Hindawi
Security and Communication Networks
Volume 2023, Article ID 4020275, 40 pages
https://doi.org/10.1155/2023/4020275

Review Article

Investigation of Different Mechanisms to Detect Misbehaving Nodes in Vehicle Ad-Hoc Networks (VANETs)

Ainaz Nobahari,[1] Danial Bakhshayeshi Avval,[2] Abbas Akhbari,[3] and Solmaz Nobahary[4]

[1]*Department of Computer, South Tehran Branch, Islamic Azad University, Tehran, Iran*
[2]*Department of Information Systems Engineering, Sakarya University, Serdivan, Sakarya, Turkey*
[3]*Department of Information Technology Engineering, Payame Nour University, Jolfa, Iran*
[4]*Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran*

Correspondence should be addressed to Solmaz Nobahary; solmaz_nobahary@yahoo.com

Received 31 October 2022; Revised 5 July 2023; Accepted 19 July 2023; Published 21 August 2023

Academic Editor: Vijayakumar Pandi

The vehicle ad-hoc network (VANET) is a crucial technology that will play a significant role in shaping the future of transition systems, which is widely used as a subset of ad-hoc networks. VANET aims to ensure driver safety by establishing independent communication with nearby vehicles. A key requirement for successful data transmission is cooperation among nodes, as factors such as high mobility, limited radio range, signal fading, and noise lead to packet loss. Security issues in vehicle ad-hoc networks have recently become a major concern. One factor that affects security is the presence of abusive nodes in the network. Like selfish nodes, they are reluctant to share their sources with their neighbors and try to keep their property. The misbehavior of malicious nodes includes dissemination of false traffic information, false location information, and redirection of packets to a wrong path, retransmission of packets, impersonation, so these nodes should be tracked down to ensure the operation of the network. This article provides a complete summary of various research works proposed to detect selfish and malicious nodes and isolate them from honest vehicles. This review article first describes the types of attacks. It then presents the methods proposed by researchers to deal with uncooperative nodes and compares their performance based on parameters such as the number of misbehaving nodes detected, overhead, throughput, layer involved in the attacks.

1. Introduction

People have been trying to drive safely and away from traffic for several years. Due to the availability of wireless networks called vehicle ad-hoc networks, this is easier today. Wireless techniques have played an important role in next-generation communication in recent years. In this network, wireless communication plays an essential role in the stability of the network [1–5]. Vehicle ad-hoc networks refer to a collection of automobiles that interact with one another through communication channels using a new type of radio frequency used for sending and receiving data between vehicles and roadside units, which is called DSRC.

The vehicle network has an unstable infrastructure and centralized management that informs each other of certain events on the road by exchanging messages between neighboring vehicles, such as an accident, a hazard on the road, a blind spot warning, or an emergency vehicle. They also exchange a variety of information for the convenience of passengers, such as information about the weather, the location of the nearest restaurants and gas stations, and even the nearest parks.

It is assumed that each vehicle is equipped with a vehicle communication system to exchange alerts in real-time via vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communication, as shown in Figure 1 [7]. To establish this communication, a number of infrastructures need to be provided. For example, OBU is used for wireless communication between two vehicles (V2V), with one unit installed in each vehicle. The following infrastructure refers to RSUs

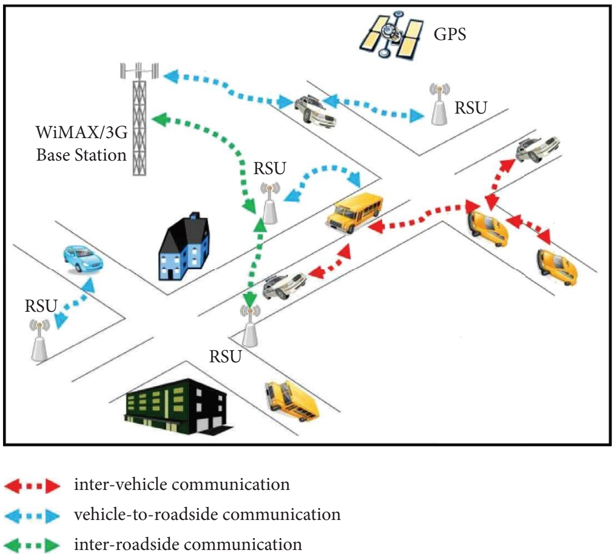
GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 1: Communications in the vehicle ad-hoc networks [6].

placed off the road to enable V2R communications. If needed, it can connect the network vehicles to the Internet. A directional antenna is used when the RSU wants to send a message to a specific location. The RSUs have the storage capacity to store the information received from the vehicle's OBU.

The following is the TPD (tamper-proof device), which, like the black box of an airplane, contains all the information about the vehicle, its route, and its speed. All traffic violations are stored in the TPD. The communication range in VANETs can be increased by multi-hop message forwarding techniques [5, 7–15]. Since message passing is done through multiple intermediaries, the listed security requirements (integrity, confidentiality, privacy, non-reputation, and authentication) are essential to protect the information in the packets from tampering by attackers or malicious vehicles [7, 15–19].

One last feature is the TA, which manages the overall VANET network and records things like OBU, RSU, and the vehicle driver ID, which are later authenticated using the registered ID for each person or device. In this way, any malicious vehicle or false message can be detected.

In this article, we will discuss various challenges associated with VANETs. Specifically, Section 2 will delve into these challenges and explore potential solutions. Section 3 discusses the categorized uncooperative nodes and their impact on network performance. Section 4 describes previous works and summarizes what has been discussed in each work. Sections 5–7 present various algorithms for detecting uncooperative nodes (selfish and malicious nodes) in vehicle ad-hoc networks. Section 8 explains the parameters discussed in Tables 1, 2, and 3. Section 9 discusses the categories of papers published in various journals. Section 10 summarizes some of the problems with VANETs that researchers can work on in the future. Section 11 contains the conclusion.

2. VANET Challenges and Security Impact

Due to some features in the structure of VANET networks that can make them require to ensure safe and confidential communications for V2V and V2R, it is essential to implement security measures.

Below are some of the VANET challenges that you might encounter. The challenges of VANET include network volatility, delay-sensitive applications, signal fading, lack of communication, limited bandwidth, and multi-hop connection [8].

(1) Network volatility: Vehicles' communications are temporary; therefore, the connection between vehicles may be established for a short time. Then, it is disconnected because of the vehicle's velocity.

(2) Delay-sensitive messages: Some messages are related to safety, passengers' comfort, and some risks on the road. These messages are time-sensitive that should forward with small overhead and low processing delays.

(3) Signal to fade: Objects that stand as obstacles between two vehicles can affect network performance. These obstacles can be other vehicles or tall buildings stationed along the way. Their effect prevents the transmitted signal from reaching the destination and increases the fading of a propagated signal.

(4) Lack of communication: High mobility and rapid changes in topology lead to multiple and consecutive outages in the network. The time required to extend the life of a connection should be as long as possible. This can happen by increasing the data transmission power, although it can reduce and degrade the operational power (average successful message delivery rate in a communication channel).

(5) Bandwidth limitations: It appears that there is only one main coordinator to control node communication and perform bandwidth management responsibilities. There is a high possibility of forming a channel density in the frequency range of 10 to 20 MHz. Therefore, the appropriate use of bandwidth significantly reduces the time delay of published messages.

(6) Multi-hop connection: Vehicle ad-hoc networks (VANETs) occasionally depend on multiple vehicle connections to transmit information, where each vehicle must disseminate the received messages to potential neighbors within its range of communication. The conduct of vehicles must be discerned, and any deviant vehicles (selfish or malicious) should be penalized or driven out of the network.

One of the significant concerns in VANET networks is the nodes that have selfish behaviors. They drop packets, so other nodes in the network will be forced to retransmit their packets because the packets are not delivered to the destination. Due to the misbehaving nodes, the traffic will

Table 1: Comparison of detection algorithms of selfish nodes.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
DSAM [20]	2023	—	—	—	—	—	Resistant to attacks like message forgery, jamming, eavesdropping, spoofing	Spending a lot of fee and time on training, limited comparison charts
System based on deep learning [21]	2021	NS-2	—	$O\ (N^2)$	—	—	Higher accuracy, and precision than KNN and ANN methods, both parameters are above 90	Decrease the prediction performance by increasing the number of nodes under simple and opinion tampering attack
DISOT [22]	2018	MATLAB	69%~85%	$O\ (N^2)$	~80%	—	Low positive alarm rate, High detection accuracy, Low end-to-end delay	High negative alarm rate, high energy consumption, communication overhead, lack of incentive to cooperate
A credit-based method [23]	2018	MATLAB	72%~82%	$O\ (N^2)$	33%~55%	—	Low end-to-end delay, energy consumption Long network life	Low detection accuracy in high rounds
Contact-based model [24]	2016	Not mentioned	—	$O\ (KN)$	—	—	Using local watchdog, Low detection time, Low FAR, FPR	Requires a buffer to store information
QoS-OLSR [25]	2014	MATLAB	68%~100%	$O\ (N^2)$	~90%	72%~ 91%	Using watchdog, Maintaining the network stability, Minimize FAR	Low probability of detection in comparison with some methods
Reputation-based model [26]	2013	Trans	—	$O\ (N^2)$	—	—	Prevent false messages spreading in the network, Effectively build trust, Using all nodes to detect selfish node, Isolating the malicious nodes	Lack of encouragement for nodes to cooperate with each other
A Dempster–Shafer based tit-for-tat strategy [27]	2013	MATLAB-VANETMobiSim	87%~93%	$O\ (N^2)$	~90%	—	Using watchdog, OBU-based (hierarchical)	Isolation black hole attack, Give second chance

increase, and bandwidth and network performance will decrease. So, the primary focus of this study is to investigate different approaches for detecting selfish and malicious nodes [19, 28–35].

(i) This study outlined and classified the various mechanisms for detecting misbehaving nodes in vehicle ad-hoc networks.

(ii) Each method's key aspects and drawbacks are explicitly written, and the algorithms of different techniques are compared with the help of three parameters: detection of the number of selfish nodes, overhead, and throughput.

(iii) The article used comparative research to recognize the critical weakness, and open issues are discussed to inspire new algorithms to detect misbehaving nodes in vehicle ad-hoc networks.

3. Introduction of Uncooperative Nodes and Security Attacks

This section presents different types of attacks that occur on vehicle ad-hoc networks. The effectiveness of an attack depends on how good the attacker is and what they can do. The potential impact of attacks on the lifesaving application of VANET cannot be predicted with certainty. Such attacks have the capability to interrupt the whole system or even manipulate the system's operations to gain ownership. The classification of attackers in VANET is determined by the nature of the attacks executed, as illustrated in Figure 2 [36, 37].

3.1. Classification Based on Activity. In this version of the classification, there are two types of attackers. One category of attackers attempts to modify the network's data by producing fake information. It is much more harmful than the second type of attacker, who reads information from the network. Passive attackers act like radio listeners. They listen to the data you send (eavesdrop) but do not change them.

3.2. Classification Based on Membership. Two distinct categories of attackers exist, reliable nodes and external nodes. The former type is utilized to disseminate information amongst other members within the network and is referred to as internal. Despite their official status, these members can employ diverse tactics to impact the network negatively. Conversely, external nodes lack the privilege of direct communication with any nodes present within the network, thereby limiting their capability to attack other nodes.

3.3. Classification Based on Intension. There are two general categories for uncooperative nodes: selfish and malicious nodes. In vehicle ad-hoc networks, the cooperation between nodes has an essential effect on the network's stability. However, a node with selfish motives or malicious motives may want to get an advantage over the other nodes.

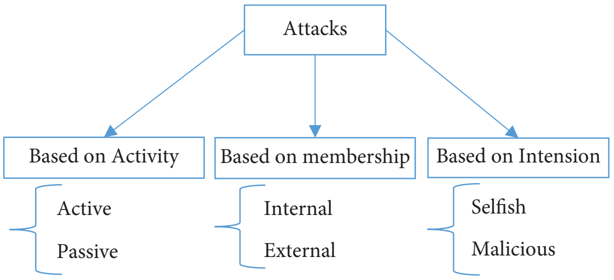

Figure 2: Classification of types of attacks.

3.3.1. Selfish Nodes. The nodes' selfish motives are limited bandwidth and low resources such as battery, memory, and CPU. A selfish node may drop packets of neighboring nodes, wasting time for retransition, creating congestion in the network, and disrupting the network.

3.3.2. Malicious Nodes. A malicious node can transmit false warnings, tamper messages, and create congestion in the network by modifying, dropping, replying to earlier transmission, or misrouting data packets. These malicious behaviors cause problems such as vehicle crashes, increased congestion, and issues that mostly intend to destroy the network.

There were numerous possible attacks on VANET and the potential for a complete network shutdown and performance degradation is a distinct possibility.

Some attacks for which a solution has been provided in the studied articles are explained below.

Another classification proposed by the researchers in reference [38] for the types of attacks is shown in Figure 3, where the attacks are classified according to the security services challenged by the attacks.

3.3.3. Attacks on Availability. Information availability is critical to users, as a lack of information results in it not reaching users and degrading the network's performance. Attacks such as denial of service, jamming, and blackhole attacks fall into this category.

3.3.4. Attacks on Data Confidentiality. Confidentiality guarantees that access to the information is restricted to authorized users only. Confidentiality is of utmost importance due to the absence of confidentiality that could leak vital information to the public. Attacks such as eavesdropping and man-in-the-middle fall into this category.

3.3.5. Attacks on Data Integrity. Data integrity means that the contents of packets do not change during the transmission of the packet from one node to another in the network. Data integrity for data packets guarantees the reliability and accuracy of the data. Attacks such as illusion and masquerading belong to this category.

3.3.6. Attacks on Authentication. Authentication is the first way of protection from attackers. It is a mechanism to protect the network from the abusive behavior of vehicles

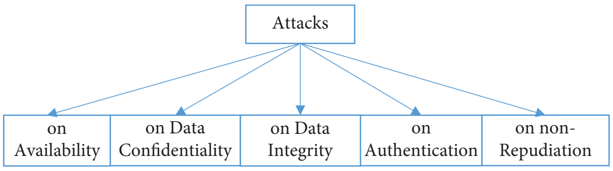

Figure 3: Another classification of types of attacks.

entering with bad intentions. The action of authentication in VANETs serves the purpose of safeguarding legitimate nodes from both internal and external malicious entities. The classification of Sybil and Global Positioning System (GPS) spoofing attacks and replay attacks can be attributed to this category.

3.3.7. Attacks on Non-Repudiation. Non-repudiation is a concept that denotes the inability of the message sender to refute having sent the message or for the message receiver to deny the receipt of the packet. An attack that utilizes this approach involves the attacker denying having both sent and received the message.

(1) Denial of Service (DOS) Attack. The availability of the network is of utmost importance in the case of VANET, as all automobiles are dependent on it.

The DOS attack is often one of the most severe attacks on any network. The primary purpose of the VANET is to provide honest users from accessing the network. This purpose is not accomplished when a DOS attack occurs on the network because malicious vehicles send many bogus messages on the control channel to gain attention, get extra benefit from the network, or disrupt network performance. It is a problem that the DOS attack uses up a lot of memory, bandwidth, and provided memory. In this situation, an assailant transmits a notice regarding mishaps to the automobiles within its wireless radius and simultaneously to the roadside unit (RSU). In this circumstance, the RSU and the vehicles are preoccupied with receiving messages from a malevolent vehicle. However, even with this attack, the vehicle nodes present in the network cannot execute all the crucial undertakings, and the transfer of information among all the nodes is impeded.

The architecture of the attack is shown on the right side of Figure 4 [39, 40]. On the right side of Figure 4, the black vehicle carries out the DOS attack because it repeatedly sends the false message "accident occurred ahead" to the neighboring vehicles and RSU.

(2) Distributed Denial of Service (DDOS) Attack. The DDOS attack poses a more significant threat than its denial of service (DOS) counterpart in the VANET circumstance. This is primarily due to the attack's distributed mechanism within the environment. In a DDOS attack, multiple malicious vehicles execute an attack on an honest vehicle from various locations. The attackers send large number of packet and cause network traffic all the time. So, it is hard to find out from which vehicle this attack came. This attack is much faster than the DOS attack. The left side of Figure 4 shows a DDOS attack in which malicious vehicles perform a DDOS attack from varying locations and at distinct temporal intervals in a manner considered lawful, so the attacked vehicle cannot communicate with trusted vehicles in its radio frequency range [41]. As you can see, the black vehicles act as malicious vehicles, and they all repeatedly send the wrong message, "accident occurred ahead," to the nearby vehicles.

(3) Illusion Attack. In this particular attack, the perpetrator deliberately alters the traffic data of their vehicle and transmits erroneous information to neighboring vehicles and RSUs. Within VANET, drivers' conduct depends upon the warning messages they receive; receiving such messages may result in a shift in the driver's response and consequentially lead to an accident, traffic congestion, or a detours route to the destination. Furthermore, the adjustment of the network topology may lead to a decline in network performance [42]. Next, how to perform the Illusion attack is shown in Figure 5. In this attack, the black vehicle, which is the cause of the attack, can confuse the drivers in choosing the route with various fake messages such as "There has been an accident ahead or drive slowly, the road is slippery, or the weather ahead is foggy."

(4) Replay Attack. This attack occurs when a malicious vehicle replays the transmission of previous information to benefit the message's situation at sending. The attacker replays the earlier message repeatedly to confuse other nodes because the previous message is not correct now. For example, sending an accident message that happened several minutes before is considered the wrong message for the vehicles ahead. The timestamp can prevent replay attacks. In Figure 6, the yellow vehicle, which received a packet about the collision of two black and green vehicles earlier at time T1, sends it to the other vehicle after traveling a distance again at time T2 [43].

(5) Black Hole Attack. The black hole attack in vehicle ad-hoc networks (VANET) is considered one of the subclasses of denial-of-service attacks. If a vehicle on the road tries to get packets of a vehicle, it will tell other vehicles on the road that it is the fastest way to get to that vehicle. This is called a black hole attack. Furthermore, after receiving the packets, it throws them away in this attack, the number of malicious nodes can be more than one, and sometimes they gather in a place close to each other, called a black box. In Figure 7, the black car presents itself as the closest node to the destination, and instead of taking the correct path indicated by the arrows in Figure 7, the packets are all sent to the black vehicle [44].

(6) Wormhole Attack. In vehicle ad-hoc networks, malicious nodes (nodes that do not follow the rules) can listen to the packets that are not supposed to be heard by others. Little by little, they replace themselves with honest vehicles to receive information and then broadcast the packets to their colleagues to the other end of the tunnel. A wormhole attack is a way to disrupt the routing of a network by sending a packet to an unexpected destination. Figure 8 shows how the

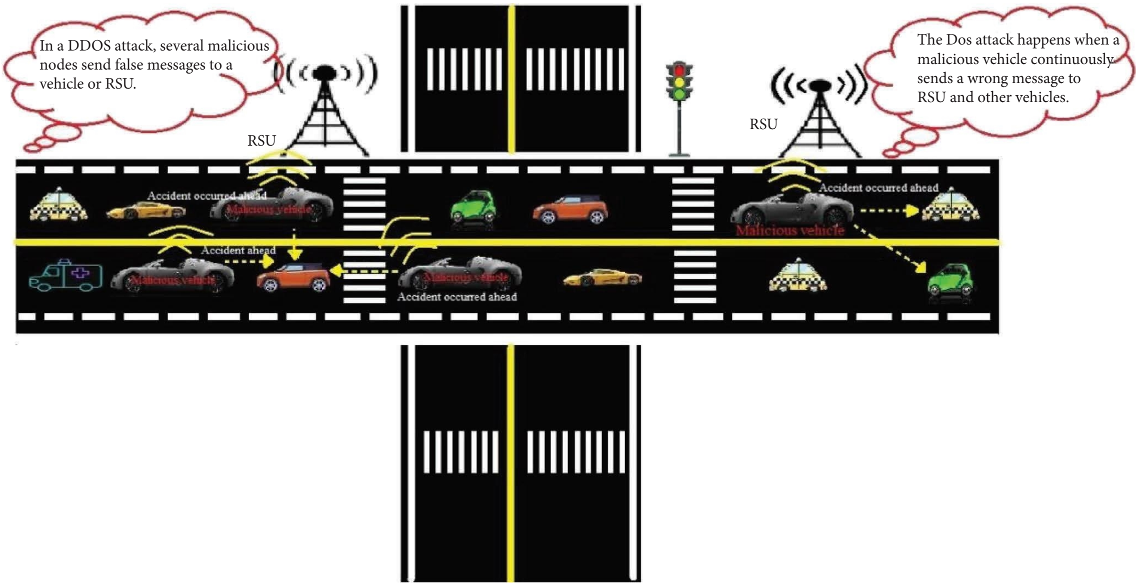
In a DDOS attack, several malicious nodes send false messages to a vehicle or RSU.
RSU
RSU
The Dos attack happens when a malicious vehicle continuously sends a wrong message to RSU and other vehicles.
Accident occurred ahead
Malicious vehicle
Accident occurred ahead
Malicious vehicle
Accident ahead
Malicious vehicle
Malicious vehicle
Accident occurred ahead

Figure 4: A small view of DOS and DDOS attacks.

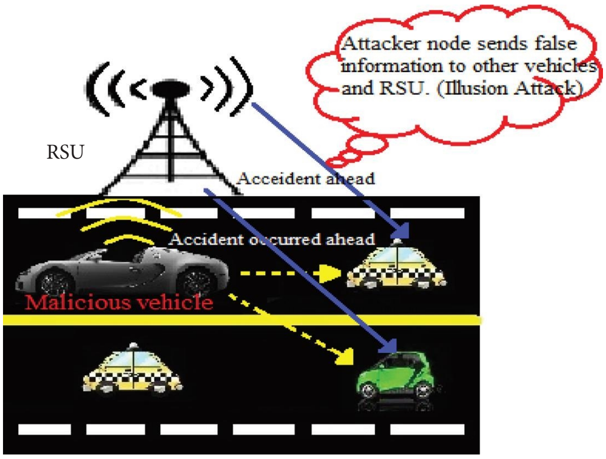
Attacker node sends false information to other vehicles and RSU. (Illusion Attack)
RSU
Accident ahead
Accident occurred ahead
Malicious vehicle

Figure 5: A small view of the illusion attack.

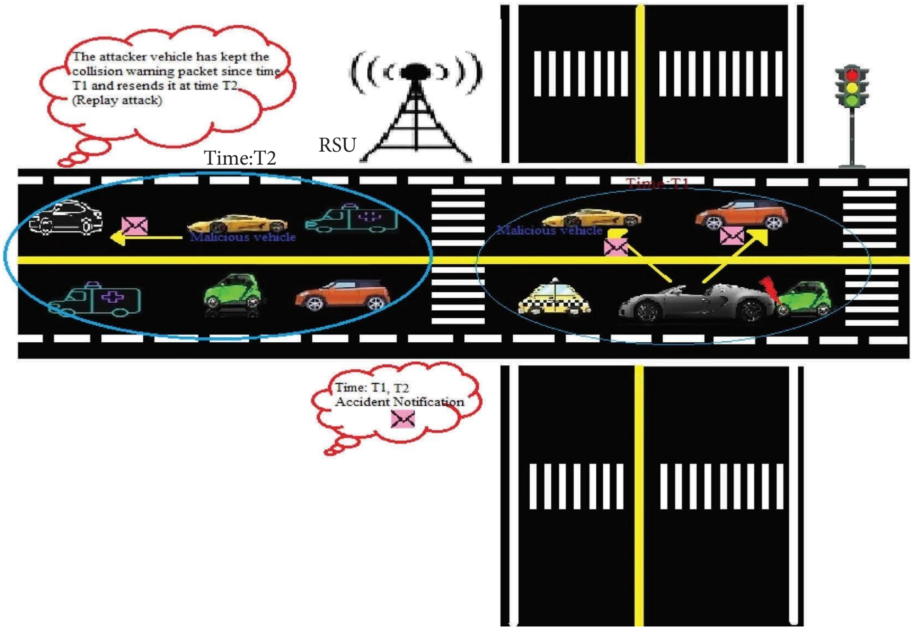
The attacker vehicle has kept the collision warning packet since time T1 and resends it at time T2. (Replay attack)
RSU
Time:T2
Time:T1
Malicious vehicle
Malicious vehicle
Time: T1, T2 Accident Notification

Figure 6: A small view of the replay attack.

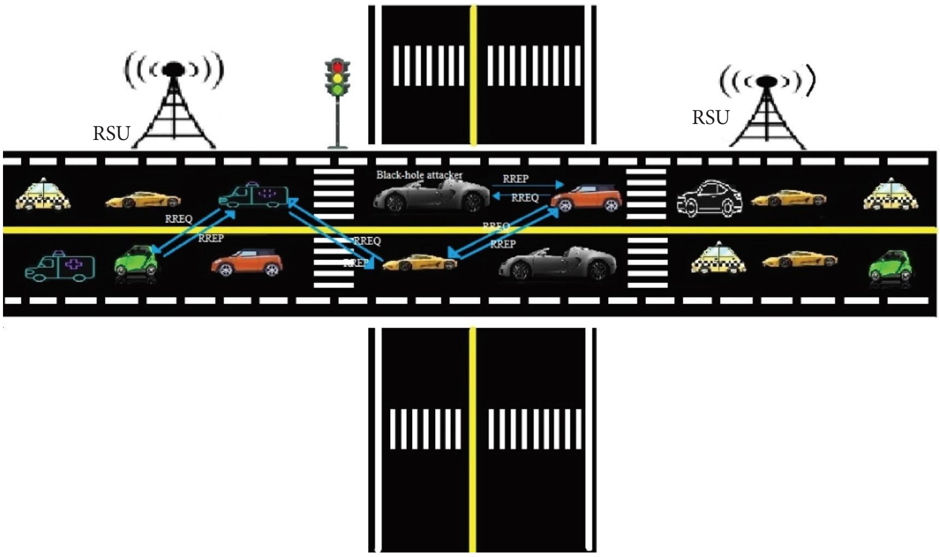

Figure 7: A small view of the black hole attack.

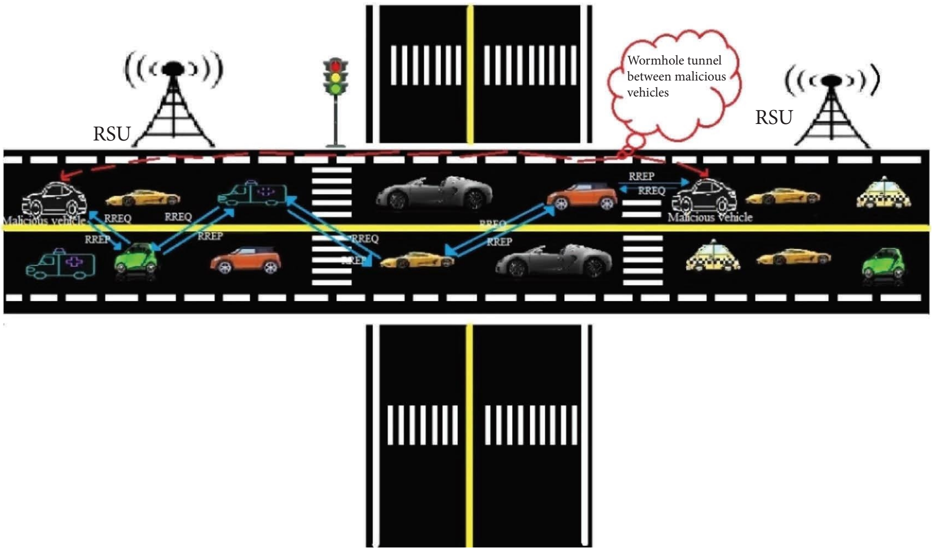

Figure 8: A small view of the wormhole attack.

attacker nodes work in this attack. The malicious vehicle receives the information and sends it through the tunnel to its malicious colleague on the other side. Wormhole attacks can be categorized into three main categories: open wormhole, half-open wormhole, and closed wormhole. The difference between these three divisions lies in how the packet reaches the malicious wormhole nodes [45].

3.3.8. Open Wormhole. The source, destination, and neighbor nodes in their one-hop are visible, but other malicious nodes in the path are kept hidden. The source and destination nodes do not know they have malicious nodes in their neighborhood. In this case, the malicious nodes put themselves in the header of the route request packets.

3.3.9. Half-Open Wormhole. A malicious node near the origin is visible, but the malicious node near the destination remains hidden. So, to send the packet to the destination, it is sent to the center, and the malicious node is near the origin node; then, it is sent to the destination, and the malicious node sends the packet through the tunnel to the attacking node on the other side. In this case, the content of the packets is not changed.

3.3.10. Closed Wormhole. In this classification, the identity of all malicious nodes remains hidden between the source and the destination so that the source and destination nodes feel that they are in a one-level relationship and exchange packets directly with each other.

(1) Gray Hole Attack. The attack, referred to as the gray hole, significantly impacts various parameters of VANET, including but not limited to packet delivery, throughput, and end-to-end delay. The gray hole attack is a similar type to the black hole attack in which the malicious node behaves like black hole nodes. They forward the packets, but sometimes, it drops them for a while and then changes to its usual behavior [46].

(2) Jellyfish Attack (JF). In this form of attack, the offender's vehicle causes disruptions to the network. If the intruder manages to breach the network, the packet replication and discarding process can potentially cause delays in the network, while also rearranging the sequence of the packets. JF attacks executed at the network layer negatively impact the transport layer's functionality, leading to a decrease in the network's end-to-end delay levels [47].

(3) Jamming Attack. One of the most significant attacks in the field of security applications for VANETs occurs when an untrustworthy vehicle endeavors to impede broadcasting communication using various techniques, including the transmission of a potent signal that possesses a frequency range comparable to that of the receiver or sending packets with a legal header but worthless payload. This attack is not energy efficient for the attacker because of that; the attacker uses as much noise as possible in the packet to change bits; in this case, little energy is consumed. If the receiver obtains a packet with an incorrect checksum, the receiver will discard it and will not accept any more packets with the same checksum as the discarded packet [48].

(4) Timing Attack. Most packets should be sent in real-time in VANET, but some attacker vehicles do not forward the safety-critical data to other vehicles at the right time. They add some extra packet delays regarding time slots. This attack is called the timing attack; a few malicious vehicles participate in this attack with destructive thoughts, such as creating traffic and causing consecutive accidents [49].

(5) Eavesdropping Attack. Eavesdropping is a passive attack. The attacker eavesdrops on the transmission channel to access security certifications or secret information. Hence, a vehicle that is not registered employs a legitimate certification to amass pertinent data about the vehicle, including the vehicle's identification, location, velocity, and other relevant details [50].

(6) Sybil Attack. In a Sybil attack, an attacker creates many forged identities (multiple false vehicles) to conquer the whole network and broadcast false information to hurt honest users or ruin the network's performance. According to the performance of this type of attack, it can be introduced as one of the most destructive attacks in the network. The attacker falsely asserted to be present at another geographic site at the same time, so they forced vehicles to change their direction to other roads to make that road clean [51].

(7) GPS Spoofing Attack. All vehicles within the VANET system transmit information to the GPS system. The satellites ensure the location of vehicles within the network by keeping track of their distinct identities and locations. During a GPS spoofing offense, the attacker vehicle generates a misleading output generated by the GPS system to think they are located in a different location. This is accomplished through the use of a GPS satellite simulator, which generates much stronger wrong signals than the actual one [52].

(8) Sensor Tampering. It is easy for attackers to fool a device's sensors by making them think that something is true when it is not, which is called sensor tampering. In this example, an attacker could use ice to trick the sensors that tell cars how cold it is outside and the road is covered in ice, then send messages that indicate the road is icy when it actually is not. Same way, tampering with the GPS's sensors can even possibly send false position information. Therefore, it is possible to send false data to the network, even though the data are accurate and the integrity is preserved in appearance [53].

(9) Man-In-The Middle Attack (MITM). An attacker joins the network, includes himself in the communication between two vehicles, and receives packets exchanged between the source and destination to achieve access to the packets, both source, and destination, were attempted to transmit. The messages are changed before being delivered to the destination. But both sender and receiver think this connection is secure [54].

(10) Masquerading Attack. The attacker gains entry into the VANET infrastructure through valid user identification and passwords, although under unauthorized auspices to disseminate incorrect messages that seem to originate from the officially registered vehicle [55].

4. Related Surveys

This section reviews previous related works, discovering the selfish and malicious nodes presented in VANET. Each paper provides a different category for the behavior of different nodes.

In [56], first, the description of vehicle ad-hoc networks is provided, which includes the network overview, features (high mobility, dynamic network topology, frequent network disconnection, transmission media, no power limitation, transmission power limitation, weakening of wireless transmission, and extensive computing processing), security services (availability, confidentiality, authentication, data integrity, and non-repudiation) and threats, attacks in these networks, which are categorized in three general groups (attack on communications, attack on security applications, attack on entertainment information applications). Location privacy techniques have been extensively investigated to safeguard sensitive vehicle data, including vehicle location and driver information. Subsequently, an in-depth explanation is provided regarding the various trust management models utilized in VANETs and trust management simulation tools are introduced for evaluating the efficiency of the trust models in VANETs, such as MATLAB, NS-2, NS-3, TRMSIM-V2V, TraNS, VANETMobiSim, and Veins. Discussions including the development of the VANET to VCC (vehicle cloud computing), the reason for becoming the VCC (providing various services at low cost, including reducing traffic and traffic accidents, improving the traffic environment and road safety), VCC architecture, and security and privacy issues are provided. This article discusses how architectural design and security issues can affect privacy. It also discusses research challenges related to the VANET and VCC projects. This study presents a detailed review of related research conducted to detect and reverse node misbehavior in VANETs to establish a secure network. In a comprehensive article that includes a complete description of all the elements of security and attacks, the authors can examine more techniques about the trust model and its impact on security and privacy are significant concerns that can prevent various attacks and methods which provide security in the network.

This study [57] reviews related research to detect node misbehavior in VANETs and revoke malicious node certifications to establish a secure network. Then, after dividing the nodes into two categories, static and dynamic, they examine the different methods presented in the articles in this field and place each technique in the subcategories in this category. Once malicious nodes are detected, certificate revocation is a method of removing malicious vehicles from the network, and the information about vehicles revoked by the CA is disseminated through the revocation process so that other neighbor vehicles do not consider the received message. As a result, the private information of misbehavior vehicles is blocked. The presented article has studied each method's features, advantages, and disadvantages well. Still, it was better to use numerical parameters to compare each technique with another one.

The review paper [58] first introduced intelligent transportation systems and then examined security shortcomings based on the PKI method. Then, a categorization of distinct detection mechanisms for inappropriate behavior has been presented, which is explicitly designed for vehicular ad-hoc networks. This categorization encompasses both data-centric and node-centric mechanisms (comprising mechanisms centered around data and nodes) that identify malicious messages according to the characteristics of the sender node, and the mechanisms that are data-centric in nature predominantly engage in the analysis of the significance of messages that are received.

They are divided into two categories, consistency and plausibility mechanisms. In the first category, only the packets of a specific sender are analyzed. Still, in plausibility mechanisms, the messages received from several different senders are analyzed, and all messages must be matched. This study summarizes each article and the pros and cons of each method are studied in full detail. Techniques have been analyzed in terms of parameters such as qualitative analysis of diagnostic range, required resources, generalizability, security, and privacy.

Arshad et al. [59] conducted a study on how to detect fake messages in VANETs. The classification of false message detection schemes is based on the two main categories of node-centric and data-centric detection, which is categorized by node behavior, trust, local and cooperative. The paper discusses the limitations of the papers published so far and what the future holds for them. Suitable parameters have been used to compare the studied approaches, which show what features each method provides in the presented article. Still, it was better to determine how much more or less the authors mean in some cases.

In [60], Lu et al. have described the characteristics of vehicle ad-hoc networks and then the system model, which includes the three main components OBU, RSU, and TA. Then, the security and operational criteria they will try to eliminate in these cases are explained in detail. In addition to presenting the protection mechanisms against various attacks in VANET, the critical features of effective trust management models are stated. Several location privacy protection mechanisms are also described to protect vehicle privacy further and ensure the quality of location-based services. Finally, the types of simulators used in VANET are described. The authors should compare different methods according to several parameters in a comparison table.

This study [53] examines the security challenges in VANET, such as privacy, scalability, mobility, long delay constraints, and cooperation. The points mentioned in the article include the introduction of attacks (such as Sybil, denial-of-service (DoS), blackhole, and wormhole attacks), how the attacks work (such as sending false location information, tampering with sensors, replaying data packets, and eavesdropping on packets and publishing this information on the network), and an explanation of the impact of these attacks on the network. The following section examines the security solutions provided in previous articles for each attack and the advantages and disadvantages of each solution. Then, in an evaluation table, items such as the infrastructure used in the proposed method, how each method works, how to respond to the attacks, and which attacks the proposed methods cover are presented. The authors of this study have written a table that lists all the different characteristics used in the study. Still, it would be better to provide a comparison table according to the essential parameters in the network.

This study [61] first introduces the vehicle ad-hoc networks, and then the network characteristics have been provided (including network topology and communication model). In the following, network challenges such as the size of these networks, uncertainty about the non-manipulation of messages, various algorithms for sending packets, and security restrictions such as congestion and collision control, sender anonymity, and privacy are examined, and their causes and available solutions are provided for them. Then, security requirements such as authentication, availability, confidentiality, non-repudiation, honesty, privacy and anonymity, data verification, flexibility and performance, and error detection are examined. The authors then focus on classifying the various known attacks and suggested solutions. The proposed solutions enable VANET to implement a secure system for trusting vehicles and protecting them from selfish and malicious nodes. One of the positive points of this article is the study of the features of each proposed method in different tables and the detection rate of attacks.

In [62], the authors address issues such as the types of communication, the reason for existing communication between vehicles and security requirements, reviewing different types of attacks, familiarity with different types of attackers, the impact of different kinds of attacks on vehicle ad-hoc networks and geographical location information and various threats. Networks have clearly and comprehensively discussed the threats to spatial details here. The article should have included more methods worked in this field and used a comparison table to compare the proposed techniques.

The paper [38] first gives an introduction to the VANET network. The components and characteristics of the VANET network are described. Then, a classification for the types of attacks is presented based on the security services in VANET, showing which attack threatens each security service. After defining the known attacks that challenge each security service, some of the most effective approaches to improve the services are given. At the end of the article, there are comparison tables that can show the efficiency of each method by calculating the energy consumption, throughput, overhead, etc.

The paper [63] presents several research areas for building reliable and secure vehicle ad-hoc networks. A detailed review of the research has been done to identify malicious nodes and nodes' misbehavior in vehicle ad-hoc networks. The type of misbehavior is examined first and then the techniques used to distinguish the misbehavior. This study divides the proposed methods into two general categories: node-based and data-centric. The usefulness and weaknesses of these two sorts of methods are explained to make them work better. A combination of node-based and data-centric designs has been proposed, which can identify more complex attacks with the advantages of both approaches. In this study, it would be better to compare all the studied techniques based on the parameters written in Table 1, and there will be a complete table of features of all methods.

In [64], first, an overview of vehicle ad-hoc networks is performed. The security features and requirements, challenges, and types of attacks in VANETs have also been discussed, and a classification is presented of the kinds of attacks that classify security threats in VANET according to the different layers in the five layers of the stack model (application, transmission, network, data link, and physical). This article uses figures to show attacks understandable to the readers. I also recommend using comparison tables for techniques to prevent attacks from improving the quality of the paper.

In [65], the aim of classifying the current techniques is to be aware of intrusion detection in vehicle ad-hoc networks. The intrusion detection systems are architecturally divided into three categories (independent, partner and distributed, and hierarchical); different intrusion detection methods are divided into several different types, such as the system based on watchdog node monitoring, reputation-based system, area-based system, signature-based system, etc. A one-dimensional short review paper describes an intrusion detection (IDS) attack and examines various techniques to identify this attack.

In [6], the authors first discuss the unique features and applications of VANETs. The following contexts are about the challenges in these networks, such as frequent changes in the environment, increasing channel load, irregular connection due to changes in the strength of the received signal, and loss of packets. Then, the authors discuss the types of attackers, known attacks so far, and critical cryptographic requirements to solve security issues such as accessibility and integrity. Also, the last topic discussed is the trust management models available in these networks, the unique challenges in modeling trust management, and the methods presented in previous articles to solve these challenges. A short review paper explores ways to deal with some of the attacks, which can be further improved by reviewing recent papers.

In the following, we discuss different methods for detecting selfish and malicious nodes, or both, since there can be several different selfish and malicious behaviors in the network and each method can only solve some cases. In the description of each method, we have highlighted the type of selfishness or malice emanating from the node so that it is clear what type of selfishness or malice each method can detect or what exactly the proposed method does to solve the problem.

5. Detection Schemes of Selfish Nodes

This part of the paper reviews various papers that provide an algorithm for detecting selfish nodes. In the following, Table 1 discusses the advantages and disadvantages of these algorithms and Table 4 examines the features of each paper.

5.1. DSAM (Deep Q-Network to Suppress the Attack Motivation of Selfish OBU).

In this study, the authors utilized a DDQN-based algorithm to establish an indirect mutual security frame for the computation and maintenance of the reputation of each OBU in the VANET. The algorithm effectively represses the motivation of selfish OBU attacks. Additionally, blockchain technology was implemented to safeguard against malicious tampering with the reputation model. Consequently, every node possesses a copy of the blockchain in the network of distributed devices, containing blocks that comprehensively document the past manner of individual nodes. These blocks cannot be falsified or modified with retrospective effect due to a uniformity mechanism and specialized encryption. To compact the learning state space and guess each communication behavior's Q value, the proposed algorithm includes a complex CNN (convolutional neural network) [20].

5.2. System Based on Deep Learning.

Jyothi and Patil [21] proposed a model that uses deep learning to detect **selfish vehicles** by their trust values. In this method, a deep belief

Table 2: Comparison of detection algorithms of malicious nodes.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
Rashid et al.'s model [66]	2023	OMNET++ and SUMO	~90%	$O(N^n)$	99%	—	High accuracy, recall, precision	The complexity of the algorithm and the need for high memory to perform calculations
Bayesian-based model [67]	2023	—	—	$O(N^2)$	—	—	Reducing the attacks of malicious nodes by applying the proposed method	The complexity of the algorithm and the need for high memory capacity
MDFD [68]	2023	ONMET++, veins, and SUMO	80%~100%	$O(N^2)$	—	—	High accuracy, recall, precision	High data processing time
Awan et al.'s model [69]	2022	Veins	—	$O(N^2)$	~50%	—	Low energy consumption	The proposed method does not provide the necessary efficiency in all conditions
Fog-based DDoS detection method [70]	2022	ONMET++, veins, and SUMO	90%	$O(N^2)$	100%	100%	High precision and true negative rate above 90%	The results are a bit doubtful. Lack of comparison chart with other recently proposed methods
Signature-based authentication [71]	2022	CYGWIN	—	—	—	—	Low computational time O (N), communication cost	High memory and computation overhead
F-RouND [72]	2022	OMNET++ and SUMO	98%~100%	12%~16%	65%~85%	60%~84%	Low FPR and end-to-end delay	As the number of rogue nodes increases, network efficiency decreases
BCSM [73]	2022	One and SUMO	~80%	Light traffic: 25%~40% heavy traffic: 86%~65%	~80%	Light traffic: 86%~93% heavy traffic: 79%~95%	Low FAR value in heavy and light city traffic	Decreasing efficiency with the presence of malicious vehicles above 45% in the network
EPORP-based security protocol [74]	2022	NS-2	25%~85%	$O(N^n)$	~86%	~80%	In the proposed method, the encryption and decryption time is 280 ms that is lower than the WOA method	High memory consumption for encryption and decryption
SAODV [75]	2022	NS-3	>98%	$O(N^n)$	>87%	>95%	High detection rate	High end-to-end delay with increasing nodes, high memory usage and complicated computation

Table 2: Continued.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
FBTRP-DBN [76]	2022	MATLAB-NS-2	>98%	$O(N^2)$	~98%	Gradual increase until reaching 100%	Low end-to-end delay, high packet delivery rate, throughput	Absence of flowchart and semi-code of the proposed method
TREE [77]	2022	NS-2 and vanet MobiSim	Up to 99%	$O((m * n) + (r * n))$	>90%	Up to 80%	Low end-to-end delay, high packet delivery rate	Increasing the percentage of lost packets with the increase in the number of vehicles
BBAAS [78]	2021	—	—	$O\ (N + 1)$	—	—	Providing a high level of confidentiality during message transmission, useful for real-time applications	It does not have high reliability in error-free operation
Fog-assisted networks based on blockchain and neuro-fuzzy [79]	2021	NS-3 and SUMO	>90%	$O(N^3)$	>90%	92%–98%	Accuracy of neuro-fuzzy up to 91.5%, it can validate a large number of messages with and without batch presence	Complexity of calculations
Sharma and Jaekel's model [80]	2021	Not mentioned the simulator but the dataset is VeReMi (vehicular reference misbehavior dataset)	95%~100%	$O\ (N)$	>90%	>96%	High precision, recall	Not providing any comparison chart between the proposed method and other methods
Improved secure AODV [81]	2021	NS-2.33	—	$O(N^n)$	77.79	75.28	Low end-to end delay	High memory usage and complicated computation, low throughput in case of increasing malicious nodes
CBM scheme [82]	2021	Not mentioned	72%~91%	$O\ (N^2)$	97%	>90%	High TPR, prevent sybil and DoS attacks	Insufficient sample data set
ECT [83]	2021	NS-2	>70%	$O\ (KN)$	>70%	77%~85%	The proposed method has relatively acceptable results	Absence of flowchart and semi-code of the proposed method, limitation of comparison charts
RBA [84]	2020	NS-2	>70%	Routing overhead (up to 92%)	—	70%~92%	PDR relatively suitable	Routing overhead increases with increasing number of nodes, average end-to-end delay
QMM-VANET [85]	2020	NS-2	80%~91%	$O\ (N)$	90%	88%~91%	Low end-to-end delays, high packet delivery rate, maintain network stability, connectivity	Lack of encouragement to cooperate, The idea only applies to highways scenario

Table 2: Continued.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
TBM [86]	2019	NS-2	55%~62%	$O\ (KN)$	~94%	—	Low control overhead, Load distribution, successful packet delivery fraction, monitoring nodes	Low accuracy of detection
Blockchain-based model [87]	2018	MATLAB	52%~75%	$O\ (N)$	~70%	~80%	Establish a safe and efficient intelligent transportation network	Not given second chance, High delay
An AODV-based model [88]	2018	NS-2	55%~78%	$O\ (N^2)$	~67%	~74%	Low end-to-end delay, high packet delivery rate	Not provide security, privacy
EAAP [89]	2017	Cygwin	—	—	—	—	The shortest message verification time compared to other methods	As the number of messages increases, this method won't work
A game theory-based trust model [90]	2017	NS-2	82%~95%	$O\ (N^n)$	>90%	~94%	Perform a scenario in two different environments with different numbers of nodes Reduce retransmission attempts and data drop rate	Different detection accuracy in different scenarios, Do not provide security
On-demand model [91]	2016	SUMO	81%~93%	$O\ (N^2)$	>90%	85%~95%	High efficiency High effectiveness in detecting Able to recover the effect of misbehaving nodes	High delay, Lack of high throughput at very high or very low speeds
A model to detect black hole attack [92]	2016	NCTUNs	74%~85%	$O\ (N)$	~83%	—	Using different scenarios, Avoid attacks like black holes, Reduce dropped packets	Provide security,privacy High delay
FMBA [93]	2016	NS-2	—	$O\ (KN)$	—	—	Detect cheater vehicles Minimum delay of the alert message	High delay Energy consumption
Watchdog- and Bayesian- based model [94]	2016	Not mentioned	76%~91%	$O\ (KN)$	>85%	—	Using watch dogs as observers, provide security, low FPR	Not given second chance Do not provide privacy
A distributed reputation-based scheme [95]	2016	Not mentioned	—	$O\ (KN)$	—	—	Provide scalability, 90% accuracy in detecting	Weakness in the face of other attacks, Do not provide security

Table 2: Continued.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
VGKM [96]	2015	JAVA	—	$O\ (KN)$	—	—	The key computation time is O (1) even with a key size of 512 bits, low storage complexity	Increasing key recovery time by increasing key size
DMN [97]	2015	Network simulator −2	42%~58%	$O\ (N)$	~47%	25%~38%	Clustered Provide privacy Low FAR (false alarm rate) Role of vehicles Monitor each node’s function	Not given second chance, Do not provide privacy, Low throughput with increasing number of malicious nodes
T-ACO [98]	2015	SUMO and NS-2.34	52%~75%	$O\ (N^2)$	>70%	64%~70%	High packet delivery rate, Average end-to-end delay, Normal routing overhead, Average energy consumption	High delay, Not given second chance
FHR [99]	2014	Not mentioned	—	$O\ (KN)$	—	—	Low approximation error Measuring the truth of PCN alert provide (privacy)	Mechanism uses for static events, High delay
DMV [100]	2013	Not mentioned	25%~41%	O (KN)	~35%	28%~35%	High detection of malicious nodes in high velocities, Using observer nodes	Cannot respond to other network attacks
D&PMV [101]	2013	Not mentioned	52%~71%	$O\ (N^2)$	~60%	~63%	Detect malicious nodes before affecting the network Avoid attacks like black holes	Do not provide privacy, Reliable channel
RAODV [102]	2012	NS-2	25%~%	$O\ (N^2)$	>25%	~21%	Develop AODV protocol, Low routing overhead, Provide privacy	High percentage of dropped nodes in the presence of malicious nodes
MDS [103]	2012	NS-2	—	$O\ (N^2)$	—	—	Encourage nodes to collaborate, Low packet drops	Encourage nodes to collaborate, Low packet drops
System based on detecting cheater [104]	2012	NS-2	—	$O\ (1)$	—	—	Detect fake congestion, without overhead for nodes, provide privacy, low delay	Low detection accuracy in the presence of a large number of malicious nodes

Table 2: Continued.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
MBRMS [105]	2012	MATLAB	25%~87%	$O\ (KN)$	>70%	>52%	Provide (scalability, decentralization, confidence), low FAR	Do not provide security
RB-CD [106]	2011	NS-2	80%~96%	$O\ (N)$	82%~95%	>90%	Broadcasting alerts High detection of malicious nodes	Do not reliable channel
VARM [107]	2011	Not mentioned	70%~82%	$O\ (N^2)$	>70%	>76%	Provide consistency Low FPR Low delay	Using complex algorithms Computation overhead for single node Not providing privacy
Data centric detection schemes (DC) [108]	2011	Not mentioned	—	$O\ (KN)$	—	—	Reliable model (due to the use of authentication) High performance against sybil attacks, Low FAR, delay	Not always provide useful information for detection
System based on machine learning [109]	2011	NCTUns-5.0	92%~93%	$O\ (N^2)$	~90%	>90%	Provide privacy Categorizing different misbehaviors Using efficient algorithm to detect malicious nodes	Do not provide privacy, High delay
Intrusion detection model [110]	2010	VanetMobiSim	≥83%	$O\ (N)$	>80%	75%~85%	Able to detect road side attackers Detect fake traffic congestions	Energy consumption, High delay
A system-based alert [111]	2010	Vanet MobiSim	92%~98%	$O\ (N)$	>90%	>92%	Able to detect false alerts, Low FAR	Produced secondary information by malicious nodes, Not provide security, privacy
Root cause-based detection (RCBD) [112]	2010	VanetMobiSim	92%~98%	$O(N^2)$	~98%	>95%	Not sensitive to small errors, High detection model	High delay, Do not provide privacy
Ghosh et al.'s method [113]	2009	Qualnet	92%~98%	$O(N^n)$	~95%	>90%	Detect at high speeds, Low FPR, low delay	Do not provide privacy
VARS [114]	2005	Not mentioned	—	$O\ (N)$	—	—	Provide (scalability, distributed, safety, message analysis, confidence)	Not provide security, privacy

network (DBN) and Red Fox Optimization (RFO) algorithm is used to evaluate the warning message sender and the integrity of the received message on the receiver side. To ensure the accuracy of these two items, the location of the vehicles is used to step by step get closer to the trust of each vehicle. With the help of time and distance, it can be determined whether the location stated by the vehicle is actual or not. To confirm location through distance, both beacons and event messages comprise geographic coordinates. The supervised machine learning approach is implemented by employing SVM. The Support Vector Machine's classification and majority voting processes are dependent on similarity measures that utilize distance. The integrity of the trust level of the messages is assessed contingent upon the event message of adjacent vehicles. Based on the threshold value, both dependable and undependable vehicles are identified. The probability value of a reliable vehicle is one, and that of an undependable vehicle is zero. The proposed method is compared with KNN and ANN (Artificial Neural Network), which has higher accuracy and precision than those methods. The accuracy is about 94%, and the precision is about 90%.

5.3. DISOT (Distributed Selfish Node Detection in Internet of Things). In paper [22], Nobahary et al. proposed a model in the hybrid system category to detect selfish nodes that drop the data packets using three steps: In the first phase (the setup and clustering), all network nodes are identified and clustered. The second phase (global phase) indicates whether a selfish node exists in the clusters or not by using the main cluster head that must monitor all other CHs and different kinds of nodes and identifying the selfish node (s) of each cluster by the cluster heads acts in the local section.

5.4. A Credit-Based Method. In the study by [23], an algorithm based on credit has been introduced to identify and resolve instances of selfish nodes that purposefully discard data packets. In each cluster, three nodes are designated as watchdogs to oversee the activities of other nodes. The parameters scrutinized to regulate the existence of selfish nodes within the cluster encompass the aggregate count of dispatched and received packets in combination, end-to-end delay, and the network traffic and throughput. The nodes are responsible for surveillance and transmit their discernment regarding the nodes under suspicion to the central node of the cluster. According to the majority vote, the central node then sends its opinion about the node to all other nodes.

5.5. A Contact-Based Model. In [24], a collaborative contact-based watchdog (CoCoWa) is introduced as a new model for identifying selfish nodes, which is a combination of identifying selfish nodes by using a local watchdog and releasing this information in the entire network. If one node has previously identified another node as selfish, it can transfer this information to other nodes when calling. In this way, the nodes are equipped with secondhand knowledge pertaining to the nodes exhibiting self-serving behavior within the network. The proposed methodology aims to decrease detection time and improve accuracy by lowering the effect of false alarm rate (FAR) and false-positive rate (FPR). The analytical evaluation generally indicated a significant decrease in selfish nodes' detection time and decreased overload compared with a traditional watchdog method.

5.6. QoS-OLSR (Quality of Service Optimized Link-State Routing). In [25], Wahab et al. examined detecting vehicular misbehavior in vehicle ad-hoc networks, whereby the vehicles either exceed or fall below the speed limit. This is accomplished by utilizing the routing protocol known as QoS-OLSR. The proposed method consists of two stages. The first stage stimulated the vehicles to behave generally during the cluster formation. After forming the cluster, the second stage tries to identify the misbehaving vehicles. The vehicles are divided into clusters in the first stage according to their location and speed. A cluster head and some MPR nodes are selected for each cluster. Each node in the network can use the services other nodes provide based on how trustworthy they think those nodes are. Some nodes are chosen as a watchdog for monitoring the conduct of MPR nodes. These nodes make determinations concerning the course of action for a given node based on their observations. Then, the final decision is made about the vehicle's behavior using the Dempster–Shafer theory and whole ideas of watchdogs, and other nodes are notified about selfish nodes.

5.7. A Reputation-Based Model. In VANETs, if the drivers have given the wrong information about a road closure, it will affect their decisions about how to get to their destination, how fast to drive, and how far to go. It could even cause accidents. In research conducted by Ding et al. [26], a new framework for vehicle reputation management has been proposed, using an ant-algorithm-based routing protocol. In this method, some event reporter vehicles are event monitoring vehicles, and event attendant vehicles include all roadside units in this path clustered as a virtual loop. Each vehicle's reputation is stored in all roadside units belonging to this ring in a distributed manner. After a run-off event, vehicles must eventually update their reputation based on their judgments about other vehicles' behavior. With this method's help, the authors could prevent false messages from spreading in VANET environments.

5.8. A Dempster–Shafer-Based Tit-for-Tat Strategy. In [27], the Dempster–Shafer Tit-for-Tat strategy is introduced as a non-cooperative repetitive game to identify selfish nodes (vehicles that sometimes use a very high speed to reach their destination and sometimes use a speed lower than the limit for selfish reasons); the Dempster–Shafer Tit-for-Tat strategy consists of five steps, including reputation calculation, maintenance monitoring, collect votes, set title rules for TAT and publish created information. In five steps, these operations are done in order, one after the other. First, some observers are designed to monitor MPR nodes' behavior; then, a voting mechanism is established between the observers in the identical transmission locale. The leader of each group subsequently assembles the ballots of the stationed observers in its corresponding cluster by applying the Dempster–Shafer principle. Ultimately, the cluster leader disseminates the verdict to all personnel within its domain and notifies other clusters in case of communication to minimize administrative burden and execution time. As a result, the members isolate the vehicles as selfish nodes.

Tables 1, 2 and 3 compare each paper's essential benefits and weaknesses for detecting selfish, malicious, and both types of these nodes. In each of these tables, each method has some key aspects and cons. None of these approaches satisfy our expectations, so researchers in this field can provide better algorithms.

The parameters studied in Tables 1, 2, and 3 include scheme name, year of publication of papers, the simulator used in the article, number of detected misbehavior nodes, the overhead of the proposed method, throughput, packet delivery rate (PDR), key aspects, drawbacks of the proposed methods.

The parameters of the number of detected misbehavior nodes, throughput, and PDR, in some cases, their exact value is not written by the authors of the articles, or the graph related to these parameters is not drawn. In this case, as far as the authors were able, they calculated their values and put them in the relevant Table, but otherwise, their place is left empty.

Out of 62 papers, eight focus on detecting selfish nodes, 45 deal with identifying malicious nodes, and nine concentrate on detecting both selfish and malicious nodes.

6. Detection Schemes of Malicious Nodes

In this part of the document, we discuss several works that provide an algorithm for malignant node detection. Table 2 discusses the advantages and disadvantages of these algorithms, and Table 5 examines the characteristics of each work.

6.1. Rashid et al.'s Model. In this research [66], the authors have posited a real-time system for detecting malicious nodes. Especially for DDoS attack detection using machine learning which includes two algorithms: The initial approach employed in machine learning optimization is the Brayden–Fletcher–Goldfarb–Shannon (L-BFGS) method. At the same time, the secondary objective entails the quest to identify the apt optimization technique for the proposed VANET machine learning model. To achieve this, a distributed multilayer perceptron classifier (MLPC) is utilized, and the outcomes are assessed via OMNET++ and SUMO simulators, leveraging GBT, LR, MLPC, RF, and SVM models for machine learning categorization.

6.2. Bayesian-Based Model. In the present study [67], the authors devised a quantitative framework centered on the concepts of the coalition and signaling games to fashion an intrusion detection game. The game replicates the interactions between vehicles and the IDS agent and demonstrates the features of varied attack and defense phases. In addition, this approach endeavors to simulate the interactions between malicious nodes and the coalition leader outfitted with an intrusion detection system (CH-IDS). The intrusion detection game phase ascertains the essence of VANETs in every time slot. Concurrently, the Bayesian Nash equilibrium, with both pure and mixed strategies, compels the IDS agent to opt for the actions of idling or defending and not always defend, which, in turn, diminishes network overload. The simulation results evince the proposed scheme's dependability, which can forecast the type of nodes. The CH-IDS agent can select the most advantageous action, or optimal strategy, to counteract any malicious vehicle attacks.

6.3. MDFD. In their scholarly article [68], the authors present a comprehensive analysis of the nature of Sybil attacks, utilizing traffic flow state data from multiple sources. Additionally, they propose a novel framework for detecting such attacks, known as the multi-source data combination detection (MDFD) method. This method incorporates crucial safety messages, maps, and sensor data, utilizing a multi-dimensional approach to feature extraction across four domains: spatiotemporal relationships, traffic flow state changes, vehicle behavior features, and sensor data verification. Finally, the proposed framework employs a machine learning-based classification approach to identify instances of attack behavior.

6.4. Awan's Model. In this article [69], the authors present a novel clustering mechanism that utilizes an infrastructure-less method to ensure the network, ensuring the safety and privacy of information while also maintaining quality post-cluster formulation. The mechanism is based on predefined Quality of Service (QoS) parameters, such as packet delivery rate for facilitating communication, runtime required to assess response rate, and average comment score. During cluster head selection, QoS parameters are integrated into trust parameters, and decision-making involves utilizing the absolute value that has been calculated. The proposed mechanism employs blockchain to encrypt trust parameter calculations to address possible attacks, including detecting malicious and vulnerable nodes in the VANET network. The trustworthiness of each vehicle is measured by the base station and transmitted to Roadside Units (RSUs) for further use. By integrating QoS and Trust, the proposed methodology presents a ranking system enabling the cluster to select its backup cluster head through computation efficiently.

6.5. Fog-Based DDoS Detection Method. Fog-based models within VANET encompass highly dynamic nodes, including roadside units (RSUs) and parked vehicles that receive information from other nodes and transmit it to fog servers for processing. In their work, Gaurav et al. [70] proposed a schema to detect DDoS attacks that leverages specific fog nodes and servers. Within VANET, the fog nodes undertake network analysis and save critical information in the fog

Table 3: Comparison of detection algorithms of selfish and malicious nodes.

Scheme name	Year	Simulator	Number of misbehavior nodes detected	Overhead	Throughput	PDR	Key aspects	Drawbacks
Secured VANET (SV) [115]	2022	MATLAB	90%~95%	$O\ (N^2)$	> 90%	> 90%	High throughput, low delay	Not comparing with previous methods and having graphs related to fuzzy logic
A cooperative game-based mechanism [116]	2021	Not mentioned	—	$O\ (N^2)$	—	—	Consider fixed and mobile gateways scenarios, Increases the capacity of communication and connectivity	Different detection accuracy in different scenarios
Hierarchical game theory-based model [117]	2019	MATLAB	92%~100%	$O\ (N^2)$	~91%	> 90%	Low end-to-end delay, High detection accuracy	High negative alarm rate, Lack of encouragement to cooperate
A trust-based approach [118]	2018	NS3	—	$O\ (KN)$	—	—	Given second chance, High packet delivery rate	Energy consumption, High delay
UAV-assisted technique [119]	2018	NS-2	> 80%	$O\ (N)$	> 70%	~75%	High detection even with large number of misbehavior nodes High packet delivery in crowded environments	An expensive model, using less parameters for choosing cluster head
Credit-based model [120]	2016	NS-2	~85%	$O\ (N)$	> 70%	> 75%	High packet delivery, high cooperation between nodes (due to the limited flexibility threshold)	High error accuracy, Do not provide privacy
PPS [121]	2015	NS-2	72%~79%	$O\ (N^2)$	~34%	> 50%	High cooperation between nodes High stability of clusters provide privacy, safety Low incorrect judgments	Local observation, No provide reliable channel, second chance
DTM [122]	2013	NS-2	> 75%	$O\ (N)$	> 70%	72%~ 85%	Evaluate the performance of the method by presence of 25%, and 50% of malicious or selfish nodes, drop false data packets, provide integrity of message	No provide reliable channel, second chance
WD-TT [123]	2007	Not mentioned	—	$O\ (KN)$	—	—	Using watchdog for monitoring	High memory overhead

servers. The fog servers can deliver storage, computing, and other cloud infrastructures to the end device, expeditiously process incoming information, make swift decisions (thereby reducing latency), and identify malicious vehicle nodes. Each node generates a database for its neighbors, considers the initial trust value of all its neighbors as zero, adjusts their trust value based on its performance, and subsequently shares the database with the fog node. The fog node also sends this information to the fog server, which then shares it with the other fog servers, to ensure that every fog server holds the trustworthiness rating of each node within the system. The amount of trust can be range from −0.5 to +2. Suppose that the trust rating of any given node falls below the minimum threshold. In that case, it is flagged as a malicious node, and this information is disseminated to all users via the fog servers, leading to its blacklisting.

Table 4: Details of the papers reviewed about the detection of selfish nodes.

Publisher	Scheme name	Author	Journal/conferences
Elsevier	DSAM [20]	Zhang, B., Wang, X., Xie, R., Li, C., Zhang, H., and Jiang, F.	Future Generation Computer Systems
	System based on deep learning [21]	N. Jyothi, R. Patil	International Journal of Pervasive Computing and Communications
	QoS-OLSR [25]	O. A. Wahab, H. Otrok, A. Mourad	Computer Communications
Springer	A dempster–Shafer based tit-for-Tat strategy [27]	O. A. Wahab, H. Otrok, A. Mourad	WireLow Pers Commun
Other journals	DISOT [22]	S. Nobahary, H. Gharaee, A. Khademzadeh, A. Rahmani	International Journal of Information & Communication Technology Research
	A credit-based method [23]	S. Nobahary, Sh. babaie	Applied Computer Systems
	Contact based model [24]	V. Vidhya, S. Ramkumar	International Journal of Advanced Research in Engineering (IJARMATE)
	Reputation based model [26]	Q. Ding, X. Li	International Journal of Multimedia Technology

6.6. Signature-Based Authentication. In [71], an authentication system based on an anonymous signature is presented so that unauthorized users do not enter the network and forged messages are not exchanged. First, all VANET users must submit their original credentials. Then, TA generates public and private key pairs for each registered user; the private key must be kept secret by the VANET user. Registered vehicle users can communicate with RSUs and other vehicles. However, RSUs and other vehicles perform anonymous authentication to ensure a particular vehicle is legitimate before communicating with that vehicle. They check two conditions to ensure that the vehicle sending the message is legitimate. If these two conditions are met, the signature is valid, and the vehicle user is thus authenticated; otherwise, the user is rejected. (A unique value for the two parameters Zc and Ac (Authentication code) is given to the user during the offline registration process from TA.) Hence, message manipulation and impersonation attacks become practically impossible.

6.7. F-RouND (Fog-Based Rogue Node Detection). In their scholarly article denoted as [72], Paranjothi and Atiquzzaman introduced a proposed model that builds upon the Greenshield traffic model. The suggested methodology utilizes a guardian node to identify anomalous nodes within a geographical area. The exchange of vital information, which includes the status of braking and acceleration and the location of a vehicle, is facilitated through the transmission of beacon messages between vehicles. The categorization of vehicles into anomalous nodes by the safeguard node is followed by theory testing to verify the identification's accuracy. Vehicles with an acceptable range of speeds during the hypothesis test are categorized as cooperative nodes, while those that fall outside this range are flagged as anomalous nodes. Upon successfully validating the hypothesis test, the anomalous node proceeds to disseminate data regarding the anomalous nodes for every vehicle situated within the predefined zone.

6.8. BCSM (Blockchain-Based Security Method). In this study [73], the authors propose a security system based on blockchain technology for communication security in VANET. The proposed system constructs two types of blockchains in VANET: BCIR (Blockchain for identification on RSU) and BCCA (Blockchain for certification on CA), where the BCIR blockchain is connected to the RSU, which evaluates the reliability of the message, and the BCCA in the CA, which determines whether a node is legitimate or not. The legitimacy of a message is evaluated considering various factors such as message integrity, the reputation of the sending node, event type, loc_{event}, EventTime, time effectiveness, and distance effectiveness. The reputation of a node is defined by its communication behavior. By analyzing the communication behavior of a node, this method can determine whether the node is malicious or not. The proposed method detects denial-of-service (DoS) attacks, integrity targets, and false alarms and defends against their sabotage.

6.9. EPORP (Emperor Penguin Optimization-Based Routing Protocol)-Based Secure Protocol. The EPORP-secured protocol, as suggested in reference [74], has been proposed to augment the system's security and detect the existence of **Sybil attack** nodes. In the context of vehicular ad-hoc networks (VANETs), detecting Sybil attacks is crucial to mitigate instances of system failure. The Rumor riding technique has been employed to identify nodes participating in Sybil attacks. Furthermore, the SXOR (Split XOR) function ensures that the message and information remain secure. The EPO (emperor penguin optimization) algorithm is utilized to compute generating keys in the SXOR function. The proposed technique has demonstrated more satisfactory results than those produced by the FA (firefly algorithm), PSO (particle swarm optimization) algorithm, and WOA (whale optimization algorithm).

6.10. SAODV (Secure Ad-Hoc On-Demand Distance Vector). Dhanaraj and colleagues proposed a novel cryptographic scheme, as documented in reference [75], which is integrated into the AODV protocol to identify and counteract a black hole attack in the context of VANET environments. The SAODV algorithm, which improves the AODV routing protocol by incorporating security features, operates by storing and modifying RREQ and RREP packets. Encryption and decryption of these packets are carried out using the RSA algorithm, with the results being recorded in a lookup table. Any modifications made by malicious vehicles to the contents of the packets or the lookup table will be detected through this mechanism.

6.11. FBTRP-DBN (Fuzzy-Based Trust Recommendation Policy-Deep Belief Network). The FBTRP-DBN model proposed is a mechanism grounded in trust that aims to eliminate malicious nodes (the initiators of DOS attacks) from the VANET network by selecting an ideal cluster head, which is accomplished by identifying the highest trusted node. The cluster head selection involves certain vehicles, known as recommenders, who oversee the monitoring process. These recommenders evaluate the accuracy of data transmission and discern the actions of individual vehicles. The policy of FBTRP, in its determination of the retransmission trust value, employs two factors network density and the retransmission node distance factor. The fuzzy system calculates the "trust value" output using the provided inputs. Following the evaluation of the trust value, a deep belief network is utilized to predict the vehicle's malicious behavior in the future with the obtained threshold value. The cluster head then separates the vehicles into various lists, namely, green (cooperative), gray (abnormal), and black (malicious). Vehicles on the blacklist hold a heightened level of distrust and exhibit peculiar behavior. These particular vehicles are deemed malicious and possess an elevated threshold of untrustworthiness. The ash list associated with these automobiles displays abnormal conduct and occasionally disseminates fraudulent information across the network. Additionally, these vehicles may discard or duplicate packets. Conversely, vehicles on the Green List are proficient in sending and receiving messages and usually conduct themselves [76].

6.12. TREE. In the publication denoted as [77], the authors have formulated a trust-based message propagation scheme for a vehicular network for the purpose of discerning the issue of fraudulent nodes transmitting spurious alarm messages. Initially, they have contrived a trust-based mechanism to assess the credibility of the node through the node's message transmission pace and event notification execution to validate the veritable emergency warning messages. Based on the nodes' reputations, the trust score is approximated for each node in the network by means of assessing the average direct trust value according to the estimated trust value. The subsequent phase entails an evaluation of the vehicle's indirect trust, which is founded on the recommendations that are obtained from multiple neighboring vehicles. The assessment of the vehicle's efficiency in terms of reliability is carried out through the employment of both direct and indirect reliability measurements. Such an evaluation yields valuable information regarding the message transmission patterns of the node. Furthermore, the selection of the subsequent relay node is predicated on three essential parameters, namely trust score, node similarity, and link durability. To recognize fake alarm messages, a trust-based authentication approach is employed, utilizing the trust score and weight factor of vehicle network nodes.

6.13. BBAAS (Blockchain-Based Anonymous Authentication Scheme). The present article [78] delineates an anonymous authentication system that is founded on the blockchain. The proposed system entails the transfer of crucial materials and private information pertaining to vehicles directly to the closest trusted authority (TA) by vehicle units. The private information is managed exclusively by the TA and is securely stored in its database. In the proposed system, the TA is connected to the blockchain network along with the roadside units (RSUs). The RSUs and vehicle units undergo a preliminary authentication process at TA to obtain an authentication code and an alias identity. The TA utilizes this private information to establish the true identity of the vehicle based on the alias identities in the event of a dispute. After the initial authentication process at TA, RSUs can authenticate vehicles via the blockchain network using the verification code when they enter the RSU's coverage area. Upon entering the current RSU's communication area, the novel roadside unit (RSU) performs authentication of the vehicle by verifying the certificate presented by the preceding RSU, provided that the authentication process was successful in the current RSU. At this point, the RSU transfers the verification password to the vehicle. Additionally, the RSU and the vehicle establish a session key in this step [78].

6.14. Fog-Assisted Networks Based on Blockchain and Neuro-Fuzzy. In this research work [79], the authors proposed a lightweight and privacy-preserving authentication scheme without a certificate in VANET with the help of Fog using blockchain technology and fuzzy neural machine learning technique. An authentication scheme using certificate-less signatures based on elliptic curve cryptography (ECC) and hash functions has been developed. A neural fuzzy algorithm is proposed to detect unusual requests before the authentication process and reject them to prevent denial-of-service attacks. The proposed authentication method can defend against known attacks such as man-in-the-middle, replay, impersonation, and modification.

6.15. Sharma et al.'s Model. In this method, the authors try to discover frauds of location with the help of machine learning. One machine learning approach, supervised learning, is utilized for categorizing. Some well-known classification algorithms in this research include KNN (K-Nearest Neighbor), Decision Tree, Random Forest, and Naïve Bayes algorithm to detect misbehaving nodes. Also, this study has classified the types of attacks to fake the vehicle's location: constant attack, constant offset attack, random position attack, random offset position attack, and eventual stop attack, which, according to the type of their method, are as follows, pretending to be in a fixed place of the road in the network; add a constant, fixed value to the actual position; using a random Position; send a random number from a small area around their vehicle; act normally for some time then send a fixed position repeatedly to expose the vehicle stopped to gain trust in the network. The result showed that the KNN algorithm better detected misbehavior vehicles than others [80].

6.16. Improved Secure AODV. Kumar et al. improved [81] the routing protocol AODV to overcome the black hole attacks by adding security to the RREP and RREQ packets exchanged in the network. The security problem is improved with the help of digital signature, which is done in both encryptions in the source and decryption in the destination to ensure the identity of nodes. Also, a hash algorithm has been used for the message's authenticity. Then, the reputation of each node decreases or increases according to its performance in forwarding packets.

6.17. CBM (Collaborative-Based Misbehavior) Scheme. In a paper [82], Sultan et al. have proposed a malicious detection scheme based on participatory trust to detect vehicles that use fake identities in message forwarding and spread counterfeit data. The authors have used one of the physical criteria here: the extraction of received signal strength (RSS) that prevents vehicles from sending fake data or does not let them send it at all. The vehicular node, which is a participant in the system, generates a trust evaluation report utilizing the approach of SVM classification and its subsequent implementation transmits it surreptitiously to the trustworthy authority. The support vector machine (SVM) utilizing a Gaussian kernel function serves as the utilized mechanism for identifying misbehavior in vehicles. The present study in this investigation incorporates direct and indirect reputation calculation approaches. The direct form comprises gathering communication history and pertinent information through direct communication with the intended node. In the indirect reputation, each vehicle assigns a point to its neighbor vehicles and the nearest roadside unit after calculating the combined reputation for a particular vehicle; one can determine whether the vehicle is reliable by comparing the calculated values with the defined threshold values or not.

6.18. ECT. The proposed algorithm in [83] employs trust-based security measures to identify malicious activities, encompassing packet dropping and packet modification/modification attacks. The algorithm is rooted in direct and indirect trust, allowing for the computation of trust value and satisfaction of a given node sans supplementary control overhead. Direct trust can be computed by leveraging a given node's satisfaction value and weight coefficient. The satisfaction value can be derived by carefully examining three parameters that underlie the data transfer process over a designated time interval. Despite the significance of direct trust, more is needed to serve as a standalone metric of a node's dependability. The proposed model inquiries about the recommendations of neighboring nodes subsequently to direct trust concerning the observed node. The observed node's indirect trust or recommendation trust is computed based on these recommendations. A decision regarding the observed node is then made based on the trust gained directly and indirectly.

6.19. RBA (A Reputation-Based Algorithm). The algorithm expounded in reference [84] is founded on the esteem of nodes within the network to detect **DOS attacks**. The esteem of every individual node is determined by its transmission rate, precisely, the ratio of packets dispatched to subsequent nodes concerning the total packets received. In the proposed algorithm, when assimilating every node into the network, a default esteem value is conferred upon it. However, it is noteworthy that the said reputation of the node may undergo alterations subsequently, predicated upon the performance of the specific node in question. The observer node is responsible for monitoring each node's reputation value as and when deemed necessary. The selection of the observer node is contingent on various parameters. To qualify as the observer node, stringent criteria, including a good reputation value and minimal computational load, must be met.

6.20. QMM (QoS and Monitoring of Malicious Vehicles)-VANET. The proposed algorithm [85] monitors vehicles' behavior to identify malicious vehicles in the network. The stability of the network and communication is one of the critical concerns that significantly impact network performance. In this work, the authors have tried to maintain the stability of the network and prevent the performance of nodes that disturb the stability of the network. To select cluster heads, the proposed QMM-VANET clustering protocol carefully evaluates the quality-of-service parameters, including bandwidth, speed, interval, number of neighboring nodes, and distrust value. A vehicle that boasts of maximum local quality of service value is deemed eligible to be chosen as a head of a group of entities. Following this selection, the chosen vehicle identifies a set of appropriate gateways that facilitate packet transmissions and enable the connection of clusters. Finally, to tackle link failures, a recuperation method that involves the selection of different access routes possessing a satisfactory quality of service is employed.

6.21. TBM (QoS and Monitoring of Malicious Vehicles). The aforementioned study [86] presented a trust-centric framework for the identification of malicious nodes in ad-hoc networks that are utilized in vehicular settings.

Rogue or malicious nodes can receive the data packets and drop them between the source and destination. The proposed model first estimates the nodes' degree of trust and identifies the network's rogue nodes. The proposed method selects only reliable nodes to relay data in the routing process and then chooses the set of observer nodes to monitor nodes in the network. The observer node evaluates a particular node's combined trust, spreads the node's status in a binary flag across the network, and this study assesses the performance of a network through the examination of four key performance metrics, namely: packet delivery rate, throughput, distribution of load, and end-to-end delay.

6.22. A Blockchain-Based Model. Owing to the significant level of mobility and diversity of vehicle networks, adjacent vehicles are often unfamiliar with one another and need help to establish trust fully. This issue is further exacerbated by the misbehavior of vehicles within the network. Such attackers may deliberately disseminate untrustworthy messages. For instance, a vehicle may transmit a message indicating that it is safe to proceed when there may be an accident or traffic congestion ahead, thereby deceiving other vehicles. In their paper [87], Yang et al. utilized blockchain technology to propose a decentralized trust administration method for vehicular ad-hoc networks. The proposed model leverages the Bayesian inference model to enable vehicles to verify messages received from neighboring vehicles. Roadside units (RSUs) utilize vehicle-based rankings to compute the trustworthiness of each vehicle and consolidate the information into a "block." Subsequently, each RSU endeavors to add its "blocks" to the trust blockchain maintained by all RSUs. Through a collaborative effort, all RSUs work collectively to uphold a dependable and consistent database utilizing the blockchain technique. Simulation outcomes indicate that the proposed model effectively captures, computes, and stores trust values in vehicle ad-hoc networks.

6.23. An AODV-Based Model. The malicious node sends a lot of traffic (packets) to the network, so the network cannot handle it and becomes congested. When malicious nodes (nodes that are trying to disrupt the network) are in the network, it will take more bandwidth and more packets to send information through the network. This will slow down the entire network. In [88], Zaidi et al. try to detect malicious nodes with the AODV routing protocol's help so that vehicles and roadside units register in the certificate authority (CA) and receive their unique Id. But the way to distinguish a malicious node is that the certification authority receives the vehicle entry form, RSU, and the certification authority confirms the information. The RSUs and the vehicles make a communication to exchange packets. If the vehicle's ID does not match the registered ID, the certification authority will identify it as a malicious node.

6.24. EAAP (Efficient Anonymous Authentication Scheme with Conditional Privacy Preserving). In their paper [89], the authors proposed a novel scheme for ensuring secure VANET communication among vehicles. Specifically, the EAAP model introduced in the paper enables an RSU to authorize vehicles anonymously before transferring LBSI messages to others. Anonymously authenticating an RSU prior to receiving LBSI messages is ability vehicles possess, as described in the authors' paper [85]. Additionally, the EAAP mechanism offers anonymous authentication, certification validation, and digital signature expenses necessary for VANET applications. Additionally, the proposed scheme can function as a powerful mechanism for tracking privacy conditionally, facilitating the detection of the true identity of a disruptive vehicle. This can significantly enhance the overall efficiency and effectiveness of VANET.

6.25. A Game Theory-Based Trust Model. The vehicles share information about traffic conditions (accidents, delays, etc.) with other vehicles. If one of these vehicles gets an incorrect message about traffic conditions, it will tell the others. Hence, the authors in [90] proposed a trusted method based on game theories for VANETs. In the proposed model, the security game's attacker and defender identify and deal with malicious nodes. This strategy considers three parameters: "majority opinion, centrality, and node density." The game's outcome is determined by the cost of attacking and defending vehicles, and the best strategy to use is calculated using the Nash equation. At this point, the defending nodes, with high power and low density and the effort to retransmit, achieved a higher relational priority than the first attacking nodes.

6.26. On-Demand Model. In environments characterized by high mobility, Protocols for routing that rely on location information are utilized. Particularly in vehicle ad-hoc networks (VANETs), to identify and penalize malicious nodes that may discard, alter, or redirect data packets. These disruptive activities lead to network dysfunction, making it arduous to utilize. Protocols for routing rely on location information. Typically, the process involves three stages: discovery of geographic location, Response regarding the geographical position, and data forwarding. The proposed method comprises two states, namely, listening and identifying. Each node's reputation is evaluated by considering the number of packets forwarded (F_Count) against the number of packets in the forwarding request procedure (FR_Count). Each node evaluates its credibility and identifies a misbehavior node based on the reputation of other nodes. Nodes misbehaving can intentionally manipulate their routing protocol to discard packets, significantly impacting the send value [91].

6.27. A Model to Detect Blackhole Attack. The proposed algorithm [92] for detecting and preventing black hole attacks in vehicle ad-hoc networks, implementing routing protocols like AODV and DSR engenders heightened security Within the context of the ITS, particularly in city and highway scenarios. Such protocols serve to mitigate the impact of a malicious node. The source node, in particular, facilitates this by storing information relating to all received packets within a Pseudo reply packet table. An essential feature of this table is sorting false response packets in ascending order of their sequence. The priority is subsequently calculated based on the sequential number, with the highest priority given to the least number of orders. A node possessing an odd sequential number is considered malicious and is segregated by the source node and then the source broadcasts the message in the network.

6.28. FMBA (Fast Multi-Hop Broadcast Algorithm). The paper [93] analyzed the problems of position cheating attacks that can cause a reduction in safety applications. The proposed method notes the impact of malicious vehicles on delaying alert messages and attempts to identify highly effective ways malicious vehicles use to reduce the delay of alert messages and the effect of the attackers. The proposed method uses a fast multi-hop broadcast algorithm as a vehicle safety algorithm to reduce the time needed to send a message from a source to the furthest vehicle in a particular region. This algorithm consists of two phases: the phase of estimation and the broadcast phase. The estimation phase's primary objective involves assessing the incidence frequency for each vehicle within its communication range. This occurrence is contingent upon broadcasting a message to every vehicle located within the sender's region of interest; additionally, before sending a packet, each recipient's responsible for determining its waiting time before initiating a message transmission. A vehicle with a lower contention window (CW) will be elected as the next sender. Still, a malicious vehicle that sends a "Hello" message will cause a delay by increasing CW in honest vehicles.

6.29. Watchdog- and Bayesian-Based Model. Rupareliya et al. proposed a solution for preventing attacker nodes by using a watchdog and applying a Bayesian filter to find malicious nodes that don't forward the data packets [94]. Several nodes act as observers in the network and constantly listen to the neighboring nodes. If a node does not forward the packets to its neighbor node, the observer declares that node as a malicious node. Then they used the Bayesian observer to analyze malicious behaviors at different time intervals. Based on that, the Bayesian guard calculates the percentage of packets sent by the malicious node. If the ratio is lower than the threshold value defined, the Bayesian observer does not consider the node a malicious node; otherwise, it is regarded as a malicious node.

6.30. A Distributed Reputation-Based Scheme. Oluoch [95] posited a model of reputation that enables vehicles on the road to evaluate the reliability of other vehicles, thereby verifying the trust of messages transmitted on the network by unknown vehicles. The originating node computes the trustworthiness of each vehicle; after that, each vehicle that receives messages seeks feedback from other vehicles within its transmission range regarding the dependability of the vehicle dispatching the message. In the event of a lack of feedback, the receiving vehicle will seek the assistance of the road site unit (RSU) to ascertain information about the sender vehicle. The reliability of each vehicle is indicated by a reputation mark of t, which ranges from zero to one. The trust levels are expressed on a scale ranging from 0 as the minimum to 1 as the maximum. Vehicles receiving messages implement stringent thresholds, with messages from the sender vehicle deemed trustworthy. The average rating of all population members must exceed the set threshold to proceed.

6.31. VGKM (VANET Group Key Management). This study [96] proposes a new dual authentication scheme to improve the security of vehicles communicating with the VANET environment, verify authentication, and prevent the VANET user's validity from being forged and sending false messages to other vehicles. TA classifies users into primary, secondary, and unauthorized users. Then, a dual group key management scheme is implemented to effectively distribute a group key among each user group and update these group keys during user join and logout operations. In dual mode, two components are used: the hash code of each communication vehicle and the fingerprints. Therefore, the fingerprint authentication techniques in this study are integrated into a hash code generation method to prevent malicious users from using each network user's secret key to participate in VANET communications.

6.32. DMN (Detection of Malicious Nodes). In paper [97], the proposed algorithm is that a vehicle gets cluster keys after joining the network. Then the parameters: load, distrust value, and distance are calculated for neighboring vehicle nodes to select the verifier, then the proposed model finds the nodes with lower decision threshold values, and these nodes are assigned as verifiers to the recently joined vehicle. Verifiers monitor the vehicle's behavior; if they detect abnormal behavior, they report it to the cluster head (CH). The cluster calculates the value of the new distrust parameter for the vehicle. If the distrust value is detected as higher than the threshold, the whitelist will be updated, and the vehicle will be entered into the blacklist. A warning message is sent to all other nodes based on introducing malicious nodes. The malicious vehicle has isolated access to the network, so it cannot drop and duplicate packets.

6.33. T-ACO (Ant Colony Optimization). The proposed method [98] used the trust metric and AODV routing protocol to detect malicious nodes. The proposed algorithm is based on an Ant colony with two agents, FANT and BANT. Forward ant agents (FANT) move from source to destination to collect route information about the route's quality on the way to the destination. The Backward ant agents (BANT) move from destination to source to create new paths. Ants leave the pheromone on the path while moving. So, the value of trust for each node and the amount of pheromone for each route are calculated. Suppose the trust value is lower than the threshold and the pheromone value is zero, so the node is malicious. The quality of each path is calculated, and the route with the highest quality is selected for sending packets.

6.34. Fox-Hole Region (FHR). Authors have proposed [99] a data-centric model for detecting misbehavior that broadcasts false traffic information in vehicle ad-hoc networks, focusing on alert messages, including the PCN and the beacon message (information about the vehicle's location under observation being broadcast by the OBU). The proposed model consists of an area defined by the position around the crash. It may vary for each vehicle that can observe the event (depending on its speed). In the proposed model, assume that position L is the position of the crash. Each coordinate is assigned a weight near the crash alert (L)

(0, 1). Also, a confidence parameter based on the region below is extracted from the curve that shows the vehicle's route starting from the event location. A factor "β" is used to measure the truth of the information in the PCN alert.

6.35. DMV (Detection of Malicious Vehicles). The research proposed [100] an algorithm that could detect if a vehicle is malicious or not (for example, by looking at how it behaves packets, forwarding them, or dropping or duplicating). Some of the trustier neighbors monitor each vehicle, called verifier nodes. If a verifier vehicle perceives an abnormal behavior from each of the nodes under its supervision, it raises the distrust value of the vehicle. The vehicle's ID is then announced to its appropriate Certificate Authority as a malicious node when its distrust value exceeds the threshold value. The vehicle's name is entered in the black list. The blacklist separates malicious vehicles from honest vehicles stored in the list. Malicious vehicles are isolated from the network after being added to the black lists, and other vehicles do not accept any messages from the vehicles on the blacklist. Ultimately, the review results show that the DMV technique is able to discover most vehicles that have malicious behavior due to high speeds.

6.36. D&PMV (Detection and Prevention of Malicious Vehicles). In research [101], Kadam and Limkar presented an improved DMV algorithm (improved DSR), detecting malicious vehicles and preventing them from operating in the network. In this algorithm, to detect malicious nodes, first, the nodes are placed in appropriate clusters, and the main cluster head and one spare cluster head are chosen. Then, the behavior of each node is examined with the help of observers. If it is less than or equal to the specified threshold value, its name will be whitelisted; otherwise, a malicious node will send a warning message to the other nodes in the cluster. The prevention algorithm is activated if the malicious node is found in the previous step. That path is left aside in the found path, and an alternative communication path is used. This methodology decreases the consequences of a potential black hole attack in vehicle ad-hoc networks, and the mechanism is impressive and safer than the previous ones.

6.37. Improved AODV Protocol (RAODV (A Robust AODV)). In paper [102], the AODV protocol has been presented with a security model for detecting malicious vehicles. The architecture implements a registration system managed by a central authority in each vehicle and RSU, assigning a particular identity to each node upon submission of its primary identification, such as the number of vehicles. The Government ensures the preservation of RSUs to prevent any failure. The RSUs in the network gather and retain data, including vehicle identity, vector, and classification of all vehicles that pass through their region through a camera. The proposed architecture employs performance metrics, such as Packet transmission success ratios, average end-to-end delay, the overhead of routing, and the number of discarded packets, to identify any malicious nodes. Upon identification of a malicious vehicle by the central authority (CA), a warning notification will be distributed to the surrounding zone, encompassing nearby RSUs and vehicles. The packets shall not be transmitted to vehicles with malicious intent but instead will be segregated from other vehicles using the RAODV protocol. The outcomes of the suggested mechanism have demonstrated that the RAODV protocol can successfully discern a malicious vehicle after the assignment process.

6.38. Heartbeat Message-Based Misbehavior Detection Scheme (MDS (Misbehavior Detection Scheme)). Barnwal and Ghosh [103] have developed a model to detect the misbehavior of vehicles that can detect malicious nodes that broadcast fake information about the measurement of position and velocity can be achieved through the utilization of heartbeat rate messages. The vehicle designated as the observer utilizes the data within the heartbeat messages to determine the veracity or malfeasance of a given node. From the examination of new data, it has been assumed that the expected and observed position of the reported vehicle is calculated by the observer vehicle. If the results do not match, the index of suspicion will increase compared to that vehicle. If the level of suspicion is higher than the threshold value, the vehicle will be considered malicious. This method's advantage is that it does not create any communication overhead in these networks or require additional sensors because it uses a periodic message.

6.39. System Based on Detecting Cheaters. In the proposed approach [104], Huang et al. have suggested an identification protocol aimed at identifying malicious vehicles that disseminate counterfeit information regarding traffic congestion with ulterior motives and adopt the guise of unreal vehicles. The approach employs sensors to verify the vehicle's congestion based on local speed and distance measurement, and it leverages the kinematic wave distinguish method, which allows the vehicle to anticipate over time and space. Consequently, it can recognize nodes that exhibit improper conduct by transmitting false traffic congestion information. The architecture entails a vehicle's signature to identify and stop numerous malefactors with legitimate certificates (forgery) from falsifying traffic. The certificate must be appended to the signature packet. The proposed solution is advantageous since it solely hinges on connections with adjacent nodes and does not necessitate a system to detect traffic congestion.

6.40. MBRMS (Misbehavior-Based Reputation Management System). In the proposed method [105], Kim and Bae have presented a new misbehavior-based reputation management system consisting of three components: (1) detection of misbehavior, (2) event broadcast, and (3) global eviction algorithms for detecting and filtering inaccurate information in these networks. Each vehicle maintains system information and relevant events to detect misbehavior nodes. The proposed mechanism uses a different diagnostic technique, and when an event observer receives an alert message from an event reporter, it detects the alert type of the alert message. When the event observer receives light from the warning vehicle after a while, it calculates the relative classification error (RCE) using the rough sets of variable accuracy [11] of the event. It also uses the risk level of the malicious node to measure the risk value. This method most effectively detects and isolates misbehaving nodes.

6.41. RB-CD (Repetition-Based Broadcast Diversity Technique). The study [106] proposes a new and efficient protocol for sending repetition-based messages that uses various cooperation techniques. This method contains three phases: (1) initial broadcasting, (2) selecting the relay node, and (3) repetition phases for cooperation. The main idea is to repeat a broadcast message correctly, cooperating with the source and the neighbors. The proposed relay selection algorithm is a disseminated algorithm that magnifies the broadcast message's reception rate, which is designed for broadcasting single-hop safety applications, especially for essential messaging applications (EMD).

6.42. VARM (VANET Association Rules Mining). This study [107] created a mechanism that collects transmission data about each vehicle in a neighborhood and then extracts the rules of temporary correlation between vehicles related to transmissions in a neighborhood. This method is proposed to develop communication rules for finding a faulty or malicious vehicle that transmits inaccurate information. For example, a vehicle is unrelated to the vehicles in contact with it, and adhering to these rules is unrelated. Sorted structures are constructed based on the priority relation and use the item to conceive a set tree. The proposed model displays superior performance when compared to the FP-tree. Furthermore, it has been demonstrated that the cats-tree exhibits a low and dense configuration. Both data sets exhibit a lower concentration of execution intervals when compared to the present data.

6.43. Data Centric Detection Schemes. Data exchange between nodes is examined in data-centric approaches, so the misbehavior is identified. This mainly relates to the communication between messages that leads to the detection of selfish nodes. The information disseminated by the nodes within the network is subjected to a comparative analysis with the data relayed to other nodes to ascertain the veracity of the alert announcements received. Therefore, any vehicle that sends fake details on various events in these networks, such as fake congestion messages, incorrect positions, false alarms, vehicle crashes, and road conditions, is considered misbehavior. In [108], the author has identified the transmission of false information and misbehavior nodes by monitoring vehicle actions after sending alert messages. The coordination of reported and estimated vehicle positions is essential to enable the making of appropriate decisions based on the available information. Instead of revoking the secret credentials, this scheme applies fines to misbehaving nodes; the certificate authority's credentials prevent the nodes from having malicious and selfish behavior. This will reduce the calculation and communication costs of revoking the secret credentials. The findings indicate that the suggested framework outperforms alternative frameworks with transmission overhead when transmitting a record of invalidated private certificates to the roadside unit.

6.44. System Based on Machine Learning. The study introduces a novel approach [109] that utilizes machine learning techniques to establish a Security architecture for classifying numerous forms of misconduct in vehicle ad-hoc networks. A misbehavior node can manipulate data packets by altering its identity, position, time of transmission, and safeness message. The attacker node can also fabricate counterfeit messages or coerce other nodes to generate such messages.

The features extracted from various attacks and misbehavior that the senders of the security packet are removed to distinguish between different misbehavior types. The proposed approach classifies several types of misbehaviors in this type of network. It has been observed that J-48 and Random Forest classifiers exhibit superior performance compared to other classifiers such as Naive Bayes, IBK, and AdaBoost1. A voting system that allows the majority to decide to get a better and more accurate detecting system. This method is better and highly efficient in categorizing multiple misbehavior practices in vehicle ad-hoc networks than primary classifications in other papers.

6.45. Intrusion Detection Model. In the paper [110], a method for detecting intrusion based on signature has been presented, capable of distinguishing simulated congestion and denial of congestion attacks caused by malicious vehicles. A navigation system has been launched in each vehicle that includes information about each vehicle's position and the road on which it travels. The position information received from the CAM represents the vehicle's center; given this information, a moving vehicle's rectangular model on the road can be drawn. With this model's help, it can be calculated whether different vehicles' rectangles intersect because malicious vehicles give fake information about their position and cause a fake traffic jam. Each node also calculates a certain amount of trust for its neighbors, which is achieved with the vehicle's first and latest beacon messages, which are B_j^1 and B_j^n respectively, and variable d_{i} shows the distance between the beacons calculated by N_{i}, and the minimum-distance-moved (MDM) is the shortest transmission range. If $d_i\,(B_j^1, B_j^n) \geq d_{\mathrm{MDM}}$ then the trust level is equal to $(\tau = 1)$.

6.46. A System-Based Alert. An "event" is a collection of observations that provide information on an initial alert's probability. These groups have many "event classes," each containing some events. The performance of each event in each category is defined by specific attributes that relate to that class. In their publication referenced by number [111], the authors presented a technique for detecting a possible mistake by relying on supplementary data or notifications generated after the initial notifications. The authors find a way to use information about a suspicious alert to confirm whether the initial event that caused the alert was real to reduce the number of false alarms. Secondary data received as warnings of causality can be gathered to establish credibility for the direct messages. The notified behavior is cross-referenced against the vehicle's warning system to assess the circumstances necessitating an escalated alert. Thus, if the two are incongruent, it indicates a fraudulent alert, characterizing the vehicle as malevolent.

6.47. RCBD (A Root Cause-Based Detection). In their study documented in [112], Ghosh et al. have advanced their research by acknowledging the potential for erroneous information about the vehicle's location in transmitting false collision notifications. They have also introduced the utilization of the Post-Crash Notification (PCN) application to display crucial factors contributing to the effectiveness of their proposed model. The cause-tree model is a highly effective tool in detecting instances of misbehavior and accurately identifying the underlying cause of logical cuts. This scheme proves to be healthy and identifies many misbehaving nodes.

6.48. Ghosh et al.'s Method. There is always a chance of incorrect messages being transmitted due to faulty sensors or purposeful malicious activities. In [113], Ghosh et al. proposed a robust model for detecting malicious vehicles for a crash declaration. The utilized methodology initially observes the driver's actions after an escalation in a collision warning message. The vehicle's movement is monitored, and the anticipated trajectory of the vehicle is computed using the collision transportability model. If the disparity among two given values surpasses the threshold value, the warning is regarded as erroneous; subsequently, the warning is deemed incorrect with that verge value. This methodology proficiently diminishes the rates of false alarms (FAR) and false positives (FPR) and identifies instances of misconduct.

6.49. VARS (Vehicle Ad-Hoc Network Reputation System). One of the challenges is to make sure that the emergency message the vehicle receives is reliable (it is not fake), and that it is time-stamped (it was not changed while it was being sent).

One of the hazards of malicious nodes is sending false alarms in the network. A reputation-based model [114] for vehicle ad-hoc networks introduces many mobile nodes. The proposed model has direct and indirect reputations for each event message. Each sending node adds a comment to its message about the reputation of the message. They say this mechanism is "Piggybacking," meaning when a message is sent to each node, each generates its own opinion on its reputation and attaches it to the message.

7. Detection Schemes of Selfish and Malicious Nodes

This part of the paper reviews various papers that provide an algorithm for detecting selfish and malicious nodes. In the following, Table 3 discusses the advantages and disadvantages of these algorithms, and Table 6 examines the features of each paper.

7.1. SV (Secured VANET). Alkhalidy et al. proposed [115] a new strategy for catching malicious nodes in the vehicle network. Malicious vehicles send wrong emergency information in the network to restrict nodes from accessing the channel to receive road information. Numerous elements are chosen for the fuzzy logic scheme to calculate the trust of nodes participating in the vehicle network. In this method, vehicles divide into clusters, and a roadside unit governs each. The roadside unit estimates the nodes' trustworthiness before letting vehicles access the network. The roadside unit dismisses a malicious node based on its trust value. The proposed method has been offered to detect malicious nodes. Still, by doing simulations, the authors realized that their method could also detect selfish nodes, so we put this method in the category of detecting malicious and selfish nodes.

7.2. A Cooperative Game-Based Mechanism. In the paper [116], the authors introduced a mechanism based on coalition game theory for data transmission with nodes in VANET. Based on many parameters, such as geographical location and movement direction, vehicles can be grouped into a coalition based on the predicted distance and longevity of links created between vehicles and the gates and their joint transmission planned. On the other hand, the gates can join the coalitions to cooperate in relaying the vehicle's data over the Internet. Every vehicle tries to access the wireless Internet or the fixed Internet. Two scenarios are used to evaluate the proposed solution better: the fixed gate scenario and the mobile gateway scenario. The simulation results show that the gates' mobility increases the transmission with cooperation and increases the communication and connection capacity in the vehicle networks.

7.3. Hierarchical Game Theory-Based Model. Nobahary et al. [117] showed that the misbehavior nodes could be identified and stimulated, as the proposed method takes three steps. The setup and clustering algorithm is run in the first phase and starts sending data and playing the game to detect the malicious and selfish nodes. In the next step, each cluster's nodes cooperate in executing a limit Low repeated game while forwarding their packets or neighbor nodes' packets. In the next phase, each node monitors its neighbor nodes' actions to know if they forward the packets or not. The cooperation procedure is excavated for specifying the selfish or malicious nodes that did not send the packets or forwarded the packets with a latency. In the end, the network's misbehavior nodes' reputation has been decreased by other nodes.

7.4. A Trust-Based Approach. In this study [118], a completely decentralized approach aims to encourage and implement the plan to identify and prevent malicious nodes from injecting false information into the network.

Table 5: Details of the papers reviewed about the detection of malicious nodes.

Publisher	Scheme name	Author	Journal/conferences
Elsevier	Rashid et al. 's model [66]	Rashid, K., Saeed, Y., Ali, A., Jamil, F., Alkanhel, R. and Muthanna, A.	sensors
	Bayesian based model [67]	Mabrouk, A., and Naja, A.	Computer Networks
	MDFD [68]	Chen, Y., Lai, Y., Zhang, Z., Li, H., and Wang, Y.	Computer Networks
	Awan's model [69]	Awan, K. A., Din, I. U., and Almogren, A.	Sustainability
	Fog-assisted networks based on blockchain and neuro-fuzzy [79]	Ogundoyin, S. O., and Kamil, I. A.	Vehicle Communications
	Signature-based authentication [71]	Rajasekaran, A. S., and Islam Satti, M.	Security and Communication Networks
	F-RouND [72]	Paranjothi, A., and Atiquzzaman, M.	Digital Communications and Networks
	BCSM [73]	Liu, G., Fan, N., Wu, C. Q., and Zou, X.	Sensors
	EPORP-based secure protocol [74]	N. C. Velayudhan, A. Anitha, and M. Madanan	Wireless Personal Communications
	SAODV [75]	R. K. Dhanaraj, SK. H. Islam and V. Rajasekar	Wireless Networks
	BBAAS [78]	Maria, A., Pandi, V., Lazarus, J. D., Karuppiah, M., and Christo, M. S.	Security and Communication Networks
	Improved secure AODV [81]	An. Kumar, V. Varadarajan, Ab. Kumar, P. Dadheech, S. S. Choudhary, V. A. Kumar, B. K. Panigrahi and K. C. Veluvolu	Microprocessors and Microsystems
	QMM-VANET [85]	H. Fatemidokht, M. K. Rafsanjani	Systems and Software
	A game theory-based trust model [90]	M. Mehdi, I. Raza, S. Hussain	Computer Networks
	A model to detect blackhole attack [92]	P. Tyagi, D. Dembla	Egyptian Informatics Journal
	FMBA [93]	W. B. Jaballah, M. Conti, M. Mosbah, C. E. Palazzi	Ad-hoc Networks
	Watchdog and Bayesian based model [94]	J. Rupareliya, S. Vithlani, Ch. Gohel	Communication, Computing and Virtualization
	DMN [97]	U. Khan, S. Agrawal, S. Silakari	International Conference on Information and Communication Technologies (ICICT)
	RB-CD [106]	H. Yoo, D. Kim	Computer Communications
	Root cause-based detection (RCBD) [112]	M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, S. N. Muthaiah	Ad-hoc Networks
Springer	FBTRP-DBN [76]	K. N. Tripathi, A. M. Yadav, S.C. Sharma	Wireless Personal Communications
	TREE [77]	K. N. Tripathi, A. M. Yadav, S. C. Sharma	Arabian Journal for Science and Engineering
	Fog-based DDoS detection method [70]	A. Gaurav, B. B. Gupta, F. J. G. Peñalvo, N. Nedjah, and K. Psannis	Security and Privacy Preserving for IoT and 5G Networks
	CBM scheme [82]	Sultan, S., Javaid, Q., Malik, A. J., Al-Turjman, F., and Attique, M.	Environment, Development and Sustainability
	ECT [83]	K. N. Tripathi, G. Jain, A. M. Yadav, S. C. Sharma	In Next Generation Information Processing System
	RBA [84]	K. N. Tripathi, S. C. Sharma, G. Jain	Soft Computing: Theories and Applications
	TBM [86]	K. N. Tripathi, S. C. Sharma	International Journal of System Assurance Engineering and Management
	DMV [100]	A. Daeinabi, A. Ghaffarpour Rahbar	Multimed. Tools Appl
	D&PMV [101]	M. Kadam, S. Limkar	Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)
	MBRMS [105]	C. Kim, I. Bae	Embedded and Multimedia Computing Technology and Service
	System based on machine learning [109]	J. Grover, N. K. Prajapati, V. Laxmi, M. S. Gaur	International Conference on Advances in Computing and Communications
	A system based alert [111]	A. Vulimiri, A. Gupta, P. Roy, S. N. Muthaiah, A. A. Kherani	International Conference on Research in Networking

Table 5: Continued.

Publisher	Scheme name	Author	Journal/conferences
Other journals	A AODV based model [88]	T. Zaidi, Sh. Giri, Sh. Chaurasia, P. Srivastava, R. Kapoor	International Journal of Ad-hoc, Sensor & Ubiquitous Computing
	On-demand model [91]	H. Yao-Hua, L. Chun-Han, C. Ling-Jyh	International Journal of Distributed Sensor Networks
	RAODV [102]	V. Lakshmi Praba, A. Ranichitra	ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY
	T-ACO [98]	Patel, Kishan N., and Rutvij H. Jhaveri	International Journal of Computer Applications
IEEE	Sharma et al. 's model [80]	Sharma, A. Jaekel	In 2021 International Conference on Computer Communications and Networks (ICCCN)
	Blockchain-based model [87]	Yang, Z., Yang, K., Lei, L., Zheng, K., and Leung, V. C.	Internet of Things Journal
	EAAP [89]	Azees, M., Vijayakumar, P., and Deboarh, L. J.	IEEE Transactions on Intelligent Transportation Systems
	A distributed reputation based scheme [95]	J. Oluoch	International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)
	VGKM [96]	Vijayakumar, P., Azees, M., Kannan, A., and Deborah, L. J.	IEEE Transactions on Intelligent Transportation Systems
	FHR [99]	S. K. Harit, G. Singh, N. Tyagi	Third International Conference on Computer and Communication Technology
	MDS [103]	R. P. Barnwal, S. K. Ghosh	International Conference on Connected Vehicles
	System based on detecting cheater [104]	D. Huang, S. A. Williams, S. Shere	International Conference on Trust, Security and Privacy in Computing and Communications
	VARM [107]	J. Rezgui, S. Cherkaoui	Local Computer Networks
	Data centric detection schemes (DC) [108]	S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, I. Stojmenovic	In Vehicle technology conference
	Intrusion detection model [110]	N. Bißmeyer, C. Stresing, K. M. Bayarou	Vehicle Networking Conference
	Ghosh et al.'s method [113]	M. Ghosh, A. Varghese, A. A. Kherani, A. Gupta	WireLow Communications and Networking Conference
	VARS [114]	F. Dotzer, L. Fischer, P. Magiera	World of WireLow Mobile and Multimedia Networks

Table 6: Details of the papers reviewed about the detection of selfish and malicious nodes.

Publisher	Scheme name	Authors	Journal/conferences
Elsevier	Secured VANET (SV) [115]	M. Alkhaliday, A. F. Al-Serhan, A. Alsarhan, and B. Igried	Future internet
	A cooperative game-based mechanism [116]	A. Mabrouk, A. Naja, O. A. Oualhaj, A. Kobbane, M. Boulmalf	Simulation modeling practice and theory
	UAV-assisted technique [119]	C. A. Kerrache, A. Lakas, N. Lagraa, E. Barka	Vehicle communications
	PPS [121]	A. Jesudoss, S. V. Kasmir Raja, A. Sulaiman	Ad-hoc networks
Springer	Hierarchical game theory-based model [117]	S. Nobahary, H. Gharaee, A. Khademzadeh, A. Rahmani	Wirelow communications and networking
	WD-TT [123]	Z. H. Wang and C. H. Chigan	Wirelow personal communications
IEEE	Credit based model [120]	C. A. Kerrache, A. Lakas, N. Lagraa	In electronic devices, systems and applications (ICEDSA)
	DTM [122]	N. Haddadou, A. Rachedi	International conference on communications (ICC)
Other journals	A trust-based approach [118]	Ah. Zouinkhi, A. Ltifi, Ch. Chouaib, M. N. Abdelkrim	Int. J. information and communication technology

By examining the proposed method, the authors realized that the algorithm for identifying selfish nodes also performs well. In the proposed method, the leader controls the transport packets, acting as an "observer." The observer uses the incentive mechanism given according to the value of the "flag" produced by the leader. Next, the observer node will distribute rewards to coworker nodes. The incentive mechanism spreads rewards to fellow nodes according to the number of "flags" generated by the leader and the punishment system, including a gray and black list. The gray list (ID) stores malicious nodes that have been temporarily deleted. If a node reaches the value "flag = (−6)", it will be placed in a gray list and become a punished node, and it shows the value of the trust flag of the node, with the help of which the selfish node is also identified. If it continues its malicious behavior, it will be blacklisted and permanently removed from the group of vehicles. The security mechanisms are based on asymmetric and RSA encryption by creating public and private keys and digital signatures to ensure packets' security.

7.5. UAV (Unmanned Aerial Vehicle)-Assisted Technique. Trust-oriented answers can effectively manage a range of security hazards in Vehicular Ad-hoc Networks (VANETs), such as Denial of Service (DoS) attacks, black holes, gray holes, and collision scenarios. The proposed approach entails the integration of a mechanism that adjusts the detecting threshold., which enables the identification of intelligent malicious activities, such as identity-changing and faking schemes.

In the proposed method [119], which is an improvement of [89], a drone separates the road parts into virtual fixed groups after determining the amount of direct and indirect trust of each vehicle. Then, a cluster head is selected, which is the closest node to the central point of the division. However, in the subsequent interactions, the selection strategy is based on 1- Trustiness and 2- Its closeness to the cluster's main topic. A cluster head interacting with cluster members has already collected their recommendations about each other; hence, it can directly list its blacklist as a local cluster localization without further processing. This will prevent further processing delays and overheads. Some malicious vehicles devote different identifiers (IDs) to stay unidentified (they change their identities when identified). These vehicles are also recognized; their IDs are included in the general blacklist and are notified to other vehicles using the roadside unit and drones.

7.6. Credit-Based Model. Credit-based methods are considered for all nodes in the network to have an initial credit, and then, in proportion to each node's performance, the cluster will reduce or increase this value. In the proposed method [120], for each vehicle, the initial confidence is 0.5, then, the trust computation, directly and indirectly, takes place. These trusts are characterized as a regional evaluation grounded on direct vehicle exchange, calculated in terms of a vehicle's legal and malicious actions. The indirect trust is calculated with the help of the neighbors' recommendations that they are one hop away from the vehicle in question. Of course, the neighbors with higher trust got increased offers. If a vehicle notices that one of its neighbors is behaving dishonestly, it will increase its level of detection (how much it trusts its neighbors), and reads the data the vehicle gives and if it sees any unusual behavior (for example, if the data is always in the same range), it will raise the detection threshold (TH) so that it will detect abnormal values. Instead of using a single fixed value to decide whether to give a vehicle punishment, vehicles can use a range of thresholds that change depending on the behavior of their neighbors. The proposed method successfully detects the attackers that cleverly adjust and change their behavior (Figure 9) to evade detection and prevent exclusion from the network's functions.

7.7. PPS (Payment Punishment Scheme). The proposed method [121] is based on motivation so that a reputation is considered for each node, and with the cooperation of the nodes, their reputation is increased. In this manner, there is a motivation for all nodes to collaborate in the network. In the proposed method, the packets are forwarded to other network nodes with clustering for enhanced monitoring. Determining the cluster-head node and an associate cluster-head node is based on specific parameters within each cluster. Additionally, three watchdog nodes, comprising the previous relay node, associate cluster head, and one of the neighboring vehicles, are chosen as cluster watchdog nodes over a short period using the round-robin method. These nodes maintain the source's data to the intermediate nodes in a table. Once the intermediate node sends the data, the watchdog node contrasts it with the data in the table, and if an inconsistency is detected, appropriate measures are taken.

It is known as a suspicious node. Data aggregation should be done with the replacement of some watchdog nodes. For this purpose, the Dempster–Shafer theory is used to determine the cooperation or selfishness of the suspicious node. The nodes of the cluster will be awarded If the node is selfish. According to the authors, this method can detect all malicious attacks such as packet dropping, replay attacks, free riding attacks, non-repudiation, reputation stealing attack, bad-mouthing attack, collusion, and false appraisal.

7.8. DTM (Distributed Trust Model). The authors proposed a practical solution that filters out the nodes that spread false information, retransmit modified data packets, or use the network's resources. Thus, their collaboration rate is low. Due to the reduction of network efficiency in these conditions, selfish and malicious nodes in the network should be discovered and discarded. The DTM [122] is a distributed trust model inspired by Spence's job market model in the economy, for each node is assigned a credit account that can be increased or decreased due to its behavior. This credential is used to gain network benefits, such as receiving messages from other nodes.

On the other hand, a node whose credit expires, the node is identified as selfish and driven out of the network. In this model, the sender sends a signal with its message. This signal indicates the integrity of the message for potential recipients. The source node must pay the price for using the signal; its cost depends on the value and the node's behavior. The signal's cost is based on the sender's behavior. If the sender is abusive, then the signal will be expensive. The model

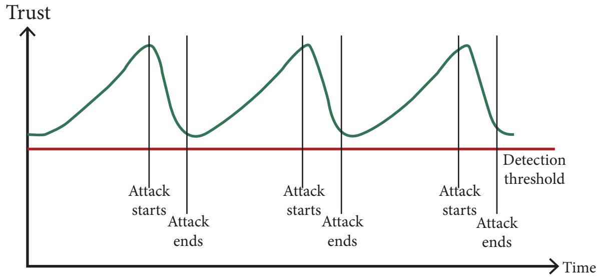

Figure 9: Attackers' clever behavior [116].

removes the sender nodes from acting maliciously because the transmitter nodes' cooperation is proportional to the signal received.

7.9. WD-TT (WatchDog-Trust Token). The proposed method tries to detect selfish nodes that do not forward packets to others and malicious nodes that attack the packet's authenticity and data integrity. The authors of the paper [123] proposed a WD-TT mechanism to predict the way a network will behave based on how vehicles send packets of data. The proposed method has three protocol nodes: prior, relay, and successor. The relay node is a part of the network that gets messages from one part of the network and passes them onto other parts. The relay nodes forward the packet to all possible routes, so the packet could reach its destination ensure. The prior (former) is a single-step relay node that acts as a Watchdog. The Successor (suc) replaces one of the single downstream from the single relay that decides whether to accept packets or not. The former and alternate nodes are within the relay node's wireless transmission range. Each node has a buffer to maintain packets.

8. Performance Metrics Discussion

The assessed articles have employed the parameters for the assessment of the efficacy of each approach; these parameters are [124–127]:

(a) Detection Accuracy (DA): The number of misbehavior nodes detected; depending on the method's performance, the detection rate of misbehavior nodes will be different.

(b) Overhead: Each method has memory consumption and computational overhead. These values will be very low in high-performance methods.

(c) Throughput: The average number of packets delivered to the destination by all network nodes.

(d) Packet delivery rate: The packet delivery rate (PDR) is accomplished by splitting the total number of received packets at the intended destination by the overall quantity of packets initiated at the source for the specific purpose of transmission to a designated node.

(e) End-to-end delay: The average time for packets to reach from origin to destination in the network.

(f) Energy consumption: The energy used to send and receive packets.

(g) False alarm rate (FAR) or (FPR): Indicates the number of normal nodes designated as misbehavior nodes to the total network nodes. (The total number of the normal nodes that have been falsely detected (FP) and the number of normal nodes that have been truly detected (TP))

(h) False-positive rate (FNR): measures the percentage of normal nodes designated by selfish nodes to the overall quantity of network nodes. (The total number of the misbehavior nodes that have been falsely detected as normal (FN) and the number of normal nodes that have been truly detected (TN))

(i) Second chance: A node that once has selfish or malicious behavior is not removed from the network and allowed to cooperate with other nodes again. Table 7 shows the Notation and description of each metric.

9. Further Investigation of Attacks and Solutions Provided for Them

In the following, we have presented another table for the types of attacks and the specified solutions for each of the attacks. In this table, the type of attack is specified first, then the type of nodes, the layers involved in that attack (It is specified according to the layers of the OSI model and the opinion of the authors), and which security service is called into question when each attack occurs. The primary security services are categorized into several items, the most important of which are availability, confidentiality, authentication, data integrity and non-repudiation, and privacy. The last column of this table is dedicated to the proposed method to deal with attacks.

In Table 8, the type of attack is either selfish or malicious. If the studied paper, a specific type of attack has been solved by the method proposed by the authors, we have mentioned it in the Table 8 Otherwise, it is written as malicious, selfish, or both, and the type of attack that resolves is bolded in the description of each method.

Table 7: The notation and their description.

Notation	Description
Detection accuracy (DA)	$\mathrm{DA} = (T_p/(T_p + F_N))$
Overhead	Memory consumption and computational
Throughput	Throughput = (total number of received packet/total number of all send packet)
Packet delivery rate (PDR)	PDR = (Number of de livered packet in the Destination/total number of send packet by source)
End-to-end delay	D = (sum of time taken packet to recieve de stination/number of recieved packet)
Energy consumption	E = (Transmitted − power × packet − size/2 ∗ 10^6)
False positive rate (FPR)	FPR = (FP/TP + FP)
False negative rate (FNR)	FNR = (FN/TP + FN)
Second chance	Giving the misbehaving node another chance to operate in the network

Table 8: General summary of attacks and proposed solution.

Scheme name	Classification of attacks	Threats (attack name)	Layers involved in each attack	Security services targeted in the attack	Solution
DSAM [20]	Active, internal	Message forgery, jamming, eavesdropping, spoofing	ALL layers	Availability, data integrity	Using blockchain and CNN
System based on deep learning [21]	Active, internal	Selfish node attack	Application layer	Authentication, non-reputation	Using deep learning
DISOT [22]	Active, internal	Selfish node attack	Layer2 (sublayer MAC) to transport layer	Availability, data integrity	Using clustering and watchdog nodes
A credit-based method [23]	Active, internal	Selfish node attack	Layer2 (sublayer MAC) to transport layer	Availability, data integrity	Using watchdog nodes and majority vote
A contact-based model [24]	Active, internal	Selfish node attack	Layer2 (sublayer MAC) to transport layer	Data integrity	Using a local watchdog
Qos-OLSR [25]	Active, internal	Selfish node attack	Layer2 (sublayer MAC) to transport layer	Availability, data integrity	Using the routing protocol (QoS-OLSR) and Dempster–Shafer theory
A reputation-based model [26]	Active, internal	Selfish node attack	Layer2 (sublayer MAC) to transport layer	Data integrity	Using an ant-algorithm-based routing protocol
A Dempster–Shafer based tit-for-Tat strategy [27]	Active, internal	Selfish node attack	Layer2 (sublayer MAC) to transport layer	Data integrity	Using Dempster-Shafer theory and tit-for-tat strategy
Rashid et al. ’s model [66]	Active, internal	DDOS attack	ALL layers	Availability	Using machine learning
Bayesian based model [67]	Active, internal	Intrusion attack	Layer2 to application layer	Authentication	Designing a numerical model based on coalition game and signaling game and using Bayesian Nash equilibrium (BNE) to detect intrusion
MDFD [68]	Active, internal	Sybil attack	Layer2 (sublayer MAC) to application layer	Availability, authentication, privacy	Using machine learning

Table 8: Continued.

Scheme name	Classification of attacks	Threats (attack name)	Layers involved in each attack	Security services targeted in the attack	Solution
Awan's model [69]	Active, internal	Malicious node attack	Network layer to application layer	Privacy, data integrity	Using blockchain and trust
Fog-based DDoS detection method [70]	Active, internal	DDOS attack	ALL layers	Availability	Using nodes and fog servers to calculate the trust of each node
Signature-based authentication [71]	Active, internal	Malicious node attack	Network layer to application layer	Authentication, privacy, data integrity	Using digital signature
F-RouND [72]	Active, internal	False information attack	Application layer	Data integrity	Using beacon message and hypothesis test based on fog layer
BCSM [73]	Active, internal	False information attack, denial of service (dos)	ALL layers	Data integrity, availability	Using blockchain
EPORP-based secure protocol [74]	Active, internal	Sybil attack	Layer2 (sublayer MAC) to application layer	Availability, authentication, privacy	Using rumor riding technique and EPO algorithm
SAODV [75]	Active, internal	Black hole attack (a subset of dos attacks)	Network layer	Availability, data integrity	Improve AODV by using RSA encryption
FBTRP-DBN [76]	Active, internal	Denial of service (dos)	All layers	Availability	Using fuzzy logic and a deep belief network
TREE [77]	Active, internal	False information attack	Application layer	Data integrity	Using direct and indirect trust
BBAAS [78]	Active, internal	Replay, man-in-the-middle, No traceability and impersonation, message modification attack	Layer2 (sublayer MAC) to application layer	Availability, authentication, data integrity, privacy	Using blockchain
Fog-assisted networks based on blockchain and neuro-fuzzy [79]	Active, internal	Denial of service (dos)	All layers	Availability	Using blockchain and neuro-fuzzy based on fog-assisted
Sharma and Jaekel model [80]	Active, internal	Malicious node attack	Application layer	Authentication, non-reputation	Using machine learning techniques
Improved secure AODV [81]	Active, internal	Black hole attack (a subset of dos attacks)	Network layer	Availability, data integrity	Using encryption and reputation
CBM scheme [82]	Active, internal	Malicious node attack	Layer2 (sublayer MAC) to application layer	Authentication, availability, data integrity, non-repudiation	SVM-based vehicle classification mechanism with a Gaussian core function
ECT [83]	Active, internal	Dropping and packet modification attacks	Layer2 (sublayer MAC) to transport layer	Availability, data integrity	Calculate direct and indirect trust of each node and using the observer nodes
RBA [84]	Active, internal	Malicious node attack	Physical layer	Availability	Calculate the reputation of each node and using the observer nodes
QMM-VANET [85]	Active, internal	Malicious node attack	Physical layer	Availability	Using quality of service (QoS) protocol for clustering
TBM [86]	Active, internal	Malicious node attack	Transport layer	Availability, data integrity	Using observer nodes and assign trust to each node
A blockchain-based model [87]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using blockchain technique

Table 8: Continued.

Scheme name	Classification of attacks	Threats (attack name)	Layers involved in each attack	Security services targeted in the attack	Solution
A AODV based model [88]	Active, internal	Malicious node attack	Transport layer to application layer	Availability, data integrity	AODV routing protocol
EAAP [89]	Active, internal	Malicious node attack	Network layer to application layer	Authentication, privacy, data integrity	Using digital signature, encryption key
A game theory-based trust model [90]	Active, internal	Malicious node attack	All layers	Authentication, data integrity	Using game theory
On-demand model [91]	Active, internal	Malicious node attack	Network layer to application layer	Availability, data integrity	Location-based routing protocol
A model to detect blackhole attack [92]	Active, internal	Black hole attacks	Network layer	Availability, data integrity	Using table to store RREQ and RREP messages
FMBA [93]	Active, internal	Malicious node attack	Application layer	Authentication, non-reputation	Using fast multi-hop broadcast algorithm
Watchdog and Bayesian based model [94]	Active, internal	Malicious node attack	Transport layer	Availability, data integrity	Using a watchdog and applying a Bayesian filter
A distributed reputation based scheme [95]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Calculate trust for each node
VGKM [96]	Active, internal	Malicious node attack	Network layer to application layer	Authentication, privacy, data integrity	Using fingerprints and hash code
DMN [97]	Active, internal	Malicious node attack	Layer2 (sublayer MAC) to application layer	Availability, data integrity	Using verifiers as monitoring node
T-ACO [98]	Active, internal	Black hole attack (a subset of dos attacks)	Network layer	Availability	Using ant colony
Fox-hole region (FHR) [99]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Measuring the truth of the information
DMV [100]	Active, internal	Malicious node attack	Layer2 (sublayer MAC) to application layer	Availability, data integrity	Using clustering and verifiers as monitoring node
D&PMV [101]	Active, internal	Black hole attack (a subset of dos attacks)	Network layer	Availability, data integrity	Using clustering and verifiers as monitoring node
RAODV [102]	Active, internal	Malicious node attack	Transport layer	Availability, data integrity	Improved AODV
MDS [103]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using heartbeat messages and observer vehicle
System based on detecting cheaters [104]	Active, internal	Malicious node attack	Data link layer to application layer	Availability, authentication, data integrity	Using traffic flow theory and vehicle's signature
MBRMS [105]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using the event observers and categorizing events
RB-CD [106]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Detecting trusted relay nodes and choosing the node in the best location
VARM [107]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using data mining
Data centric detection schemes [108]	Active, internal	Selfish and malicious node attack	Application layer	Availability, authentication, data integrity	Monitoring vehicle actions and applies fines to misbehaving nodes

Table 8: Continued.

Scheme name	Classification of attacks	Threats (attack name)	Layers involved in each attack	Security services targeted in the attack	Solution
System based on machine learning [109]	Active, internal	Malicious node attack	All layers	Availability, authentication, data integrity	Using machine learning methods
Intrusion detection model [110]	Active, internal	Malicious node attack	Application layer	Authentication, non-repudiation	Using signature and trust
A system-based alert [111]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Create a degree of trust for the main messages
RCBD [112]	Active, internal	Malicious node attack	Application layer	Authentication, non-repudiation	Extract the root cause of the observed misbehavior by using cause-tree approach
Ghosh et al.'s method [113]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using the observer node and threshold value
VARS [114]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using direct and indirect reputations
Secured VANET (SV) [115]	Active, internal	Malicious node attack	Application layer	Availability, data integrity	Using fuzzy logic model
A cooperative game-based mechanism [116]	Active, internal	Selfish and malicious node attack	Transport layer	Availability, data integrity	Using game theory
Hierarchical game theory-based model [117]	Active, internal	Selfish and malicious node attack	Data link layer to application layer	Availability, data integrity	Using game theory
A trust-based approach [118]	Active, internal	Selfish and malicious node attack	Application layer	Availability, data integrity	Using reward and punishment system and RSA encryption
UAV-assisted technique [119]	Active, internal	Selfish and malicious node attack	Data link layer to application layer	Authentication, confidentiality, privacy	A trust-based method that uses clustering and drones
Credit based model [120]	Active, internal	Selfish and malicious node attack	Data link layer to application layer	Authentication, confidentiality, privacy	Using direct and an indirect trust and decision making with the help of threshold
PPS [121]	Active, internal	Selfish and malicious node attack	Data link layer to application layer	All items	Using watchdog nodes and Dempster-Shafer theory
DTM [122]	Active, internal	Selfish and malicious node attack	Data link layer to application layer	Availability, data integrity	Assign a credit for each node and pay the price for using the signal
WD-TT [123]	Active, internal	Selfish and malicious node attack	Data link layer to application layer	Availability, authentication, data integrity	Using watchdog nodes

10. The Classification of the Papers Published in Various Journals

In this study, we have reviewed different articles on detecting uncooperative nodes. Figure 10 illustrates the papers' classification in various international journals, including Springer, Elsevier, Other Journals, and IEEE. Elsevier publishes 34% of the articles, IEEE publishes 26% of the papers, Springer publishes 22% of the total paper of journals, and the remaining 18% of the papers are published in other Journals.

11. Related Open Research Issues

For years, research in the field of intelligent vehicle ad-hoc networks has attracted the attention of many researchers because having an intelligent vehicle is easy. Of course, safe driving has been a human dream. There has been a lot of research about the different types of attacks on these networks to realize this dream and have a safe network of vehicles. Of course, the authors suggested that countering specific attacks have been significant, but the network is still vulnerable to other attacks. This study reviews the

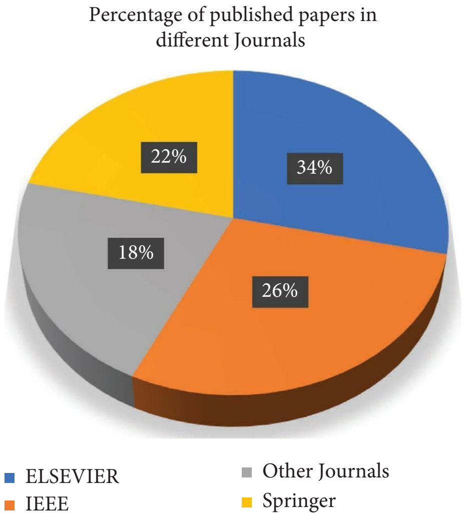

Figure 10: The percentage of the papers published among different journals.

mechanisms for detecting selfish and malicious nodes that trigger multiple attacks. Research into the discovery of misbehavior nodes still has many open issues. We will look at some of them that may become new areas of study for researchers in the future.

11.1. Having More Secure Communication Links. One area needing more research is reliable connections. The high density of vehicles in these networks can cause packet distribution storms, failure to deliver packets to vehicles on time, change of packet content, etc., which will disrupt network links. In a network where the correct reception of data is crucial due to its dependence on human life, such attacks in the communication link of its nodes are not acceptable and must be improved.

11.2. Elimination of Some Restrictions in the VANET Network, such as Low Bandwidth of Communication Links and Short Radio Range. Low bandwidth prevents packets from reaching their destination on time, and if a DDoS attack is started on the network, no packets reach their destination, and messages about redirects due to an accident or heavy fog, etc. In general, security messages don't reach the drivers. Also, the short radio range causes the packets to be transferred step by step from one node to another to reach the destination, and even if one of the intermediate nodes is selfish or malicious, it causes the packet to reach the destination either with a delay or by change, or do not reach its destination at all. This is a disaster in vehicle ad-hoc networks due to the immediate sending of vital packets.

11.3. Rapid Topology Change. Another major problem in these networks is rapid topology change because the vehicles have very high mobility. Therefore, instead of using the neighboring vehicles that are constantly moving, roadside units can be used to determine the performance of these vehicles as cooperative or uncooperative. In this way, the vehicle obtains information from its neighbors and shares it with the nearest roadside unit, and roadside units can make decisions about the performance of each vehicle. The roadside unit sends this message to all vehicles and other roadside units.

11.4. Prevention of Attacks. As mentioned earlier, in vehicle ad-hoc networks, packets should reach the vehicles in the shortest possible time, but attacks such as DDoS prevent other packets from reaching the destination immediately by sending fake packets rapidly. So, the best way to solve some attacks is not to identify and isolate these types of nodes but to prevent attacks. We propose solutions to deal with malicious and selfish nodes that include using learning algorithms. Several methods to detect selfish and malicious nodes, among which it seems that the use of machine learning-based methods such as artificial neural networks, support vector machines, and decision trees, can bring significant results for researchers to solve the problem of uncooperative nodes.

12. Conclusion

Vehicle ad-hoc networks have attracted much attention because of their potential to improve road safety and driving conditions. In this study, the authors provide a comprehensive overview of the problem of detecting misbehaving vehicles in VANETs. This is a critical problem because the effect of selfish and malicious nodes can cause significant damage to the network. In this study, we classify the types of attacks and provide explanations of the most commonly used attacks in VANETs and the various methods proposed by the authors to prevent and detect them. Tables 1–6 also examine the performance of each method. By examining various parameters, it is possible to understand what the strengths and weaknesses of each method are, for example, by examining parameters such as the percentage of detection of uncooperative nodes, overhead, throughput, etc., and Table 8 also examines which layer each attack occurs and which security service is challenged by it. It was found that no single method can detect all misbehaving nodes in VANETs. This study intends to provide valuable insights for researchers seeking to explore the realm of identification of inappropriate conduct strategies in VANETs.

Considering that there are many challenges in this field and solving these challenges will improve the efficiency of intelligent vehicles and allow drivers to drive safely, it can be said that it will provide them with many opportunities for discovery and innovation in research that can lead to significant results using new technologies such as blockchain or neural network algorithms, or even by improving parameters in a fuzzy logic or combining them.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] T. Yeferny and S. Hamad, "Vehicle ad-hoc networks: architecture, applications and challenges," 2021, https://arxiv.org/ftp/arxiv/papers/2101/2101.04539.pdf.

[2] F. Pereñiguez, J. Santa Lozano, P. J. Fernández, F. Bernal, A. F. Skarmeta, and T. Ernst, *Vehicle Ad Hoc Networks: Standards, Solutions and Research*, Springer, Berlin, Germany, 2015.

[3] A. Rahim, X. Kong, F. Xia et al., "Vehicular social networks: a survey," *Pervasive and Mobile Computing*, vol. 43, pp. 96–113, 2018.

[4] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," *Cluster Computing*, vol. 24, no. 2, pp. 1235–1253, 2021.

[5] A. L. Beylot and H. Labiod, *Vehicle Networks: Models and Algorithms*, John Wiley and Sons, Hoboken, NJ, USA, 2013.

[6] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proceedings of the 2013 4th International Conference on Computing Communications and Networking Technologies (ICCCNT)*, Hoboken, NJ, USA, July, 2013.

[7] R. Riebl, M. Monz, S. Varga et al., "Improved security performance for vanet simulations," *IFAC-PapersOnLine*, vol. 49, no. 30, pp. 233–238, 2016.

[8] D. Singh, S. Narayanan, M. F. I. L. Abdullah, and B. Vicknasingam, "IBMDA: information based misbehavior detection algorithm for VANET," *Journal of Ethnicity in Substance Abuse*, vol. 9, pp. 1–11, 2020.

[9] S. Hao, H. Zhang, and M. Song, "A stable and energy-efficient routing algorithm based on learning automata theory for MANET," *Journal of Communications and Information Networks*, vol. 3, no. 2, pp. 52–66, 2018.

[10] U. D. Prasan and S. Murugappan, "An analysis on vehicle ad-hoc networks: research issues, challenges and applications," *International Journal of Applied Engineering Research*, vol. 11, no. 6, pp. 4569–4575, 2016.

[11] D. Singh and M. Kaur, "Mitigation of Sybil attack using location aware nodes in VANET," *International Journal of Science and Research*, vol. 4, no. 11, 2015.

[12] N. Bißmeyer, "Misbehavior detection and attacker identification in vehicle ad-hoc networks," Doctoral Dissertation, Technische Universität, Berlin, Germany, 2014.

[13] Z. Ullah, M. S. Khan, I. Ahmed, N. Javaid, and M. I. Khan, "Fuzzy-based trust model for detection of selfish nodes in MANETs," in *Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 965–972, IEEE, Crans-Montana, Switzerland, March 2016.

[14] S. Dubey and N. Tripathi, "A survey on intrusion detection systems," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 1, pp. 29–40, 2015.

[15] B. M. Silva, J. J. Rodrigues, N. Kumar, and G. Han, "Cooperative strategies for challenged networks and applications: a survey," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2749–2760, 2017.

[16] S. Goli-Bidgoli and N. Movahhedinia, "Determining vehicles' radio transmission range for increasing cognitive radio VANET (CR-VANET) reliability using a trust management system," *Computer Networks*, vol. 127, pp. 340–351, 2017.

[17] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, "VANET security and privacy-an overview," *International journal of Network Security and Its Applications*, vol. 10, 2018.

[18] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[19] R. Sultana, J. Grover, and M. Tripathi, "A novel framework for misbehavior detection in SDN-based vanet," in *Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, Crans-Montana, Switzerland, December 2020.

[20] B. Zhang, X. Wang, R. Xie, C. Li, H. Zhang, and F. Jiang, "A reputation mechanism based Deep Reinforcement Learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network," *Future Generation Computer Systems*, vol. 139, pp. 17–28, 2023.

[21] N. Jyothi and R. Patil, "An optimized deep learning-based trust mechanism in VANET for selfish node detection," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 3, pp. 304–318, 2021.

[22] S. Nobahary, H. Gharaee Garakani, A. Khademzadeh, and A. M. Rahmani, "DISOT: distributed selfish node detection in internet of things," *International Journal of Information & Communication Technology Research*, vol. 10, no. 3, pp. 19–30, 2018.

[23] S. Nobahary and S. Babaie, "A credit-based method to selfish node detection in mobile ad-hoc network," *Applied Computer Systems*, vol. 23, no. 2, pp. 118–127, 2018.

[24] V. Vidhya and S. Ramkumar, "A survey of techniques used to detect the selfish nodes in vanet," *International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)*, vol. 2, no. 11, 2016.

[25] O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles," *Computer Communications*, vol. 41, pp. 43–54, 2014.

[26] Q. Ding, X. Li, M. Jiang, and X. Zhou, "A novel reputation management framework for Vehicle Ad Hoc Networks,"

International Journal of Multimedia Technology, vol. 3, no. 2, pp. 62–66, 2013.

[27] O. A. Wahab, H. Otrok, and A. Mourad, "A dempster–shafer based tit-for-tat strategy to regulate the cooperation in vanet using qos-olsr protocol," *Wireless Personal Communications*, vol. 75, no. 3, pp. 1635–1667, 2014.

[28] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, "Vehicle ad-hoc network (VANET)," in *Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, pp. 1–6, IEEE, New York, NY, USA, May 2018.

[29] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515–1555, 2021.

[30] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: a trust-based framework for reliable data delivery and DoS defense in VANETs," *Vehicular Communications*, vol. 9, pp. 254–267, 2017.

[31] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PLoS One*, vol. 15, no. 2, Article ID e0228319, 2020.

[32] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: an adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[33] C. Lai, J. E. Karp, C. S. Hourigan, H. Li, and X. Shen, "SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs," *Expert Review of Hematology*, vol. 9, no. 1, pp. 1–3, 2016.

[34] A. Ghaffari and S. Nobahary, "FDMG: fault detection method by using genetic algorithm in clustered wireless sensor networks," *Journal of AI and Data Mining*, vol. 3, no. 1, pp. 47–57, 2015.

[35] S. Nobahary, H. Gharaee Garakani, and A. Khademzadeh, "Detecting noncooperation nodes mechanisms in wireless networks: a survey," *Security and Communication Networks*, vol. 2022, Article ID 6486816, 20 pages, 2022.

[36] S. Babaie, N. Zekrizadeh, and S. Nobahary, *A Survey: Wireless Sensor Network Attacks and Countermeasures*, Springer, Berlin, Germany, 2009.

[37] T. Zaidi and S. Faisal, "An overview: various attacks in VANET," in *Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA)*, pp. 1–6, IEEE, Greater Noida, India, December 2018.

[38] M. Azees, P. Vijayakumar, and L. Jegatha Deborah, "Comprehensive survey on security services in vehicular *ad-hoc* networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[39] A. Ilavendhan and K. Saruladha, "Comparative analysis of various approaches for DoS attack detection in VANETs," in *Proceedings of the 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 821–825, IEEE, Coimbatore, India, July 2020.

[40] B. Parno and A. Perrig, "Challenges in securing vehicle networks," in *Workshop on Hot Topics in Networks (HotNets-IV)*, Springer, Berlin, Germany, 2005.

[41] C. Guleria and H. K. Verma, "Improved detection and mitigation of ddos attack in vehicle ad hoc network," in *Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA)*, pp. 1–4, IEEE, Greater Noida, India, December 2018.

[42] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Security and Privacy*, vol. 1, no. 5, p. e39, 2018.

[43] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicle ad hoc networks (vanets)," in *Proceedings of the 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*, pp. 394–398, IEEE, Shanghai, China, September 2020.

[44] M. A. Mastouri and S. Hasnaoui, "effect of the black-hole attack in vehicle ad-hoc networks," in *Proceedings of the 2021 26th IEEE Asia-Pacific Conference on Communications (APCC)*, pp. 205–210, IEEE, Kuala Lumpur, Malaysia, October 2021.

[45] S. Ali, P. Nand, and S. Tiwari, "Detection of wormhole attack in vehicle ad-hoc network over real map using machine learning approach with preventive scheme," *Journal of Information Technology Management*, vol. 14, pp. 159–179, 2022.

[46] G. Kaur, M. Khurana, and A. Kaur, *Gray Hole Attack Detection and Prevention System in Vehicle Ad-Hoc Network (VANET)*, EasyChair, Amsterdam, the Netherlands, 2021.

[47] T. Pavithra and B. S. Nagabhushana, "A survey on security in VANETs," in *Proceedings of the 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 881–889, IEEE, Coimbatore, India, July 2020.

[48] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol. 13, pp. 56–63, 2018.

[49] S. Gurusubramani, S. Subhashini, K. Venusamy, V. Nagaraju, and K. Thaiyalnayaki, "An efficient timing attack management in VANETs using Monte Carlo Markov chain sampling," *Journal of Green Engineering*, vol. 10, pp. 8813–8824, 2020.

[50] D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in VANET," in *Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–8, IEEE, Kanpur, India, July 2019.

[51] S. S. Sefati and S. G. Tabrizi, "Detecting Sybil attack in vehicular ad-hoc networks (vanets) by using fitness function, signal strength index and throughput," *Wireless Personal Communications*, vol. 123, no. 3, pp. 2699–2719, 2022.

[52] M. M. Hamdi, L. Audah, M. S. Abood et al., "A review on various security attacks in vehicular ad hoc networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2627–2635, 2021.

[53] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[54] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, 2018.

[55] X. Xu, Y. Wang, and P. Wang, "Comprehensive review on misbehavior detection for vehicular ad hoc networks," *Journal of Advanced Transportation*, vol. 2022, Article ID 4725805, 27 pages, 2022.

[56] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing:

a survey," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 5129620, 25 pages, 2020.

[57] D. Singh, N. Ranvijay, and R. S. Yadav, "A state-of-art approach to misbehaviour detection and revocation in VANET: survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 28, no. 2, pp. 77–93, 2018.

[58] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 779–811, 2019.

[59] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 62–17, 2018.

[60] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[61] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[62] D. Shukla, A. Vaibhav, S. Das, and P. Johri, "Security and attack analysis for vehicle ad hoc network—a survey," in *Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 625–630, IEEE, New Delhi, India, April 2016.

[63] U. Khan, S. Agrawal, and S. Silakari, "A detailed survey on misbehavior node detection techniques in vehicle ad hoc networks," in *Information Systems Design and Intelligent Applications*, pp. 11–19, Springer, Berlin, Germany, 2015.

[64] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[65] M. Erritali and B. El Ouahidi, "A survey on VANET intrusion detection systems," in *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics*, pp. 16–19, Singapore, April 2013.

[66] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, 2023.

[67] A. Mabrouk and A. Naja, "Intrusion detection game for ubiquitous security in vehicular networks: a signaling game based approach," *Computer Networks*, vol. 225, Article ID 109649, 2023.

[68] Y. Chen, Y. Lai, Z. Zhang, H. Li, and Y. Wang, "MDFD: a multi-source data fusion detection framework for Sybil attack detection in VANETs," *Computer Networks*, vol. 224, Article ID 109608, 2023.

[69] K. A. Awan, I. U. Din, and A. Almogren, "A blockchain-assisted trusted clustering mechanism for IoT-enabled smart transportation system," *Sustainability*, vol. 14, no. 22, Article ID 14889, 2022.

[70] A. Gaurav, B. B. Gupta, F. J. G. Peñalvo, N. Nedjah, and K. Psannis, "Ddos attack detection in vehicle ad-hoc network (vanet) for 5g networks," in *Security and Privacy Preserving for IoT and 5G Networks*, pp. 263–278, Springer, Cham, Switzerland, 2022.

[71] A. S. Rajasekaran and M. Islam Satti, "An anonymous signature-based authentication and key agreement scheme for vehicle ad hoc networks," *Security and Communication Networks*, vol. 2022, Article ID 1222660, 9 pages, 2022.

[72] A. Paranjothi and M. Atiquzzaman, "A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing," *Digital Communications and Networks*, vol. 8, no. 5, pp. 814–824, 2022.

[73] G. Liu, N. Fan, C. Q. Wu, and X. Zou, "On a blockchain-based security scheme for defense against malicious nodes in vehicular ad-hoc networks," *Sensors*, vol. 22, no. 14, p. 5361, 2022.

[74] N. C. Velayudhan, A. Anitha, and M. Madanan, "Sybil attack with RSU detection and location privacy in urban VANETs: an efficient EPORP technique," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3573–3601, 2022.

[75] R. K. Dhanaraj, S. H. Islam, and V. Rajasekar, "A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments," *Wireless Networks*, vol. 28, no. 7, pp. 3127–3142, 2022.

[76] K. N. Tripathi, A. M. Yadav, and S. C. Sharma, "Fuzzy and deep belief network based malicious vehicle identification and trust recommendation framework in VANETs," *Wireless Personal Communications*, vol. 124, no. 3, pp. 2475–2504, 2022.

[77] K. N. Tripathi, A. M. Yadav, and S. C. Sharma, "TREE: trust-based authenticated and secure dissemination of emergency event information for the network of connected vehicles," *Arabian Journal for Science and Engineering*, vol. 47, no. 8, pp. 10689–10717, 2022.

[78] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Security and Communication Networks*, vol. 2021, Article ID 6679882, 11 pages, 2021.

[79] S. O. Ogundoyin and I. A. Kamil, "An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy," *Vehicular Communications*, vol. 31, Article ID 100384, 2021.

[80] A. Sharma and A. Jaekel, "Machine learning approach for detecting location spoofing in VANET," in *Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–6, IEEE, Manchester Metropolitan University, UK, July 2021.

[81] A. Kumar, V. Varadarajan, A. Kumar et al., "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, Article ID 103352, 2021.

[82] S. Sultan, Q. Javaid, A. J. Malik, F. Al-Turjman, and M. Attique, "Collaborative-trust approach toward malicious node detection in vehicle ad hoc networks," *Environment, Development and Sustainability*, vol. 8, pp. 1–19, 2021.

[83] K. N. Tripathi, G. Jain, A. M. Yadav, and S. C. Sharma, "Entity-centric combined trust (ECT) algorithm to detect packet dropping attack in vehicular Ad Hoc networks (VANETs). In Next Generation Information Processing System," *Proceedings of ICCET*, vol. 2, pp. 23–33, 2021.

[84] K. N. Tripathi, S. C. Sharma, and G. Jain, "A new reputation-based algorithm (RBA) to detect malicious nodes in vehicular Ad Hoc networks (VANETs)," in *Soft Computing: Theories and Applications: Proceedings of SoCTA*, pp. 395–404, Springer, Singapore, 2020.

[85] H. Fatemidokht and M. Kuchaki Rafsanjani, "QMM-VANET: an efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," *Journal of Systems and Software*, vol. 165, Article ID 110561, 2020.

[86] K. N. Tripathi and S. C. Sharma, "A trust based model (TBM) to detect rogue nodes in vehicle ad-hoc networks (VANETS)," *International Journal of System Assurance Engineering and Management*, vol. 9, pp. 1–15, 2019.

[87] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[88] T. Zaidi, S. Giri, S. Chaurasia, P. Srivastava, and R. Kapoor, "Malicious node detection through aodv in vanet," *International Journal of Ad hoc, Sensor and Ubiquitous Computing (IJASUC)*, vol. 9, no. 2, pp. 33–43, 2018.

[89] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[90] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for Vehicular Ad hoc Networks (VANETs)," *Computer Networks*, vol. 121, pp. 152–172, 2017.

[91] Y. H. Ho, C. H. Lin, and L. J. Chen, "On-demand misbehavior detection for vehicle ad hoc network," *International Journal of Distributed Sensor Networks*, vol. 12, no. 10, Article ID 1550147716673928, 2016.

[92] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 133–139, 2017.

[93] W. Ben Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "The impact of malicious nodes positioning on vehicular alert messaging system," *Ad Hoc Networks*, vol. 52, pp. 3–16, 2016.

[94] J. Rupareliya, S. Vithlani, and C. Gohel, "Securing VANET by preventing attacker node using watchdog and Bayesian network theory," *Procedia Computer Science*, vol. 79, pp. 649–656, 2016.

[95] J. Oluoch, "A distributed reputation scheme for situation awareness in vehicle ad hoc networks (VANETs)," in *Proceedings of the 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 63–67, IEEE, New York, NY, USA, March 2016.

[96] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[97] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," *Procedia Computer Science*, vol. 46, pp. 965–972, 2015.

[98] K. Npatel and R. Hjhaveri, "Isolating packet dropping misbehavior in VANET using ant colony optimization," *International Journal of Computer Application*, vol. 120, no. 24, pp. 5–9, 2015.

[99] S. K. Harit, G. Singh, and N. Tyagi, "Fox-hole model for data-centric misbehaviour detection in vanets," in *Proceedings of the 2012 3rd International Conference on Computer and Communication Technology (ICCCT)*, pp. 271–277, IEEE, Massachusetts, MA, USA, November 2012.

[100] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 325–338, 2013.

[101] M. Kadam and S. Limkar, "D&PMV: new approach for detection and prevention of misbehave/malicious vehicles from VANET," in *Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013*, pp. 293–303, Springer, Cham, Switzerland, 2014.

[102] V. L. Praba and A. Ranichitra, "Detecting malicious vehicle in a VANET scenario by incorporating security in AODV protocol," *ICTACT Journal on Communication Technology*, vol. 3, no. 3, pp. 594–598, 2012.

[103] R. P. Barnwal and S. K. Ghosh, "Heartbeat message based misbehavior detection scheme for vehicle ad-hoc networks," in *Proceedings of the 2012 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 29–34, IEEE, Beijing, China, December 2012.

[104] D. Huang, S. A. Williams, and S. Shere, "Cheater detection in vehicle networks," in *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 193–200, IEEE, Liverpool, UK, June 2012.

[105] C. H. Kim and I. H. Bae, "A misbehavior-based reputation management system for vanets," in *Embedded and Multimedia Computing Technology and Service*, Springer, Berlin, Germany, 2012.

[106] H. Yoo and D. Kim, "Repetition-based cooperative broadcasting for vehicular ad-hoc networks," *Computer Communications*, vol. 34, no. 15, pp. 1870–1882, 2011.

[107] J. Rezgui and S. Cherkaoui, "Detecting faulty and malicious vehicles using rule-based communications data mining," in *Proceedings of the 2011 IEEE 36th Conference on Local Computer Networks (LCN)*, pp. 827–834, IEEE, Bonn, Germany, October 2011.

[108] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "on data-centric misbehavior detection in VANETs," in *Proceedings of the 2011 IEEE Vehicle Technology Conference (VTC Fall)*, pp. 1–5, IEEE, New York, NY, USA, September 2011.

[109] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in VANET," in *International Conference on Advances in Computing and Communications*, pp. 644–653, Springer, Berlin, Heidelberg, 2011.

[110] N. Bißmeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in *Proceedings of the 2010 IEEE Vehicle Networking Conference (VNC)*, pp. 166–173, IEEE, Jersey City, NJ, USA, December 2010.

[111] A. Vulimiri, A. Gupta, P. Roy, S. N. Muthaiah, and A. A. Kherani, "Application of secondary information for misbehavior detection in VANETs," in *International Conference on Research in Networking*, pp. 385–396, Springer, Berlin, Heidelberg, 2010.

[112] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," *Ad Hoc Networks*, vol. 8, no. 7, pp. 778–790, 2010.

[113] M. Ghosh, A. Varghese, A. A. Kherani, and A. Gupta, "Distributed misbehavior detection in VANETs," in *Proceedings of the WireLow Communications and Networking Conference WCNC 2009*, pp. 1–6, IEEE, New York, NY, USA, April 2009.

[114] F. Dotzer, L. Fischer, and P. Magiera, "Vars: a vehicle ad-hoc network reputation system," in *Proceedings of the WoWMoM 2005 6th IEEE International Symposium on a World of*

WireLow Mobile and Multimedia Networks, pp. 454–456, IEEE, Belfast, UK, June 2005.

[115] M. Alkhalidy, A. F. Al-Serhan, A. Alsarhan, and B. Igried, "A new scheme for detecting malicious nodes in vehicular ad hoc networks based on monitoring node behavior," *Future Internet*, vol. 14, no. 8, p. 223, 2022.

[116] A. Mabrouk, A. Naja, O. A. Oualhaj, A. Kobbane, and M. Boulmalf, "A cooperative game based mechanism for autonomous organization and ubiquitous connectivity in VANETs," *Simulation Modelling Practice and Theory*, vol. 107, Article ID 102213, 2021.

[117] S. Nobahary, H. G. Garakani, A. Khademzadeh, and A. M. Rahmani, "Selfish node detection based on hierarchical game theory in IoT," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 255–319, 2019.

[118] A. Zouinkhi, A. Ltifi, C. Chouaib, and M. N. Abdelkrim, "A trust management based on a cooperative scheme in VANET," *International Journal of Information and Communication Technology*, vol. 13, no. 3, pp. 291–304, 2018.

[119] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Vehicular Communications*, vol. 11, pp. 1–11, 2018.

[120] C. A. Kerrache, A. Lakas, and N. Lagraa, "Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control," in *Proceedings of the 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, pp. 1–4, IEEE, Ras Al Khaimah, Saudi Arabia, December 2016.

[121] A. Jesudoss, S. Kasmir Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme," *Ad Hoc Networks*, vol. 24, pp. 250–263, 2015.

[122] N. Haddadou and A. Rachedi, "DTM: adapting job market signaling for distributed trust management in vehicle ad hoc networks," in *Proceedings of the 2013 IEEE International Conference on Communications (ICC)*, pp. 1827–1832, IEEE, Budapest, Hungary, June 2013.

[123] Z. Wang and C. Chigan, "Cooperation enhancement for message transmission in VANETs," *Wireless Personal Communications*, vol. 43, no. 1, pp. 141–156, 2007.

[124] A. Ghaffari, "Vulnerability and security of mobile ad hoc networks," in *Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization*, pp. 124–129, Istanbul, Turkey, September 2006.

[125] P. Mohammadi and A. Ghaffari, "Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis," *Wireless Personal Communications*, vol. 106, no. 2, pp. 365–376, 2019.

[126] A. Nobahari and S. J. Mirabedini, "DSVL: detecting selfish node in vehicle ad-hoc networks (VANET) by learning automata," *Ad Hoc & Sensor Wireless Networks*, vol. 53, no. 1-2, pp. 1–27, 2022.

[127] A. Akhbari and A. Ghaffari, "Selfish node detection based on fuzzy logic and Harris hawks optimization algorithm in IoT networks," *Security and Communication Networks*, vol. 2021, Article ID 2658272, 20 pages, 2021.