),* 6496–6505.
8. Azam, F., Yadav, S. K., Priyadarshi, N., Padmanaban, S., Bansal, R. C. (2021). A comprehensive review of authentication schemes in vehicular ad hoc network. *IEEE Access, 9,* 31309–31321.
9. Rashid, S. A., Audah, L., Hamdi, M. M., Abood, M. S., Alani, S. (2020). Reliable and efficient data dissemination scheme in VANET: A review. *International Journal of Electrical and Computer Engineering (IJECE), 10(6),* 6423–6434.
10. Panday, M., Shriwastava, A. (2013). A review on security issues of AODV routing protocol for MANETs. *IOSR Journal of Computer Engineering (IOSR-JCE), 14(5),* 127–134.
11. Magsi, A. H., Yovita, L. V., Ghulam, A., Muhammad, G., Ali, Z. (2023). A content poisoning attack detection and prevention system in vehicular named data networking. *Sustainability, 15(14),* 10931.
12. Kumar, P., Verma, A., Singhal, P. (2019). VANET protocols with challenges-A review. *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, IEEE.
13. Yang, Y., Li, H., Huang, Q. (2013). Mobility management in VANET. *2013 22nd Wireless and Optical Communication Conference*, Chongqing, China, IEEE.
14. Qi, Y., Wu, J., Bashir, A. K., Lin, X., Yang, W. et al. (2022). Privacy-preserving cross-area traffic forecasting in ITS: A transferable spatial-temporal graph neural network approach. *IEEE Transactions on Intelligent Transportation Systems,* 1–14.
15. Cao, Z., Shi, K., Song, Q., Wang, J. (2017). Analysis of correlation between vehicle density and network congestion in VANETs. *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*. Macau, China, IEEE.
16. Rao, B. T., Patibandla, R. L., Narayana, V. L. (2021). Comparative study on security and privacy issues in VANETs. In: *Cloud and IoT-Based Vehicular ad hoc Networks*, pp. 145–162. Austin, Texas: Wiley-Scrivener.
17. Srivastava, A., Verma, S., Jhanjhi, N., Talib, M., Malhotra, A. et al. (2020). Analysis of quality of service in VANET. *IOP Conference Series: Materials Science and Engineering*, vol. 993. Kancheepuram, India, IOP Publishing.
18. Ahmed, E., Gharavi, H. (2018). Cooperative vehicular networking: A survey. *IEEE Transactions on Intelligent Transportation Systems, 19(3),* 996–1014.
19. Safwat, M., Elgammal, A., AbdAllah, E. G., Azer, M. A. (2022). Survey and taxonomy of information-centric vehicular networking security attacks. *ad hoc Networks, 124,* 102696.
20. Kim, H., Chung, J. M. (2022). VANET jamming and adversarial attack defense for autonomous vehicle safety. *Computers, Materials & Continua, 71(2),* 3589–3605. https://doi.org/10.32604/cmc.2022.023073
21. Afzal, Z., Kumar, M. (2020). Security of vehicular ad hoc networks (VANET): A survey. *Journal of Physics: Conference Series, 1427,* 012015.
22. Gayathri, M., Gomathy, C. (2023). Fats (fuzzy authentication to provide trust-based security) in vanetto mitigate black hole attack. In: *Data analytics for Internet of Things infrastructure*, pp. 55–75. Springer.
23. Bangui, H., Ge, M., Buhnova, B. (2022). A hybrid machine learning model for intrusion detection in VANET. *Computing, 104(3),* 503–531.
24. Che, H., Duan, Y., Li, C., Yu, L. (2022). On trust management in vehicular ad hoc networks: A comprehensive review. *Frontiers in the Internet of Things, 1,* 995233.
25. Malakar, M., Bhabani, B., Mahapatro, J. (2023). NS3-based performance assessment of routing protocols AODV, OLSR and DSDV for VANETs. *Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2023*, pp. 1–14. Singapore, Springer.
26. Harrabi, S., Jaafar, I. B., Ghedira, K. (2023). Survey on IoV routing protocols. *Wireless Personal Communications, 128(2),* 791–811.
27. Kumar, S., Singh, J. (2020). Internet of Vehicles over VANETs: Smart and secure communication using IoT. *Scalable Computing: Practice and Experience, 21(3),* 425–440.

28. Ahmed, M. T., Rubi, A. A., Rahman, M. S., Rahman, M. (2021). 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, 8(5),* 524–537.
29. Rahman, M. T., Alauddin, M., Dey, U. K., Sadi, A. S. (2023). Adaptive secure and efficientrouting protocol for enhance the performance of mobile ad hoc network. *Applied Computer Science, 19(3),* 133–159.
30. Shaik, S. (2023). An efficient secured AODV routing protocol to mitigate flooding and block hole attack in VANETs for improved infotainment services. *SEAS Transactions, 2(1).*
31. Sohail, M., Latif, Z., Javed, S., Biswas, S., Ajmal, S. et al. (2023). Routing protocols in vehicular ad hoc networks (VANETs): A comprehensive survey. *Internet of Things, 23,* 100837.
32. Ajjaj, S., El Houssaini, S., Hain, M., El Houssaini, M. (2022). A new multivariate approach for real time detection of routing security attacks in VANETs. *Information, 13,* 282.
33. Gupta, B., Prajapati, V., Nedjah, N., Vijayakumar, P., El-Latif, A. A. A. et al. (2023). Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS). *Neural Computing and Applications, 35(7),* 5055–5080.
34. Malik, A., Khan, M. Z., Faisal, M., Khan, F., Seo, J. T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. *Sensors, 22(5),* 1897.
35. Maurya, H. C., Verma, P. (2023). Comparative study: Routing protocols performance for vehicular ad hoc networks. www.ijsronline.org/, https://www.ijsronline.org/issue/20230303-020425.899.pdf (accessed on 05/05/2023)
36. Dhanaraj, R. K., Islam, S. H., Rajasekar, V. (2022). A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments. *Wireless Networks, 28(7),* 3127–3142.
37. Xiong, W., Wang, R., Wang, Y., Zhou, F., Luo, X. (2021). CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs. *IEEE Transactions on Vehicular Technology, 70(4),* 3456–3468.
38. Deshmukh, S. R., Chatur, P., Bhople, N. B. (2016). AODV-based secure routing against blackhole attack in MANET. *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, IEEE.
39. Rama Abirami, K., Sumithra, M. (2018). Preventing the impact of selfish behavior under MANET using neighbor credit value based AODV routing algorithm. *Sādhanā, 43(4),* 60.
40. Hussain, M. A., Duraisamy, B. (2020). Preventing malicious packet drops in MANET by counter based authenticated acknowledgement. *Ingénierie des Systèmes d'Information, 25(2),* 173–181.
41. Haghighi, M. S., Aziminejad, Z. (2019). Highly anonymous mobility-tolerant location-based onion routing for VANETs. *IEEE Internet of Things Journal, 7(4),* 2582–2590.
42. Yasin, A., Abu Zant, M. (2018). Detecting and isolating black-hole attacks in MANET using timer based baited technique. *Wireless Communications and Mobile Computing, 2018,* 9812135. https://doi.org/10.1155/2018/9812135
43. El-Semary, A. M., Diab, H. (2019). BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access, 7,* 95197–95211.
44. Gurung, S., Chauhan, S. (2018). A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wireless Networks, 24,* 2957–2971.
45. Ponnusamy, M., Senthilkumar, A., Manikandan, R. (2021). Detection of selfish nodes through reputation model in mobile ad hoc network-MANET. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9),* 2404–2410.
46. Katakam, M., Adilakshmi, M. (2020). Black hole attack detection using machine learning algorithms in MANET performance comparision. *International Research Journal of Engineering and Technology, 7,* 6047–6051.

47. Sandhya Venu, V., Avula, D. (2018). Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks. *International Journal of Communication Systems, 31(6),* e3518.
48. Abdelhamid, A., Elsayed, M. S., Jurcut, A. D., Azer, M. A. (2023). A lightweight anomaly detection system for black hole attack. *Electronics, 12(6),* 1294.
49. Prasad, M., Tripathi, S., Dahal, K. (2023). An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad hoc networks. *Engineering Applications of Artificial Intelligence, 119,* 105760.
50. Reka, R., Singh, G. et al. (2023). Multi head self-attention gated graph convolutional network basedmulti-attack. *Computers & Security,* 103526.
51. Jahangeer, A., Bazai, S. U., Aslam, S., Marjan, S., Anas, M. et al. (2023). A review on the security of IoT networks: From network layer's perspective. *IEEE Access, 11,* 71073–71087.
52. Alawieh, M., Fahs, W., Haydar, J., Chbib, F., Fadlallah, A. (2022). A secure scheme for vehicle-to-vehicle (V2V) routing protocol. *2022 5th Conference on Cloud and Internet of Things (CIoT)*, Marrakech, Morocco, IEEE.
53. Remya Krishnan, P., Arun Raj Kumar, P. (2022). Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping. *Wireless Personal Communications, 124,* 1–36.
54. Tosunoglu, B. A., Koçak, C. (2022). FA-AODV: Flooding attacks detection based ad hoc on-demand distance vector routing protocol for VANET. *Sakarya University Journal of Computer and Information Sciences, 5(3),* 304–314.
55. Talukdar, M. I., Hassan, R., Hossen, M. S., Ahmad, K., Qamar, F. et al. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. *Wireless Communications and Mobile Computing, 2021,* 1–13.
56. Kolandaisamy, R., Noor, R. M., Kolandaisamy, I., Ahmedy, I., Kiah, M. L. M. et al. (2021). A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. *Journal of Ambient Intelligence and Humanized Computing, 12,* 6599–6612.
57. Younas, S., Rehman, F., Maqsood, T., Mustafa, S., Akhunzada, A. et al. (2022). Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs. *Applied Sciences, 12(23),* 12448.
58. Chui, K. T., Kochhar, T. S., Chhabra, A., Singh, S. K., Singh, D. et al. (2022). Traffic accident prevention in low visibility conditions using VANETs cloud environment. *International Journal of Cloud Applications and Computing (IJCAC), 12(1),* 1–21.
59. Network simulator tool version 2.33. https://sourceforge.net/projects/nsnam/files/allinone/ns-allinone-2.33/ns-allinone-2.33.tar.gz/download (accessed on 02/02/2023)
60. NS2 traffic generator. https://github.com/khalid-mohammadani/NS2 (accessed on 12/03/2023)
61. Ullah, S., Mohammadani, K. H., Khan, M. A., Ren, Z., Alkanhel, R. et al. (2022). Position-monitoring-based hybrid routing protocol for 3D UAV-based networks. *Drones, 6(11),* 327.
62. Mohammadani, K. H., Memon, K. A., Memon, I., Hussaini, N. N., Fazal, H. (2020). Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks. *International Journal of Distributed Sensor Networks, 16(5),* 1550147720921624.
63. Simulation of urban mobility sumo. https://sumo.dlr.de/releases/1.16.0/ (accessed on 12/03/2023)
64. Openstreetmap. https://www.openstreetmap.org/ (accessed 10/02/2023)
65. Ren, Z., Mohammadani, K. H., Riaz, W. et al. (2023). Optimal game routing for UAV ad hoc networks in smart city. *2023 6th World Conference on Computing and Communication Technologies (WCCCT).* Chengdu, China, IEEE.
66. Mohammadani, K. H., Hossen, M., Butt, R. A., Memon, K. A., Shaikh, M. M. (2022). ONU migration using network coding technique in Virtual Multi-OLT PON Architecture. *Optical Fiber Technology, 68,* 102788.

Appendix A

Algorithm 1: Pseudo-Code for a Reputation-Based Routing Protocol

```
INPUT: Set of nodes in the network N = {1,2,...,N}; initial reputation
for  each node initial_reputation; weights for trust score w1, w2,
w3; distance  metric for route selection
Output: updated routing table of Node
Initialization
For each node I in between N do
  reputation[I]:=  initial_reputation
routing_table[I]:= empty
end for
//Route Request:
RREQ (source_node, destination_node):
 if source_node has a valid route to
   destination_node then
  use the existing route
   end\ if
  else
           broadcast RREQ message to all neighbors
           set source_node as the originator of the RREQ message
           set RREQ_ID as a unique identifier
           set RREQ_HopCount:= 0
     end\ else
 end RREQ
//Route Reply:
 RREP(received_message):
  if node n receives an RREQ message with ID RREQ_ID then
  if if n has a valid route to the destination then
    send RREP message to the source node
    else
   update routing_table with the new route information
   set RREQ_HopCount:= RREQ_HopCount + 1
   broadcast RREQ message to all neighbors except the source node
    end if
    else if node n receives an RREP message then
    update routing_table with the new route information
    set message_transmission_quality:= quality of the received RREP
    message
    set message_accuracy:= accuracy of the received RREP message
    set consistency_score:= consistency of the route with
      the previous route, if any
    Use Equation (1) to set trust_score
    set the reputation score for the source node to the trust_score
    update the reputation scores for all nodes along the route
      end if
```

(Continued)

Algorithm 1 (continued)

```
end RREP
//Route Selection:
RRSE (source_node, destination_node):
    if source_node has multiple routes to the destination then
     select the route with the highest reputation score
     if multiple routes have the same highest reputation score then
     select the route with the shortest distance to the destination
         end if
    end if
end RRSE
```

Appendix B

Algorithm 2: Psudo Code of LOF Score Calculation

```
INPUT: list of data points in Routing Table; k - number of nearest
neighbors
to consider; max_hop_count - maximum
hop count allowed
Output: LOF scores for each data point in the input data
     Function euclidean_distance(x1, x2, hop_count):
         sum <- 0
         for i <- 0 to x1.size():
             sum <- sum + pow(x1[i] - x2[i], 2)
         End for
         distance <- sqrt(sum)
         return make_pair(distance, hop_count + 1)
     end Function
     //Function Local Reachability Density
      Function LRD(data, index, k, max_hop_count):
      sum <- 0
      distances <- []
      for each i, value in data:
         if i != index:
         hop_count <- 0
         distance_hopcount <- euclidean_distance(data[index], value,
         hop_count)
                  distance <- distance_hopcount.first
                  hop_count <- distance_hopcount.second
                  if hop_count <= max_hop_count:
                      distances.append(distance_hopcount)
          End if
          End if
```

(Continued)

Algorithm 2 (continued)

```
    end for
    distances.sort()
    k_distance <- distances[k-1].first
    for i <- 0 to k-1:
    sum <- sum + distances[i].first / k_distance
    end for
    return k / sum
end Function
//Function Local Outlier Factor
Function LOF(data, index, k, max_hop_count):
    sum <- 0
    lrd <- local_reachability_density(data, index, k, max_hop_count)
    lrd_ratios <- []
    for each i, value in data:
        if i is not index:
            hop_count <- 0
    distance_hopcount <-euclidean_distance(data[index], value, hop_count)
            distance <- distance_hopcount.first
  hop_count <- distance_hopcount.second
  if hop_count <= max_hop_count:
    lrd_i <- local_reachability_density(data, i, k, max_hop_count)
   lrd_ratio <- lrd_i / lrd
   lrd_ratios.append(lrd_ratio)
      end if
      end if
      end for
    lrd_ratios.sort()
    for i <- 0 to k-1:
        sum <- sum + lrd_ratios[i]
        LOF_score <- sum / k
    end for
    return LOF_score
end Function
```