Hindawi
Journal of Advanced Transportation
Volume 2022, Article ID 4725805, 27 pages
https://doi.org/10.1155/2022/4725805

Review Article

Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks

Xiaoya Xu,[1] **Yunpeng Wang**,[1] **and Pengcheng Wang**[2]

[1]*School of Transportation Science and Engineer, Beihang University, Beijing 100191, China*
[2]*School of Cyber Science and Technology, Beihang University, Beijing 100191, China*

Correspondence should be addressed to Pengcheng Wang; kdwpc@126.com

Received 10 January 2022; Revised 10 March 2022; Accepted 16 March 2022; Published 8 April 2022

Academic Editor: Zhenzhou Yuan

Vehicular ad hoc networks (VANETs) can increase road safety and comfort. It needs strong demand for security because the data sent in VANETs influence vehicles' behavior. Existing studies have summarized VANET security, challenge, and attacks. This study aims to present a comprehensive overview of misbehavior detection in VANETs. First, VANET characteristics, security issues, and attacks are discussed. Then, the precise definition of misbehavior, detection mode, and detection objects are presented. Generic misbehavior detection is classified as data-centric and node-centric. In this study, to adapt to the VANETs scenario, we proposed a novel taxonomy of misbehavior detection, which considers the interaction between vehicles and which is refined by emphasizing the detection modes and participants. Finally, the remaining concerns, open issues, and prospective future research directions are discussed.

1. Introduction

The vehicular ad hoc network (VANET), as a type of mobile ad hoc network (MANET), enables the communication between vehicles (V2V) and between vehicles and infrastructure (V2I) [1]. With the advancement of telecommunication, vehicular communication promotes the deployment of high-definition maps, intelligent transportation applications, autonomous driving, and coordinated driving [2]. At the same time, it also highlights VANETs' main characteristics, including self-organization, decentralized networking, and a highly dynamic topology [3]. These communication characteristics bring considerable differences in terms of security and safety requirements and challenges from traditional networks [4, 5]. Exchange messages are rarely encrypted in vehicular communication networks, including basic messages, such as navigation, traffic safety messages, and event-oriented messages [6]. Hence, the open environment of VANETs may lead to various attacks such as forgery, denial-of-service (DoS), and false reports, and then result in traffic chaos or accident [7–9]. Furthermore, malevolent entities may track participants' messages and identities, posing a substantial hazard to drivers. Therefore, for VANETs, from the security-preserving aspect, malicious vehicles should be traced and penalized in the event of any misbehavior [10, 11].

Dealing with security issues in VANETs, most surveys mainly reviewed cryptography-based solutions to address security and privacy challenges in VANETs [12–14]. Security solutions generally fall into identity-based cryptography (IBC) and public key infrastructure (PKI)-based cryptography. In identity-based techniques [5, 15, 16], ID is used as the public key, and the related private key is generated by a third-party key generator center (KGC). IBC scheme has key-escrow and malicious KGC problems. PKI is recognized in VANET as more practical than IBC alternatives. PKI-based techniques [17–20] have been proposed to authenticate vehicular messages using digital certificates. The influential international organizations, the Institute of Electrical and Electronics Engineers (IEEE) and European Telecommunications Standards Institute (ETSI), created and standardized the vehicular PKI system to keep the safe operation of VANET safety applications. A digital certificate and a valid signature can certify the authorized identity of

the participant and the validity, integrity, and nonrepudiation of the vehicular message.

Despite the security protections given by the PKI infrastructure, the existing VANET system still has security issues. For example, a malicious node in VANET has a valid certificate to certify its authorization and is according to the protocol but sends inaccurate or false data in the vehicular network. That means securing the system from the inside attackers is difficult. Threatening behavior and false information from an insider, which means misbehaviors, cannot be prevented by the existing system and may cause a very negative impact on the surrounding vehicle nodes and the overall system environment. Therefore, misbehavior detection has been proposed as a mitigation technique against various attacks in the above situation.

Although a well-researched topic, many unclear research domains still exist in misbehavior detection. Some survey works are limited in a restricted scenario. For example, a study focused on intrusion detection systems (IDSs) with malicious misbehavior. However, the schemes mentioned are around signature-based IDS using preknown attack scenarios and packet traffic analysis [21]. Some works are concentrated on individual technology for misbehavior detection, i.e., machine learning. Due to the novelty and uniqueness of vehicular networks, it is hard to cover the whole vehicular network or the Internet of Vehicle [22, 23]. Some studies focused on solutions to various attacks that may occur in VANETs instead of giving a framework of detection mechanism [24, 25].

To fill this gap, this study aims to provide a systematic investigation of misbehavior detection in VANETs with a novel taxonomy of detection mechanisms refined by considering the interaction of vehicles. As the fundamental basis of misbehavior detection analysis, current deployments, security attributes, and security issues have been discussed first. Then, a more precise definition of misbehavior, detection mode, and detection objects is provided. In most research, misbehavior detection is primarily classified as data-centric and node-centric [26–28]. Based on previous work, we further refined node-centric and data-centric detection into two branches: autonomous and collaborative. The refined approach draws on the detection mode, mathematical model, and method.

The rest of this study is structured as follows. Section 2 discusses the overview of VANETs, security attributes, challenges, and attacks. Section 3 presents the definition, the attacker model, and the detection mode of misbehaviors for VANET. Section 4 discusses the state-of-the-art detection mechanisms based on their feasibility, followed by a summary, including open issues and future directions.

2. System Model, Security, and Challenges in Vanets

VANETs are a form of MANET connecting vehicles to infrastructures [29, 30], which have several benefits in reducing road accidents, providing a more comfortable and pleasurable driving experience, and facilitating automobile parking [31]. It aims to share information and increase efficient communication between vehicles. Vehicles in VANET can share traffic flow parameters, driver behavior, and driving conditions within their vicinity by using wireless communication technologies [32]. Moreover, VANETs are more susceptible to various assaults and face more security challenges because it is an open-access environment with numerous participants and various data sources.

2.1. System Model. The VANET's architecture comprises OBU, roadside unit (RSU), and trusted authority (TA). Vehicles in VANETs are equipped with an OBU, which serves as a router and a terminal node. The RSU is stationed along the roadway to monitor network node behavior [33]. The TA is responsible for registering the RSU and the OBU in VANETs, which are utilized to maintain and operate the network system. VANETs have developed the V2X (vehicle-to-everything) communication concept (see Figure 1 for a VANET overview). V2X communications enable vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian, and vehicle-to-cloud connections, which can either use DSRC, LTE, 4G, or 5G. It could be accomplished via the employment of either an IEEE 802.11p-based technology (running at the 5.9 GHz frequency) or a long-term evolution (LTE)-based technology [2]. The network's entities could connect directly (e.g., through 802.11p-based technologies or LTE-PC5/sidelink interface) or indirectly via the LTE-Uu interface (uplink and downlink).

V2X communication technology is projected to increase traffic efficiency by minimizing collisions and conserving resources by various security applications [27, 28]. Typical V2X application use cases include the following: road safety (e.g., traffic jam/incident reporting, collision warning, and collision avoidance), cooperative autonomous driving, and infotainment services (e.g., traffic information services).

The communication information in VANETs is composed of two types of messages: beacon and safety messages. Beacon messages are a kind of periodic data that indicates the presence of a vehicle inside a network. They provide the vehicle's location, the sender's identification, the vehicle's speed, and the time. When a safety event occurs, safety messages are sent indicating the location of the occurrence [27]. To promote V2X communication deployment, V2X messages have been further defined to include basic safety messages (BSMs), cooperative awareness messages (CAMs) [34], and decentralized environmental notification messages (DENMs) [35]. BSM carries information on the transmitting vehicle, such as its position, dynamics, and status. The default portion is cyclical (sent at a rate maximum rate of 10 Hz). The other half is triggered by events (e.g., emergency braking and traffic bottlenecks) [36]. Periodic broadcasting also describes CAM [34] and event-driven DENM [35]. Event-driven BSM messages are appropriate for usage in local neighborhoods (e.g., single-hop broadcast). Moreover, DENMs may be used to specify particular geographical regions (e.g., multiple hops' geo-cast).

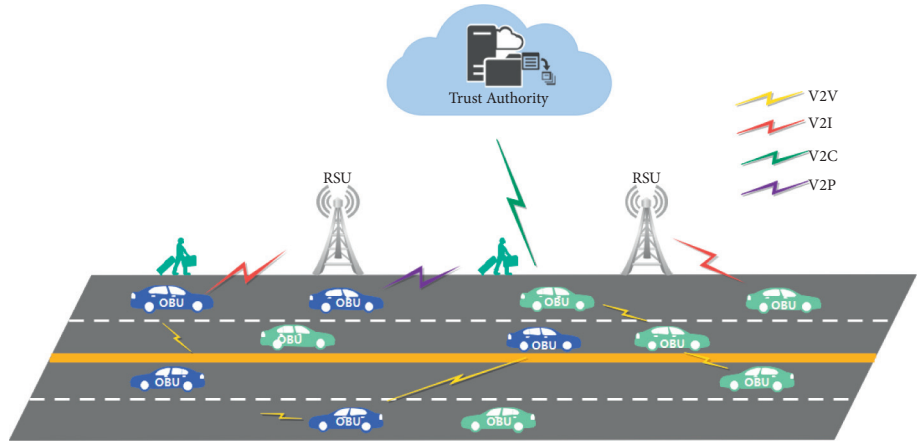

Figure 1: Attacks with corresponding Internet protocol stack layers.

2.2. VANET Characteristics. Compared with MANETs, VANETs exhibit greater mobility and frequent topology changes. During the 2010–2020 decade, the characteristics of VANETs investigated in [1, 37–46] could be generally divided into two categories. One of them is network and communication, and another is participants, including vehicles and drivers [37]. The characteristics of VANETs are as follows:

(1) VANET characteristics related to network and communication are

(a) High mobility
One of the main features of the VANET's protocol is its great mobility. In a VANET, the node travels at a fast rate, resulting in a compacted network mesh. The network's communication time is cut in half due to node mobility [43, 47], and calculating the vehicles' location is complex.

(b) Unbounded network
VANET is an unbounded, scalable network that may connect one or more cities or even whole nations. As a result, security needs necessitate collaboration and supervision.

(c) Dynamic changing network topology
Nodes are highly mobile, and vehicle speeds should be unpredictable. Node positions vary often. As a result, the topology of VANETs is fluid and unpredictably changing. This feature makes VANETs more vulnerable to assaults.

(d) Frequent network reconnection
According to the high-speed vehicle movement and other objective factors such as weather conditions, VANETs are frequently disconnected. Recurrent disconnection might also be caused by a substantial number of cars on the road, which may lead to substantial reconnection in the traffic environment.

(e) Transmission medium
In VANETs, the transmission medium is wireless. The global availability of this wireless transmission medium is a great benefit in IVC. However, several security issues depend on the nature of transmission and communication security when using open support.

(f) Information exchange frequency
VANET motivates the nodes to gather nearby automobiles and RSU data. As a result, the nodes communicate information regularly.

(g) Resource-constrained environment
In VANETs, transmission power and bandwidth are limited [48]. Transmission power is limited in the wireless access of vehicular environment (WAVE), ranging from 0 dBm to 28.8 dBm, with coverage distances ranging from 10 m to 1 km. As a result, restricted power transfer may affect VANET coverage distance [49]. The conventional DSRC band in VANET is considered limited: the DSRC bandwidth is 27 MHZ, and the throughput is 27 Mbps.

(h) Attenuations
DSRC wireless communication's performance has a constraint linked with the digital transmission with such frequency bands because of diffraction, reflection, dispersion, refraction, scattering, and various forms of fading and Doppler Effect losses [50]. That situation also leads to propagation delays.

(2) VANET Characteristics Related to Participants (Vehicles and Drivers)

(a) High processing power and sufficient energy
No issues with energy, computation capacity, or storage failure in VANET nodes are observed. They have their battery power supply and remarkable computing capabilities for executing complex cryptographic calculations such as RSA and ECDSA while providing infinite transmission power.

(b) Better physical security
VANET nodes are now more physically secure and physically protected. As a result, physically compromising a VANET node will be challenging.

(c) Low latency and accurate location
The transmitting information in VANET has a high demand for time, which must be sent to the correct node within the specified time frame to make a judgment and take appropriate action. Many applications rely on location and geographic addressing or area. Hence, the global positioning system (GPS) is a standard equipment in most automobiles, providing location-based service (LBS).

(d) Trustworthy
The majority of drivers are regarded as reliable and helpful in discovering malicious attackers. Meanwhile, vehicle registration, maintenance, and inspection must be registered with a TA and given a unique identifying number (license plate) that effectively regulars the behavior of most participants.

In summary, the vehicular network is the outcome of interactions between driver behavior, network, and infrastructure that not only promotes development but also brings security risks. Next to introducing VANET characteristics, the following section discusses VANET security issues and potential attacks.

2.3. Security Issues in VANETs. The confidentiality, integrity, and availability (CIA) method is a typical approach to security categorization, which has been used in conventional networks [14, 43, 51]. The CIA dimension and other dimensions such as authentication, identity, and nonrepudiation are used to categorize typical security vulnerabilities in ITS.

(i) Availability

Availability is critical to the security of VANET [52]. Compared with other security services, availability is more prone to harmful attacks. The most common assaults on the availability of VANET components and services are denial-of-service attacks [1]. As a result, VANETs may be protected from these attacks using trust-based and cryptography measures.

(ii) Confidentiality

Confidentiality is one of the critical security attributes that VANET must consider while dealing with sensitive information in the vehicular network. Confidentiality allows VANET devices and parties to interact safely and privately without providing information to uninvolved parties while preventing other parties and possible adversaries from listening in on the conversation [14].

(iii) Integrity

In VANET, a hostile car may attack by intercepting and changing communications messages between two vehicles before sending the messages to other vehicles. This form of assault has been researched in [53], but it is still a widespread problem in VANETs. PKI and cryptography solutions are helpful in this issue [54]. Data integrity guarantees that the content of the message is not changed or altered during transmission.

(iv) Authentication and identification

Authenticating and identifying play a vital role in ensuring the VANET by preventing them from malicious entities in the network [14]. Most VANET authentication and identification research has shifted to the concept of using pseudonyms instead of vehicle identities to enable more anonymity [53, 55, 56]. Employing pseudonyms demands more cost and computation when processing safety messages because the receiver needs to verify the sender's identification. Moreover, TA must first confirm a batch of pseudonyms when multiple cars send messages to TA simultaneously.

(v) Nonrepudiation

Nonrepudiation assures that the transmitting and receiving entities cannot deny the transmission and the receipt. Nonrepudiation prevents the deniability of harmful acts by members of the system. Notably, it focuses on the study of VANETs and V2V communications. Most nonrepudiation research [57–59] relies on a trusted third party to confirm the real-world identity.

2.4. Attacks on VANETs. With the spread of VANETs, that new security concerns against these highly mobile yet predictable networks exploited is quite probable. Attacks seek to disrupt the qualities of confidentiality, integrity, availability, identity, authentication, and nonrepudiation because of the variety of technologies and devices that make up VANET. While several attacks are derivatives of previous MANET-based assaults, several are unique to VANETs. Compared to the security issues listed in the previous section, existing attacks on VANETs are grouped according to their objectives and targets. First, different security threats in VANETs are compared by considering criteria such as attack kinds, impact area, and security properties, and categorizing each possible attack as active or passive, as shown in Table 1.

2.5. Attacks on Availability. Attacks on availability are a critical component of the VANET system, as a lack of availability functionality may drop the efficiency of information accessibility. Several attacks may destroy the availability of VANET.

(1) DoS attack

One of the most common VANET attacks is DoS, which tries to disable a system's legitimate operations. It attacks the VANET network by submitting excessive requests for the system [60]. The attacker blocks the vehicle's connection, hindering any action. For example, to interrupt communication between cars and RSUs, an attacker might attempt to disable the RSUs' network in VANETs. Many

Table 1: Category of various attacks in VANET.

Security Attributes	Attacks	Impact area	Attacker activeness
Availability	Denial-of-service attack	Application	Active
	Jamming attack	Application	Active
	Blackhole attack	Application	Active
	Gray hole attack	Application	Active
	Greedy behavior attack	Infrastructure	Active
	Bogus information attack	Application	Active
Confidentiality	Eavesdropping attack	Application	Passive
	Man-in-the-middle	Application	Active
	Traffic analysis	Application	Passive
Integrity	Masquerading	Infrastructure	Passive
	Replay attack	Infrastructure	Active
	Message tampering attack	Application	Active
	Illusion attack	Application	Active
Authentication and identification	Sybil attack	Application, infrastructure	Active
	Node impersonation attack	Infrastructure	Active
	Spoofing of GPS	Application	Active
	Wormhole attack	Application	Active
	Tunneling assault	Infrastructure	Active
	Replication attack	Infrastructure	Active
	Free-riding attack	Infrastructure	Active
Nonrepudiation	Repudiation attack	Infrastructure	Passive

attackers may launch this attack using a distributed denial-of-service simultaneously.

(2) Jamming attack

Attacker use of a highly driven signal of comparable frequency disrupts the VANET communication channel, which is the most dangerous security application attack. If a jamming assault is effective, the jammer interrupts the usable signal concurrently with an occurrence [61].

(3) Blackhole attack

In a VANET black hole attack, the malicious node may use other nodes to force them to pass their packets via it as often as feasible. Moreover, the routing protocol is primarily utilized to promote itself to other intermediary nodes as having the fastest path to the destination [47].

(4) Gray hole attack

This attack occurs when a malicious node appears as a regular node, resulting in eavesdropping and selective forwarding attacks, referred to as Gray hole attacks [62].

(5) Greedy behavior attack

This attack primarily targets MAC functionality and occurs when a malicious vehicle abuses the MAC protocol, resulting in traffic congestion and a collision on the broadcast channel. The other participants' legitimate services might be delayed [63].

(6) Bogus information attack

Vehicles utilize data created or sent by other vehicles or RSUs in VANETs. Attackers might generate and transmit misleading information to the network on its own or inject phony security messages into the network, as shown by accidents and traffic jams [64]. The attacker usually tries to control other cars with selfish or malevolent purposes [65].

2.6. Attacks on Confidentiality. Confidentiality requires assurances that unauthorized individuals in the network will never leak secret information [65]. It also prohibits unwilling access to personal data such as a person's name, license plate, and location.

(1) Eavesdropping attack

Eavesdropping aims to obtain confidential information from safe data [66]. Therefore, attackers can know of hidden information, including user identity theft and data location that can be used to identify vehicles.

(2) Man-in-the-middle attack

An attacker enters the network and intercepts a communication sent by the sender [67]. This message is altered before being delivered to the intended recipient. As a result, the sender/receiver receives incorrect information from the attacker despite believing the communication is accurate and trustworthy.

(3) Traffic analysis

An attacker analyses the traffic. The attacker collects all the information by getting involved in the vehicle network [68]. The attacker can attack by gathering information and categorizing nodes from all vehicles communicating.

2.7. Attacks on Integrity. Data integrity ensures that information obtained from nodes created during message exchange is accurate. Data integrity attacks are assaults on the transmitted data's integrity.

(1) Masquerading

An attacker can spoof privileged legitimate users for various malicious purposes, including gaining access to unauthorized information and avoiding detection and accountability [69].

(2) Replay attack

This attack aims to exploit the circumstances during the original message's transmission. An attacker might acquire network information, transmit, repeatedly provide actual data, and inject beacons and answers from the VANET network [39]. The attacker hopes to repeat or postpone fraudulent transmission.

(3) Message tampering attack

Data transported between the source and the destination targets message tampering attackers. Tampering attacks are frequently carried out when an attacker edits or changes previously delivered messages. This attack causes considerable problems in message transmission because an unauthorized person can tamper with messages and change their contents, making distinguishing between tampered messages and authentic messages difficult.

(4) Illusion attack

The attacker sends out alerts based on road conditions, giving the vehicles the impression of delays, accidents, and lower overall VANET results [70]. The adversary transmits scene-aligned traffic warning messages depending on the current road state, creating a deception for automobiles in its vicinity. The illusion assault may easily result in a vehicle accident, traffic gridlock, and a reduction in VANET bandwidth consumption.

2.8. Attacks on Authentication and Identification. The importance of based type information, such as user identification and sender address, cannot be overstated. It is required. Authentication may regulate the permission levels of cars and typically avoid Sybil attacks by providing unique identification to each vehicle [71]. While attacks against authentication are common, the attackers infiltrate the network using a false identity, disclosing faked GPS signals, changing, fabricating messages, introducing inaccurate information to cause harm, and disrupting communication between linked cars.

(1) Sybil attack

Sybil attack may be classified as one of the most severe assaults in VANETs. A node (vehicle) might pretend to have more than one identity [72]. It becomes more hazardous on networks utilizing geographical routing, as the attacker claims that the vehicle is at multiple spots by transmitting misleading information about its position.

(2) Node impersonation attack

This type of Sybil attack happens when an attacker determines the VANET's user ID [73].

(3) Spoofing of GPS

It is also regarded as a tunnel assault [74]. An attacker might feed bogus location information into another vehicle using GPS simulators. After exiting a physical tunnel or a jammed-up location, the victim may be waiting for a GPS signal.

(4) Wormhole attack

A wormhole attack (WA) is carried out by two or more hacked nodes that advertise that they have the shortest way to any destination [75]. WA extends packet tunneling between two malicious nodes in a VANET when the attacker has control of at least two malicious nodes. The attacker aims to change the network's logical topology to gather and manipulate massive volumes of network traffic.

(5) Tunneling attack

Like WA, a personal conversation on the tunnel channel starts using the same network. The attacker connects to the VANETs from two different locations. As a result, far away nodes may be connected as neighbors [47].

(6) Replication attack

The security of VANET is jeopardized by replication. In a replication attack, an attacker attempts to capture sensor nodes by obtaining the credentials of genuine sensor nodes [76]. Once captured, the adversary gathers all the credentials, such as keys and identities. To eavesdrop on transmitted communications or undermine the network's operation, the attacker creates a clone or replica of the original node in the same network to show that the injected clone is identical to the genuine node [77]. Node replication attack is a particularly severe assault on VANET. An attacker may target many sensor nodes by capturing the entire cluster or cluster head and creating a clone or duplicate of the entire cluster.

(7) Free-riding attack

This viral attack is carried out by a hostile user who uses bogus authentication and cooperative message authentication.

2.9. Attacks on Non-Repudiation. Repudiation is an attack where the attacker bypasses the transport and network layers. Denial of participation in the communication is referred to as a repudiation assault. Whatever a vehicle serves as a sender or receiver, an attacker node visits the system as a selfish node and denies any conducting action. It refuses the transmission or the receipt of a message, known as a repudiation attack. It wastes VANET resources, creates network delays, and consumes excessive network bandwidth [78].

Figure 2 depicts all of the attacks mentioned above and the protocol stack layers that may occur.

3. Misbehavior in VANETs

In VANET, security protection technologies aim to address security issues as the last section posed. That can be generally categorized into proactive and reactive processes [79]. The difference between proactive and reactive is that proactive security prevents the potential outside attackers from accessing the system. By contrast, reactive protection detects and corrects malicious node that has already occurred.

Proactive security refers to any technique that enforces a security policy. This category encompasses methods such as integrity and authenticity checks (e.g., cryptographic signature verification), access control mechanisms, and various other systems. The typical proactive security mechanism in VANET is PKIs which issue key material and certificates only to approved vehicles and entities. Without legal signatures, all unauthorized entities are excluded from the system. That setup establishes a trusted environment around all allowed entities. However, if the attack comes from an inside spy, it can still succeed in some situations. For example, an insider attacker may inject a bogus message to warn oncoming vehicles about a road hazard. To avoid obstruction, receiving vehicles brake forcefully. That attacks could result in accidents, jeopardizing passenger lives. In this situation, proactive security is not enough, which urgently needs active safety assistance. The reactive security mechanism consists of the detection and response phase that could thwart threats that are not prevented by proactive security [80]. One of the most prominent reactive security mechanisms is misbehavior detection [81].

3.1. Misbehavior Definition in VANET. Based on the target location of the attackers, attacks in VANET could be classified into intravehicle attacks and intervehicle attacks. Intravehicle describes the communications with a vehicle. For example, fake GPS information or deactivating an autonomous car's steering or braking system is exceedingly risky [82]. With the development of VANET, intervehicle communications are more complex than intravehicle communications because they are available when cars are stationary or moving [83]. Intervehicle attacks occur in vehicular communication scenarios, where vehicles gather information from other vehicles or the RSU to realize security functions. Vehicles, RSU, and cloud platforms transmit traffic-related information such as accident notifications, traffic congestion, and road conditions to aid intelligent transportation system management. Therefore, bogus message attacks caused by misbehaving nodes and fraudulent messages shared by these nodes may lead to severe consequences. With rising concerns, the primary focus of this study is intervehicle misbehavior.

Misbehavior is an ambiguous concept used in the environment of VANET. Numerous works of literature provide definitions of misbehavior [74, 84–86], which are generally implied by the attacker model. VANET misbehavior detection indicates that the node should be monitored for their misbehavior because of the false information they share. In this study, we defined misbehavior as the threatening behavior and false information carried out by the participants in intervehicle networks.

Threatening behaviors of an initiator in our misbehavior definition are not only referred to the behavior of attackers and malicious participants but also the incorrect behavior of faulty nodes. Thus, participating nodes could be distinguished into malfunctioning and malevolent nodes [87, 88]. The primary difference between these two types of nodes is whether they include malice. Faulty nodes are typically network nodes that produce incorrect data without malice. Examples include failing temperature sensors and GPS devices that cause false readings. Malevolent node behaviors are with malicious intent. Malicious nodes can be divided into two types, attackers and selfish participants. Attackers launching attacks aim to destroy the security of VANET with evil intentions and pose a direct danger to VANET security on purpose. Unlike this, selfish participants are more interested in getting priority in VANETs. For example, a traffic participant wants to prioritize using the road and sends a false message falsely claiming to be an emergency vehicle. These nodes may trick other network members into believing that they receive the real message. Classifications of misbehavior initiator and its possible threatening behaviors are as shown in Figure 3.

False information in our misbehavior definition refers to faulty and malicious packets that are not consistent with the previse message or are implausible with the underlying model. That may come from attackers aiming to disturb the environment or a damaged sensor. As we mentioned before, there are few encrypted protocols in the vehicular network, and transmitted messages (e.g., BSMs and CAMs) are approachable, and the content is rarely encrypted. Meanwhile, VANET is unbounded and scalable, which is a favorable condition to detect faulty messages. The next part classified threatening participants' attacker model by motivations and targets.

3.2. Attacker Model. In contrast to most network scenarios, no globally acknowledged attacker model is routinely utilized for VANET. This part examines the issues involved with the attacker model for VANETs and challenges. Raya and Hubaux proposed a foundational publication in security in VANET in 2007 [74]. They proposed the generic attacker model in their paper, which provides a set of classifications for attackers to identify different types of attacks by analyzing attackers' memberships, motivation, attribution, and scopes. Along with the generic attacker model, other notable attacker models remain. After reviewing the generic attacker model, we introduced a novel classification of the attacker model in VANETs, oriented by attack targets.

The generic attacker model is divided into four types: insider and outsider, rational and malicious, active and passive, and local and expanded.

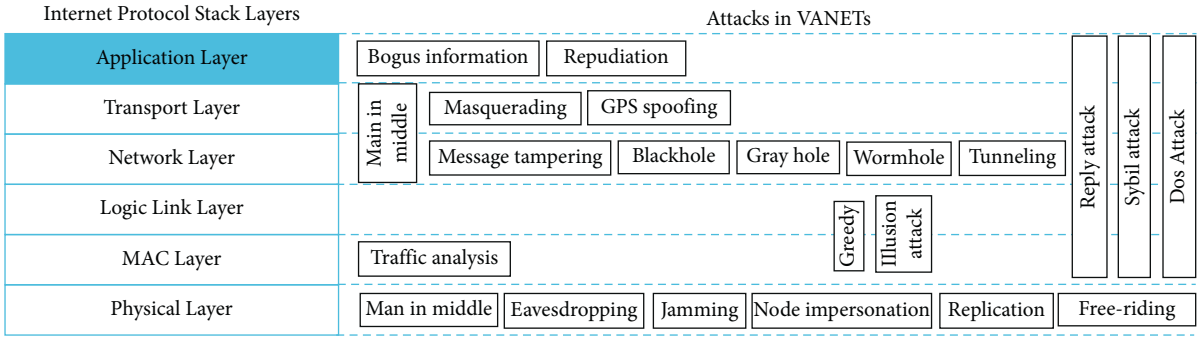

Figure 2: Attacks with corresponding Internet protocol stack layers.

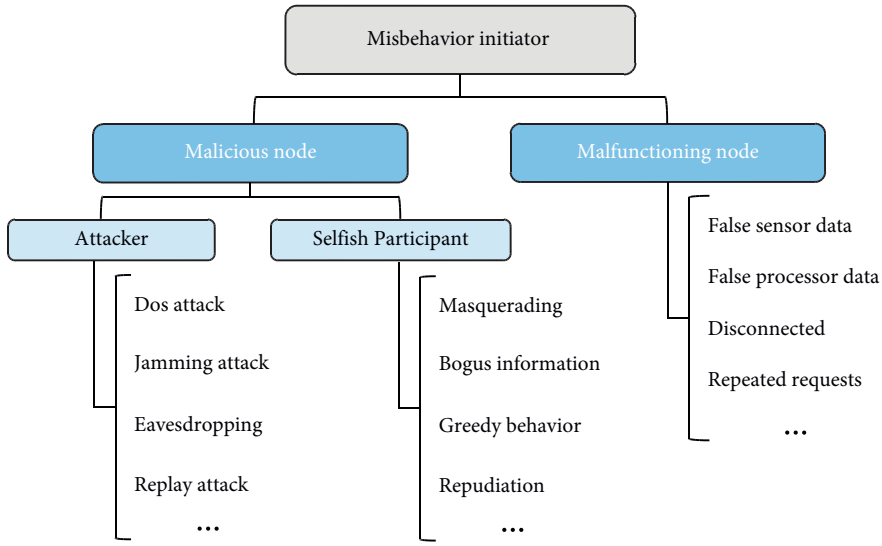

Figure 3: Classifications of misbehavior initiator.

(1) Insider and outsider

This category, which stands for membership, is discussed above. The system is inaccessible to all unlawful entities without the legally authorized certificate. The distinction depends on whether the attacker can access the system legally and possesses valid credentials. The outside attacker without valid credentials could be blocked out of VANET. For example, the insider attacker could insert a false message to harm the vehicular communication security.

(2) Rational and malicious

The attacker's motivation can be divided into two categories: rational attacker that derives a direct advantage from his attack and malicious attacker that tries to disrupt or inflict damage.

(3) Active and passive

The attacker's method can be classified into active and passive. The passive attacker only eavesdrops on the channel. However, the active attacker may threaten others by releasing malicious signals. This work aims to detect active attackers in this survey because misbehavior detection aims to ascertain if particular messages or signals represent undesired behavior.

(4) Local and expanded

The last classification criterion is the attack's scope, which might be local or global. The metric for this classification is not the number of attacked nodes but the distribution of the attackers. The scope of the local attacker model refers to the one attacker or multiple attackers existing in a limited area to control nodes. Expanded attacker model refers to the attacker's distribution across the network [25]. Dolev and Yao attacker paradigm is the most typical attacker model in this category [89]. In the Dolev–Yao model, attackers are authorized participants in the network who can intercept messages and change, delete, or copy messages to launch an attack.

With most participants being honest as a premise, several scholars have used game theory to formalize and expand these attacker models and gave examples in the literature [90–92]. Building on previous work, Monteuuis et al. [93] derived an attacker model based on the data life cycle and recent attacks. In this model, Monteuuis added one more classification of the attacker to Raya's research and

built a five-dimensional generic attacker model. The difference with previous work is taking attackers' goals as an extra dimension. The term "goal" refers to either a direct or indirect goal, which aids in identifying attackers in the perception domain. The primary target is reached directly in a direct attack, whereas the primary target is reached indirectly in an indirect attack. Monteuusis et al. also provided an example of similar attacks with a different goal, as depicted in Table 2.

Along with the generic attacker model, other notable attacker models remain. These attacker models can be classified according to the attack target: sensor-directed, data-directed, communication-directed, and processing-directed.

3.3. Sensor-Directed Attacker Model. Sensor aggressor aims at vehicle sensors, which disturb sensor perception through attacks. Petit et al. simulated the attacker model on the radar sensor [94]. They used lidar to capture, delay, and replay the signal. Additionally, they relayed and replayed the signal from a different location, paving the path for signal forging assaults. Yan et al. investigated attacks that utilize the underlying principles of sensors to blind or deceive them, such as using lights, noises, and radio waves to identify boundaries [95]. Sensor attacks can result in malfunctions, fudged readings, or physical damage. Moreover, a malicious sensor can radically alter the sensor orientation to cause the error of measurements. For example, Sitawarin et al. [96] proposed that signals vary as they are viewed from different angles, allowing the driver and sign recognition systems to interpret them differently. Therefore, the results of the sensor-directed attacker model could be disastrous for one automobile and a group of cars nearby in VANET.

3.4. Data-Directed Attacker Model. The data-directed attacker model is valuable for an attacker willing to message and data tampering. Petit et al. [97] proposed that the attack surfaces are derived using the V2X data lifecycle and used data lifecycle as foundations of a revised attacker model, which includes realistic attacks and responses. They mentioned that while data processing, rest, and transit are all well-secured, metadata and data acquisition demand special attention from the research community. Jedh et al. [98] proposed that CAN communications with arbitrary IDs and data are regularly sent by attackers, referred to as CAN message injection. Receiving ECUs has difficulty knowing if the sent message is sent by an attacker or by the intended ECU due to the broadcast nature of the protocol. An attacker may inject messages (for example, increasing the speed) that could jeopardize the driver's safety.

3.5. Communication-Directed Attacker Model. The communication-directed attacker model describes the malicious communicator who threatens vehicular communication. Malicious communicator is a term we use to describe an attacker who combines fully adversarial networking, voyeur, and communication trickster.

(a) Fully adversarial networking

Fully adversarial networking is a kind of attack in which an attacker sends arbitrary messages and then launches a selective DoS attack on a network. Several works of literature have studied the effect of this attack in VANET [99–102]. In this attack, the assailant targets the media to create a channel jam. The primary idea is to overburden the network and make legitimate nodes' access to networks and means difficult.

(b) Voyeur

Voyeur is an attacker who collects confidential information from anonymous public data transferred in cooperative ITS (e.g., routing). For threats to privacy in VANET, this attack is also one of the main issues being studied [103–105]. Voyeurs can monitor transmitting vehicles in a neighborhood using tracking. The attacker collects private data such as preferred driving path and geographic information. After processing, anonymous data can derive confidential information such as the vehicle owner's identity using its dwelling location.

(c) Communication trickster

Communication trickster refers to authentic messages that contain incorrect information. If these erroneous contents are left unchecked, several disassociations between V2X messages and sensor data may occur. It also can be used to describe an entity that transmits malicious updates over the air (OTA).

(4) Processing-directed attacker model

The processing-directed attacker model interferes with the perception system's processing and storage stages to disable or deceive the system. An attacker might construct valid virtual candidates to raise data processing's calculation demand [8]. The data processor has a gating process filtering mechanism to realize data association and track maintenance issues. It aims to reduce the amount of data processing needed to resolve the query. However, it can also be abused to create valid candidates for data processing [106, 107].

4. State-of-the-Art

As presented in Section 2, either IEEE or ETSI has a PKI-based system to protect vehicular messages. However, neither the IEEE nor the ETSI versions currently contain protections that assure the correctness of a V2X message's contents. Cryptographic techniques such as digital signatures, authentication, and encryption have long been employed as the first line of protection against various external threats. While having a valid signature, a participant vehicle with a legitimate set of digital certificates could deliver erroneous messages. Sensor failures, onboard unit problems, and hacking can cause these issues. The physical sensors that collect environmental data (e.g., GPS and radar) could provide inaccurate results. In conventional network

Table 2: Examples of similar attacks with a different goal.

Attacks	Attacker Model Membership	Motivation	Scope	Method	Goal
Alter road signs to fool sensors Alter road signs for "fun"	Outsider	Malicious	Local	Active	Indirect Direct
Camera blinding towards the unperceived stop sign Camera blinding for "fun"	Outsider	Malicious	Local	Active	Indirect Direct
Communication badmouthing Faulty safety message	Insider	Malicious	Both Local	Active	Indirect Direct

intrusion detection, detection looks for erroneous packets rather than harmful packets. Such a network deals with a high volume of encrypted traffic and a diverse range of application layer protocols. By contrast, transmitted data in VANET are rarely encrypted, which is mostly public to reach the "cooperative" goal between vehicles. Owing to the cooperative nature of VANET, malevolent nodes or intruders can still engage in harmful behavior such as DoS, vehicle hijacking, information leaking, data manipulation, and dissemination of false information. To identify and block the entrance of malevolent vehicles, intrusion detection systems (IDSs) have been suggested as a second line of defense [108–111]. IDS and intrusion prevention systems are generally deployed in traditional networks using reactive security mechanisms [25]. These mechanisms are being intensively explored, and numerous surveys have been conducted on the subject [3, 112–115]. These are mainly based on the detection methods: signature-based detection (target at known attack patterns), anomaly-based detection (target at detecting abnormal activity), anomaly-based detection (target at detecting specification deviations), and specification-based detection (target at specification deviations). However, due to the inherent features of VANETs and the harsh, dynamic environment, the traditional IDSs designed for other wireless networks such as wireless LAN, WSN, and relatively limited systems, such as an in-car system, are not directly applicable VANETs [108–111, 116, 117]. The high mobility, varying density, and network size introduce new vulnerabilities and challenges when applying IDSs on VANETs [109, 118]. Compared with intrusion detection, misbehavior detection can leverage the open nature of data and is not constrained by the absence of a system boundary, making it a potentially more suited technique. In Section 4, the state-of-the-art detection mechanisms based on their feasibility are presented.

4.1. Mode of Misbehavior Detection. The classification of detection mode is by participating nodes: local (standalone), cooperative, and global detection.

(i) Local (standalone) detection

It refers to each information packet detection by a single node (standalone vehicle or RSU) independently that uses internal consistency and, in several cases, the vehicle's sensors as correctness indicators. For this detection, these strategies do not rely on the responses of other nodes. Moreover, this detection mechanism checks for plausibility, consistency, and behavior.

(ii) Collaboration detection

With the assistance of neighbor nodes, cooperative data detection schemes monitor node verification for misinformation. When a node receives safety-related messages, cooperative data detection techniques examine data relationships with numerous vehicles in the network. The key advantage of cooperative detection is that it can more accurately locate misbehavior nodes. Cooperative-based detection schemes have sufficient information to detect fraudulent messages while also detecting spurious messages, including behavior-based detection, trusted-based detection, and consistency-based detection.

(iii) Global detection

It refers to detection that is not only by dependent nodes or cooperative detection but occurs with the help of a back-end system in some way. This operation may entail gathering the misbehavior reports received from the vehicle or RSU over a set period of time. The integrity of these misbehavior reports is then evaluated, and the misbehavior management component accurately defines the type of misbehavior. The misbehavior management component is a back-end security management system, which performs this activity in global detection. This process is assisted by vehicle, RSU, and the back-end system and does not need to be real-time due to the amount of processed data and the need for high detection reliability.

The attacks and detection strategies proposed in the literature are compiled in this part, and the potential solutions in different detection modes are listed in Table 3. A few years ago, most of the detection solutions in Table 3 were OBU-based, without any infrastructure support. The three subarchitectures of OBU-based techniques are standalone, cooperative, and hierarchical. Due to highly mobile vehicles going over broad areas, RSU-only detection uses central administration techniques to identify intrusions by installing RSUs covering large areas. To speed up detection by reducing detection accuracy, recently, the majority of the latest detection solutions have been collaborative. Hierarchical architecture is dispersed and cooperative by nature; it splits a network into groups, such as clusters, and assigns additional responsibility to specific nodes, such as cluster heads. Clustered routing protocols are often recommended for vehicle ad hoc networks [117, 118].

The local-based detection technique can be further divided into plausibility checking, consistency checking, and behavior checking. In plausibility checking, each node is verified through predefined rules. The movement of a vehicle is verified by two beacons sent to each node. A database checking model is proposed to prevent false information in VANETs. It consists of rules and a checking model. The main objective of these rules is to detect fake messages. For example, in consistency checking, false information is discovered locally rather than across VANETs. Consistency of messages from the same sender is used to detect inconsistencies. Behavior checking detection observes event reporters. These systems rely on single node behavior. The time cost of this technique is lower than others because it does not need other vehicles' behavior data [143].

Compared with local detection, cooperative detection has a higher detection success rate. The vehicles in the neighborhood are proof of misbehavior. Compared with local-based detection techniques, these schemes have a low false-positive rate, which can accurately detect Sybil attacks [72, 131–133]. Compared with local detection systems, cooperative detection generates higher overhead and processing. Moreover, the efficiency of cooperative detection techniques in VANETs may be hampered by low vehicle density [144].

Most of the global detection schemes are assisted by an infrastructure system. Within the infrastructure models, the credibility of misbehavior detection is established on infrastructure models by checking certificates supplied to vehicles [141, 145]. Global detection models also can be either entity or data-oriented models. Entity-oriented models seek to permanently exclude misbehavior nodes from all network processes permanently or temporarily. Data-oriented models are based on the similarity mining technique [120, 121], used to find similar messages or vehicles.

Furthermore, global detection mainly uses multiple levels to analyze messages to achieve global collective detection goals. Sedjelmaci and Senouci [146] proposed using three cooperative levels of intrusion detection. This scheme has a typical structure of global detection, local knowledge-based intrusion detection in each vehicle, collaborative detection by cluster heads, and global detection within the RSU and back-end.

4.2. Taxonomy of Misbehavior Detection. VANETs are vulnerable to various security risks [58, 143], as we reviewed in Section 2. Vehicles acquire not only messages but evidence for malicious behavior from around nodes.

In this situation, combining the VANETs characteristics, it is easy to find that misbehavior detection is a necessary and desirable approach to provide reactive security protection. In 2009, Raya first proposed a data-centric misbehavior detection framework, where Raya considers trust in information rather than in the information source. Following this work, many node-centric schemes have been proposed [143–145], which rely on the participants instead of information.

According to the previous work, mechanisms detecting attacks are categorized into two main classifications regularly used in the previous work: node-centric detection and data-centric detection [25, 85, 147]. Node-centric mechanisms are primarily concerned with the network's participants. To evaluate a node's forwarding behavior, they may look at packet frequencies, properly formed messages, and other variables. Alternatively, they might focus on participant participation and estimate their trustworthiness based on prior signals' accuracy. In contrast to focusing on the node, the data-centric detection mechanism focuses on the message rather than the sending node. They rely on the message's content to verify its validity. The correctness of the message must be evaluated. Based on the categorizations above, we further refined either data-centric detection or node-centric detection into two branches according to the detection mode we introduced above. The classification of branches is dependent on the feature of communication from a single-vehicle (autonomous) and mechanisms that seek to derive misbehavior from multiple vehicles (collaborative). Autonomous detection has the benefit of working regardless of whether attackers are present, whereas collaborative detection relies on the existence of an honest majority. The taxonomy of misbehavior detection is shown in Figure 4. After discussing these classifications, the two primary categories and their branches are explained in detail.

4.2.1. Node-Centric Misbehavior Detection. Node-centric strategies focus on the participants' behavior instead of the data, which analyzes the behavior or interaction with neighborhood vehicles to determine its trustworthiness. For example, based on the nodes' behavior, the detection result depends on whether a node acts stable to send reliably by examining packet frequencies and formed messages. Node-centric detections are further classified as autonomous and cooperative mechanisms.

(1) Autonomous Detection Mechanism. Autonomous detection is the first branch of node-centric detection, which analyzes data on a node-by-node basis rather than data semantics. This sort of detection uses protocol-level trends in specific node activity that examine the number of messages sent by a node and their format.

(A) Static knowledge and protocol-based detection

The static knowledge and protocol-based detection are denoted based on static knowledge and protocol rules. These checks were first mentioned by Leinmuller et al. in 2006 [148]. Within this part, this detection is divided into three types.

(1) Message transmission-based detection

Message transmission-based detections are based on the messages of a particular node, which can detect the received messages from single-hop neighboring vehicles. This detection mainly concentrates on the message format and message frequency. Because of the commonality of the vehicular communication channel, the

Table 3: Study of existing approaches in three modes.

Mode	Study	Detection node	Resist attack(s)	Proposed method	Response mechanism
Local (standalone)	Golle et al.	OBU-based	Correcting errors	Comparing received data [106]	Correction
	Hortelano et al.	OBU-based	Blackhole attack	Watchdog mechanism [119]	—
	Safi et al.	OBU-based	Wormhole attack	Packet leashes and authentication [120]	—
	Lo et al.	OBU-based	Illusion attack	Plausibility validation network model [72]	—
	Studer et al.	OBU-based	GPS spoofing	Convoy member authentication and vehicle sequence authentication [121]	—
	Adjih et al.	OBU-based	Replay attack	Counting technique and timestamps [122]	Packet dropping
	Zhou et al.	RSU-based	Sybil attack	Pseudonym pool and hashing pseudonyms [123]	Revocation
	Rahbari and Jamali	RSU-based	Sybil attack	Fixed key and encryption mechanism [124]	Revocation
	Soryal and Saadawi	RSU-based	DoS attack	2D Markov chain model [125]	Isolation
	Verma et al.	RSU-based	DoS/Flooding attack	Hashing and IP statistics [126]	—
	Verma and Hasbullah	RSU-based	DoS attack	Bloom-filter and IP-CHOCK [127]	Alarm
	RoselinMary et al.	RSU-based	DoS attack	Detecting position changes [128]	—
	Ghosh et al.	OBU-based	Bogus information	Postcrash notification based on observing deviation of trajectories [129]	—
	Vora and Nesterenko	RSU-based	Bogus information	Local verification protocol [130]	—
Cooperative	Xiao et al.	RSU and OBU	Sybil attack	Signal strength analysis [131]	—
	Hao et al.	OBU-based (cooperative)	Sybil attack	Geographic information and correlation analysis [132]	Isolation
	Grover et al.	OBU-based (cooperative)	Sybil attack	Observing similarity in neighboring nodes and motion trajectories [74]	—
	Park et al.	RSU and OBU	Sybil attack	Timestamp series approach [133]	—
	Leinmuller et al.	RSU and OBU	Falsified position	Estimation of trustworthiness of position claims [81]	—
	Sedjelmaci et al.	OBU-based (cooperative)	Denial-of-service (DoS), integrity target, and false alerts generation	Signal strength intensity (SSI), packet's round trip time (RTT), and vote mechanism [134]	—
	Zaidi et al.	OBU-based (cooperative)	False data	Hypothesis testing for data correctness [135]	—
Global detection	Lee et al.	Local server	Sybil attack	Session key-based certificate [136]	—
	Feng et al.	Hybrid	Sybil attack	Event-based reputation value and trusted value computing [137]	—
	Chang et al.	Hybrid	Sybil attack	Footprint based on trajectories identifications [138]	—
	Adhikary et al.	Individual system	DoS attack	SVM kernel methods of AnovaDot and RBFDot [139]	—
	Kerrache et al.	Hybrid	DoS attack	Trust framework and data-centric verification [140]	Blacklist
	Sedjelmaci et al.	Hybrid	Multiple misbehaviors	Three layers intrusion detection framework and cluster algorithm	Blacklist and suspected list
	Kumar and Chilamkurti	Hybrid	Multiple misbehaviors	Learning automata-based intrusion detection algorithm [120]	—
	Kerrache et al.	Hybrid	Multiple misbehaviors	Trust model using watchdog mechanism [141]	Isolation
	Kerrache et al.	Hybrid	Multiple misbehaviors	Trust evaluation based on adaptive detection threshold [142]	—

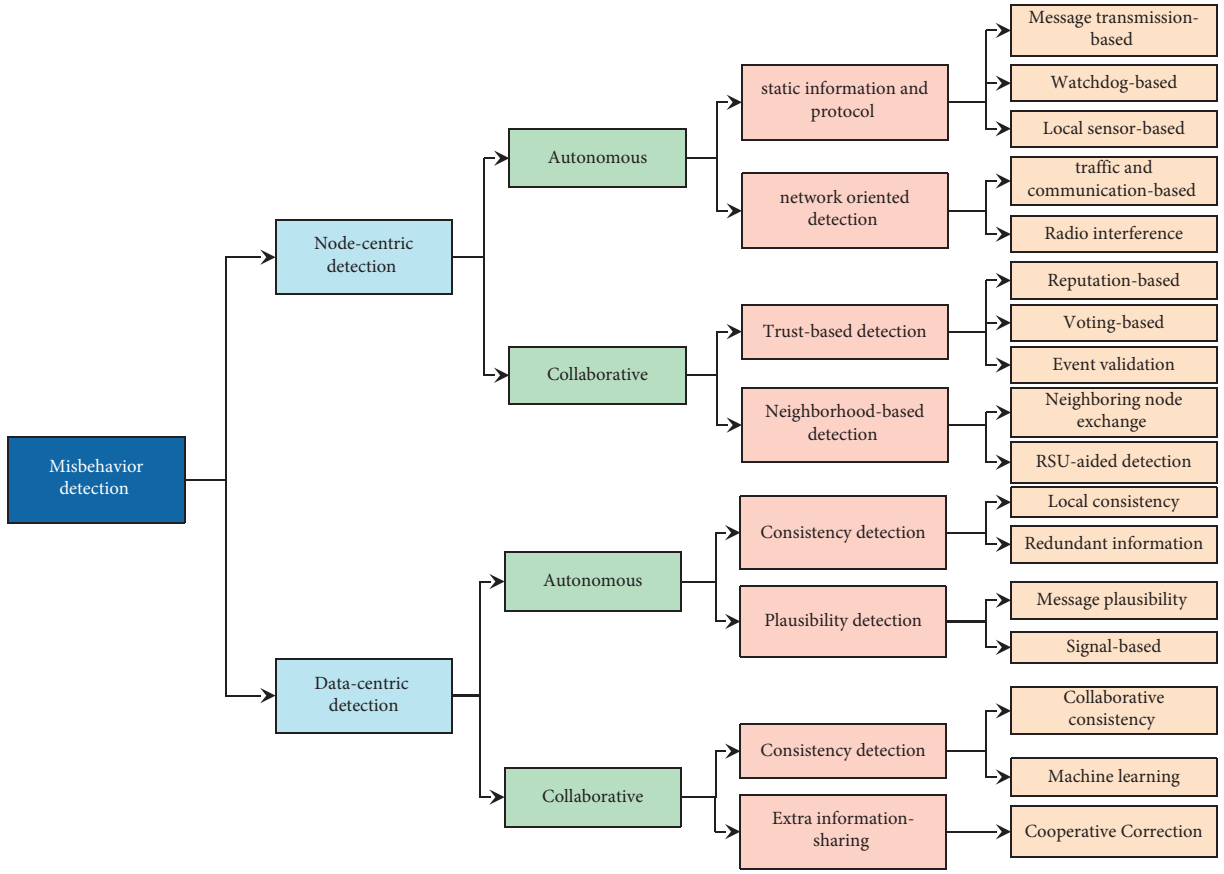

Figure 4: The taxonomy of misbehavior detection.

maximum transmission frequency of vehicular messages is limited. Moreover, vehicular messages are in a common fixed format. This mechanism in VANETs typically focuses on abnormal nodes that send messages too frequently or incorrectly. Because these assaults are similar to those targeted by some network intrusion detection systems and this question is application-oriented, few VANETs-specific types of research are available.

(2) Watchdog-based detection

As one of the intrusion detection techniques in wireless sensor networks, the watchdog is a network monitoring technique that detects misbehavior nodes based on the routing protocol. The watchdog mechanism provides the means for detecting various kinds of attacks, e.g., gray hole, delay, injection, or flooding attacks [149].

In the concept of the watchdog mechanism, each node watches the network to ensure that its neighbors forward messages, which has been proposed for routing security in mobile ad hoc networks at first [150]. Then, several approaches and mechanisms of follow-ups were used to defend VANETs from their selfish behavior. In 2014, Baburajan and Prajapati [151] described a watchdog system for detecting misbehaving and greedy individuals in networks. Each node watches its surrounding nodes to recognize misbehaving nodes by maintaining a buffer of recently delivered packets. Determinants to identify selfish nodes in this scheme are intermediate forwarding node rule-abidingly transfer the packet or keep the packet selfishly. The watchdog then eliminates and punishes such self-centered nodes from the network. John and Haroon [152] described a novel watchdog technique based on the path and thresholds assessment to avoid packet transmission through selfish nodes. According to the average of nodes' ratings in this scheme, the path with the highest metric is the most reliable to exclude the selfish nodes. Similarly, Senthilkumar and William [153] proposed a scheme composed of a watchdog mechanism, threshold computation, and manager for misbehavior node detection. In this scheme, the management system consists of a monitoring system, a reputation system, a trust manager, and a route manager. The mechanism monitors the behavior of neighboring nodes and alerts the management system to any instance of misbehavior. When a node reaches the threshold value, the path manager takes action, and the trust manager alerts other nodes to the misbehaving node.

(3) Local sensor-based detection

The local sensor-based detection is based on the local sensor measurements or checking the neighbor node's reported location. Local-equipped sensors, such as radar, camera, and detector, can track the surrounding vehicle traveling and verify its claimed position.

Due to the widespread usage of front radar systems in automobiles, radar transceivers have become the main local sensor in this mechanism. Yan et al. [154] originally explored employing local sensors to validate reported positions in VANETs in detail. They proposed an innovative method by using onboard radar to identify the announced coordinates of neighboring vehicles. They compute the cosine similarity between radar data and neighbor reports to separate fake data from real data. Their scheme is useful to defend Sybil and position-based assaults. Similarly, the framework of Jaeger et al. [155] incorporated a radar sensor into a system for detecting misbehavior. It integrated the environment sensors and tested its practical applicability using recorded traces and radar data from test cars. The camera has been widely used in local sensor-based detection despite radar-based detection in recent years. Using two independent sensors, Zacharias and Fröschle [156] proposed a unique technique for detecting misbehavior in VANETs based on local traffic density. The key to their scheme is the sensor fusion of multiple sensors. They combined information from trustworthy and unreliable sensors to detect misbehavior based on onboard camera sensors data. It has been proved that this scheme is well-suited for detecting illusion assaults. Nguyen et al. [157] proposed a novel approach to verify the motion behavior of vehicles, which solved the sensor failure problem. By extracting position information in exchanging information, their scheme supports recreating and evaluating a target vehicle's motion behavior and the authenticity of data shared via cooperative vehicular communications. Moreover, unlike previous research, this study regularly corrects the anticipated trajectory's checkpoints using periodically changing sensor data. It is effective for collusion and Sybil attacks. Local sensor-based detection is useful to deal with various attacks. To this detection mechanism, the reliability of the input data is crucial. Furthermore, it mostly relies on the availability of equipped sensors.

(B) Network oriented-detection

(1) Traffic and communication-based

The network traffic-based strategy aims to detect probable routing misbehaviors by examining and recording network traffic and communication events [158]. Shila et al. [159] proposed the scheme based on channel estimation and traffic monitoring. Each node monitors its nearby nodes' downstream and upstream network traffic. Furthermore, it determines a packet loss rate to identify the misbehavior node that launched the selective forwarding attack in wireless mesh networks (WMNs). The study presented an adaptive detection threshold for detecting selective forwarding attacks in WSNs [160]. Nearby nodes are monitored, and sensor nodes estimate the usual packet loss rates between themselves and their surrounding nodes and use these estimated packet loss rates to evaluate the downstream neighbors' forwarding behaviors along the data forwarding channel. Similarly, Swetha Priya and Prakah Reddy [161] take lifetime account to the channel aware-based misbehavior detection. The sensor nodes estimate the traditional packet loss rates between themselves and their neighbors and use the calculable packet loss rates to estimate their peers' forwarding behaviors along the information forwarding channel. During forwarding assessment periods, sensor nodes that misbehave are punished by decreasing their trust values. In subsequent research, a detection method based on adaptive learning automata and communication quality was proposed [162]. The adaptive reward and punishment parameters of a detection learning automaton are decided by the node's overall communication quality and the vote of its neighbors to reward or penalize malicious nodes.

(2) Radio interference

Not exactly like watchdog detection, Radio interference detection is mainly used to solve jamming attacks, MAC attacks, and flooding attacks. Puñal et al. explore and analyze several jamming attacks. They demonstrate, in particular, that some types of jammers are capable of completely disrupting communication with a high probability, demonstrating the critical nature of jamming detection [163]. Hamieh et al. [164] proposed a scheme for detecting jamming attempts based on patterns in radio interference. They concentrate on a particular attacker staring at the channel and launching a selective jamming attack when the particular message appears. They suggest that a correlation coefficient between the time of accurate reception and reception faults can be utilized to evaluate the degree of jamming. However, the reception mistake is random. Thus, jamming attacks only occur when the correlation is extremely strong. Various emerging technologies have been used in radio interference detection in recent years. Karagiannis and Argyriou [165] proposed an interference detection approach using unsupervised machine learning. This method uses a series of novel metrics

containing the relative speed between receiver and attacker and parameters obtained from the onboard device on the receiver. Assisted by clustering, unsupervised learning differentiates intentional from unintentional jamming and identifies each jamming attack's unique characteristics. Kasturi et al. [166] used machine learning to classify different types of interference attacks and concluded that jamming attacks could be detected with very high accuracy using the gradient boosting algorithm. However, the discrete random jamming attack is still a problem. Nallarasan and Kottursamy [167] proposed an autoencoder deep learning architecture-based jamming attack detection scheme in IoT. The jamming detection problem is modeled as anomaly detection. The suggested system simulates a random jamming assault and detects it at a certain time instantaneously, providing information that may mitigate the jammer attack.

(2) Collaborative Detection Mechanism.

(A) Trust-based detection

(1) Reputation-based detection
The reputation-based detection algorithm depends on the node's historical and current reputation. Michiardi and Molva initially presented a collaborative reputation mechanism (CORE) [168] based on the DSR routing protocol. It promotes node collaboration by monitoring nodes' cooperative behavior and utilizing a reputation system. Marias et al. [169] introduced the CORE method, in which each network member in CORE uses a reputation technique to track other members' involvement. The reputation measure is derived using data acquired by other nodes participating in network activities and data observed by the local node. Nodes with a good reputation could access network resources, but nodes with a low reputation do not. Abirami and Sumithra [170] utilized the credit-based mechanism, which gives nodes credit to encourage and urge them to collaborate. The proposed routing algorithms are based on neighbor credit value and improved neighbor credit. A credit-based incentive system utilizes credits to charge and reward members who send and receive packets. The proposed method uses cooperative game theory to discover and monitor selfish behavior nodes.

(2) Voting-based detection
This technique ensures the integrity of an event by voting or cooperative validation. This technique is often effective in a densely populated network with an honest majority and trust [171, 172]. Moreover, many researchers utilized evolved approaches dependent on establishing cooperative trust via voting or agreement. Raya et al. [173] proposed protocols as part of a framework for identifying and local containment of misbehaving or faulty nodes. It is based on the Local Eviction of Attackers by Voting Evaluators (LEAVE) protocol to protect system operation until the attacker's authorization is revoked by the CA, partially or entirely based on the evidence LEAVE provides. Leinmueller et al. [174] offered cooperative systems based on two fundamental concepts. The neighboring automobiles exchange ratings obtained from a previously passed neighbor and use the ratings used. Second, vehicles exchange their neighbors' IDs and location information. Talreja and Jethani proposed a vote-based misbehavior node detection architecture [175]. Their scheme enhanced Channappagouda et al.'s mobile agent-based technique [176] and used zonal agents (ZAs) and the relationship of trust between ZA and zone nodes [175]. Kerrache's scheme [140] enables the estimation of traffic density, entity trust, the distribution of dishonest nodes throughout the network, and the integration of several trust measures such as direct, indirect, event-based, and RSU-based trust. It excludes dishonest nodes from all network activities.

(3) Event validation
Unlike common security messages (i.e., BSMs), event messages are multiple hops in VANETs. This feature accelerates the rapid spread of false event messages in insecure situations. Thus, in trust-based mechanisms, the application of trust over multiple hops is a common challenge. Event validation is a special voting-based mechanism that overcomes this issue by enabling each vehicle to vote in favor of or against a given event using their identification. The criteria for this mechanism are usually a collaborative decision by the nodes to reach a consensus on whether the event really happened.
Hsiao et al. [172] describe the first VANET-specific threshold-based event validation system. This scheme relies on a threshold number of notifications to establish consensus among vehicles and validate an event's legitimacy. To avoid assaults, senders gather many witnesses for each probable occurrence. Moreover, they recommended z-smallest probabilistic counting, which reduces the number of signatures attached to the message, to balance security and efficiency. In this concept, to guard against the situation that attackers exaggerate the number of witnesses to an event, each vehicle signs a hash of its vehicle identification number, the event type, the geographical segment, and the time of the event. The aggregate retains just the z-smallest signatures, making it difficult for the attacker to generate these z-encrypted signatures. However, this

scheme is effective against bogus event messages created fictitiously but hard to guard against complicated cover-ups.

Recently, blockchain has been regarded as an ideal match for VANETs [177]. All the alerts sent by cars and the decisions made by the RSUs should be maintained in an immutable public ledger that is available to all the organizations engaging in these traffic occurrences. Thus, blockchain-based event validation is more reliable than other schemes. Al-Ali et al. [178] proposed a reputation-based traffic event validation scheme based on the previous threshold-based system. It validates traffic events through proof of authority and event consensus methods and leverages an efficient mutual authentication mechanism between automobiles and RSUs that can ensure the reliability of the event notifications sent by nodes. The reputation scores that are assigned to vehicles based on their statistical records can reduce internal attackers' effects and detect selfish and malevolent vehicles.

(B) Neighborhood-based detection

(1) Neighborhood node exchange

This mechanism is executed by additional information exchange between surrounding cars. Originally, Leinmüller et al. [179] proposed using data-centric strategies described in proactive neighbor table exchange in node-centric detection. Their position verification scheme combined proactive exchange of neighbor tables and reactive position requests. Nodes exchange neighbor tables and verify that the locations obtained match their own. Furthermore, Van der Heijden et al. [180] provide a statistical model-based system in which cars calculate and broadcast a flow parameter. This scheme utilized location information and applied subjective logic misbehavior identification. Their scheme improves two procedures, acceptance range threshold (ART) and proactive neighbor exchange. Due to VANETs being a large-scale complex network, limiting most schemes are limited by scalability issues. Cheng et al. [181] present an approach for detecting overlapping communities based on local growth and neighborhood information to solve this issue. Moreover, a belonging coefficient is proposed to filter away detected malicious nodes. Additionally, only neighbors of nodes in the previous iteration are added during the iterative expansion process instead of all neighbors, that can decrease the computational cost, which is the main problem in neighborhood table exchange.

(2) RSU-aided detection

RSU-aided detection is a centralized detection solution for a malicious node, which describes the detecting interactions between surrounding infrastructure and vehicles. This detection mechanism mainly focuses on spreading fake position information and Sybil attacks in VANETs. RSUs are responsible for doing these verifications to determine the authenticity of a node's location, which uses a sequence of verifications, including an acceptance range check, a maximum permissible speed check, a node density check, a speed consistency check, and a time interval substantiation check. Furthermore, various technologies are used to verify RSU-based detection, for example, trajectory tracking and identity observation. Chang et al. [138] proposed a footprint scheme by utilizing the similarity of trajectories generated by RSUs that a vehicle passes. In footprint, these trajectories are encrypted and comprised of unique signatures sought by the vehicle from the RSUs it encountered while traveling. By requiring the attacker to collect signatures via RSUs, they set a constraint-based on their actual journey. Then, when Sybil assaults are detected, all suspiciously similar trajectories are assumed to originate from the same vehicle (referred to as a Sybil community). Hamed et al. [182] proposed an identity observation-based RSU detection scheme. This scheme uses dynamic characteristics of VANETs to assume that two vehicles simultaneously crossing several RSUs are considered an unusual occurrence. The proposed approach combines multiple RSUs to detect attackers through normal communications between nodes and RSUs. The detection of two separate IDs in the area of two distinct RSUs demonstrates unequivocally that the IDs belong to different cars. They utilize these two data to establish whether or not the Sybil assault is occurring. Position verification is crucial for safety warnings, and the vehicle would delay until it receives a response from the RSU. Thus, choosing an RSU with the appropriate communication distance is a key factor affecting the efficiency and latency of such schemes. This issue is generally solved by signal strength evaluation. Sun et al. [183] proposed a unique passive RSU localization system to estimate the location of the RSU via examining the Doppler effects of the received signal. Moreover, the RSU location estimator is developed by the greatest likelihood estimate approach. The vehicle may predetermine the desired RSU to communicate based on its position and route information in this scheme.

However, widespread RSU deployment is still a deployment issue. And another concern is that in most schemes, RSUs are considered fully trusted. Full trust cannot be assumed for the devices that may let to physical attacks like sensor tampering and differential power analysis.

4.2.2. Data-Centric Misbehavior Detection

(1) Autonomous Detection Mechanism. The autonomous detection branch in the data-centric mechanism indicates messages verifications to the same sender. Verification in this mechanism may include the semantics of message, position, and physical layer signals to determine if they come from the same source.

(A) Consistency

Each vehicle verifies the consistency of each message received individually. Each data should be consistent with the previous data. In the local consistency, false message detection is based on a local database instead of surrounding vehicles.

(1) Local consistency
The result of local consistency is examined by a fusion program, which evaluates whether a vehicle is performing abnormally [28]. Ghosh et al. [129] assumed that a vehicle issuing a warning event would act predictably. For example, a vehicle delivering a blocked road notice must be close to the event. Receiving vehicles observe a vehicle producing a warning event to assess the message's legitimacy. A misbehaving node might provide messages matching events that have not happened or erroneous information relating to an actual event. They proposed a detection scheme based on a cause-tree approach to achieve misbehavior detection and identification of its root cause jointly. Ruj et al. [184] described data-centric misbehavior detection. They offered techniques for detecting false warning messages and misbehaving nodes by analyzing their behavior after the alert messages had been sent out. Each node in the data-centric misbehavior detection system may assess if the information received is accurate or incorrect on its own. The decision is made based on the regularity of previous messages and a new warning that includes reported and predicted vehicle whereabouts. Guo et al. [185] presented a context-aware trust management methodology for evaluating the content integrity of messages received by vehicles and assuring responsible decision-making. The suggested method does not require the honest majority assumption.

(2) Redundant information consistency detection
In addition to checking the consistency of existing and previous data, redundant data consistency checks for the node are another data-centric consistency detection. Unexpected deviation might occur in some cases. For example, redundant information is stored owing to several messages received across separate communication channels or on distinct layers of the OSI layer model. Moreover, due to the format of the V2X message, position information occurs in several clips of the packet. If the attacker only tampered with the information in certain fragments, it might be another explanation for deviations.
Bißmeyer et al. [186] proposed a detection mechanism that the consistency of identifiers contained in V2X packets has to be checked. They mentioned that the node ID in the network header and the station ID in the payload must be connected to the certificate included in the security header. The identifiers from the MAC header, network header, security header, and payload are gathered and compared on the topmost message processing layer upon packet reception. The packet might be considered defective if the IDs are inconsistent or cannot connect to the certificate or its ID. This scheme is useful to detect Sybil attacks. Besides redundant message consistency detection, sensor redundant information consistency check also is useful to defend against attacks. van Wyk et al. [187] mentioned that sensor redundancy could lead to enhanced, dynamic sensor fusion, in which abnormal sensor readings can be discarded while the normal data is fused to improve the dependability of the utilized data.

(B) Plausibility

(1) Message plausibility check
Message plausibility-based detection uses an underlying model of the message, predefined rules, and physical boundaries. For example, these checks are performed using a sent position vector, which contains the sender's position, current speed, and heading at a given moment in time. The provided values are compared to the preset domain of definition in this detection. The information in the packet is either compared to a model prediction or utilized to determine if the information in the packet is a feasible next step based on the model.

Firstly, Lo and Tsai [70] propose a plausibility validation network (PVN), which consists of a checking module and a rule database. In their scheme, by examining the various message fields, the rule database comprises a set of rules that control whether specific information should be deemed legitimate or not. Their detecting criteria of the message include discarding repeated messages, being in transmission range,

and legitimate time stamps. Moreover, the different message type has different detecting guidelines. This scheme is effective in defending against illusion and injection attacks. However, their scheme believes the attacker can only change messages indirectly. Furthermore, because everyone has access to the rule database, the attacker can only send legitimate messages to avoid detection.

It is difficult to meet the security requirements of VANET by simply targeting the plausibility detection of messages. Thus, most subsequent studies have used hybrid schemes for plausibility detection. For instance, Arshad et al. [188] proposed a hybrid scheme based on the Beacon Trust Management System and Fake Data Detection (BTMS-FDD). The nearby vehicles are connected based on speed and density data by trust management system connects. Moreover, the false safety event detection technique utilizes plausibility detection of beacon and relative messages positions and speeds information, which is useful to bogus safety incidents detection. Detection accuracy and false alarms are still a challenge to plausibility detection. Unlike previous work, the consistency check has been combined with plausibility by Ghaleb et al. [189]. They proposed a context-aware misbehavior detection scheme (CAMDS) technique using the sequential examination of temporal and geographical correlation of nearby vehicles' mobility information. Firstly, a dynamic context reference is created online and updated regularly using statistical approaches. Then, the Kalman filter technique tracks mobility data received from nearby cars. Using box-plot, the Kalman filter's innovation errors are used to build a temporal consistency evaluation model for each nearby car. The Hampel filter is then used to create a spatial consistency evaluation model representing the current context reference model. Plausibility assessment reference models are constructed online and updated regularly using the Hampel filter and nearby information's consistency assessment reference model. If a message's consistency and plausibility ratings differ significantly from the context reference model, it is classed as suspicious.

(2) Signal-based plausibility

For message location verification, this approach depends on the physical properties of the signal. The received signal strength indicator (RSSI), arrival time, angle of arrival, and Doppler speed (DS) are physical features. The use of distance-bounding in vehicular networks is proposed in schemes, which use the speed of light and the message timestamp to validate the distance from the signal source [74, 184]. They offer a technique for triangulating a node utilizing distributed sensors on a network, which might be classified as RSUs at the moment. In addition, many researchers imply that the signal's physical features may be used to verify the location. Xiao et al. [131] used received signal strength (RSS) in the location verification procedure. Pouyan and Alimohammadi [190] introduced that position verification methods, such as RSSI, are lightweight and straightforward. Suppose they have high accuracy for position verification. In that case, it is helpful for misbehavior detection such as position verification after receiving location information broadcast by vehicles regularly for position-related applications. Sun et al. [191] proposed a novel data trust framework, which detects false data and securely tracks vehicles. The core of this scheme is to verify the implied effect of the vehicle's reported data using secure sensing mechanisms based on an extended Kalman filter from the wireless physical layer. Faced with physical layer detection, So et al. [192] proposed three-layer plausibility tests based on the RSSI of the exchanging messages. These plausibility tests use multistep procedures to increase detection rates and the number of false positives. These detections may be performed separately by each vehicle and do not assume that the majority of vehicles are trustworthy. Gyawali and Qian's work [6] presented a cooperative machine learning-based strategy to identify two types of assaults in the physical layer: false alert attacks that broadcast false alarm messages and position falsification attacks that falsify location information. Each vehicle broadcasts the detection result to its neighbors. Then, misbehaving automobiles are ejected from the system based on the aggregated results of all adjacent vehicles.

(2) Collaborative Detection Mechanism. Collaborative detection mechanism techniques examine packet sequences from different vehicles. These methods are primarily concerned with recognizing and resolving conflicting data and using secure aggregation techniques to integrate data from several vehicles into aggregates and determine the conflict node. Collaborative detection is defined as a pairwise comparison of messages from various vehicles. The benefit of collaborative-based detection is that constructing appropriate schemes is easier and more efficient. However, an honest majority prerequisite is often required to obtain factual findings. If multiple collaborating assailants surround a victim, the collaborative scheme may collusively attack information from legal cars.

(A) Consistency-based detection

(1) Collaborative consistency-based detection

Despite the local consistency check, which only uses local information instead of information from other nodes, consistency can also be

defined as a pairwise comparison of messages from different vehicles in the collaborative mode. The advantage of consistency-based detection is that only a small amount of domain knowledge is required to design reasonable schemes. However, an honest local majority must be prerequisites for reliable conclusions. Moreover, some schemes use collaborative consistency and plausibility in collaborative consistency-based detection. For instance, vehicles that use data-centric detection assess the accuracy of the information by looking at the consistency and the plausibility of the data they transmit [193]. If the consistency and plausibility scores surpass predefined criteria, it is classified as a misbehavior message, and the sender vehicle is accused of misbehaving. Golle et al. [106], who used an abstract model of the cITS to verify consistency between messages, reported the earliest example of data-centric detection. Nodes may attach observations to the received communication. They can identify nearby vehicles and authenticate to another. Zaidi et al. [135] compared the data from a single car to the overall flow of all nearby neighbors. The authors recommended that beacon messages be expanded to include three fields, flow, average speed, and density, all of which must be computed and transmitted regularly by all vehicles. They used statistical techniques to detect anomalies and identify rogue nodes using a traffic model and statistical techniques to determine false data, especially in emergency messages. Rakhi and Shobha proposed a data-centric strategy based on comparing average flow rate or mobility information provided across network vehicles [194]. This method does not require any assistance from the infrastructure during the identification of attackers.

Similarly, based on the previous work, Ranaweera et al. [195] incorporated traffic flow phenomena into anomalous data detection systems. This study includes data sources utilized for vehicular flow measurements and traffic flow theory to detect anomalous data in vehicular networks. According to the nature of traffic flow physics, the headway and speed of vehicles are constrained around an average value under a steady-state situation. The suggested technique identifies anomalous sources by detecting contradictory beacon attributes separately.

(2) Machine learning

With the growing interest in machine learning, most research in security schemes is turning to machine learning and its derivations (i.e. deep learning) [196]. Thus, we made this technology a separate branch of consistency detection. Firstly, this mechanism is suffered from two problems. Some work on adversarial machine learning has revealed that the current situation is volatile [197] and has not met expectations performance. Another challenge is a dearth of trustworthy public datasets for vehicle networks since they are still a developing class of networks [198]. However, these do not affect this technology's rapid adoption and development. In 2021, Kamel et al. [28] modified the dataset based on the first publicly available dataset for misbehavior detection. The VeReMi dataset has been utilized in misbehavior detection research. Recently, they added a realistic sensor error model, a new set of assaults, and a higher amount of data points to the dataset. Furthermore, they utilize a set of local detectors and a basic misbehavior detection technique.

Firstly, in 2011, when machine learning was not investigated in misbehavior detection, Grover et al. used ensemble-based machine learning approach to classify misbehaviors in VANET, which is expanded on their prior work by replacing the single classification method with a collection of classification algorithms. However, these efforts rely on specific attack implementations and a specific scenario. In particular, no specifics about attack implementation or the base scenario are disclosed. Thus, it is impossible to identify whether these classifiers give a general solution or a solution particular to the circumstance. As this technology matures, ML-based abnormal behavior detection solutions have increased in recent years. Mahmoudi et al. [199] proposed a detection scheme based on sending messages to misbehavior authority (MA) by nodes. Furthermore, using ML in the MA processing period to classify reports from nodes and identify the different types of misbehavior. Solving the position falsification attacks, Ercan et al. [200] proposed an ML scheme that uses three additional features connected to the sender position to improve the performance of IDS for position falsification attacks. These three features are estimated angle of arrival, estimated distance between sender and receiver, and the difference between the declared and estimated distance between sender and receiver. They also compared two distinct machine learning (ML) classification algorithms, namely k-nearest neighbor (kNN) and random forest (RF), which are used to detect hostile cars using these features. At last, ensemble learning (EL) boosts detection performance by integrating several ML algorithms (i.e., kNN and RF). Additional, ML-based misbehavior detections can also solve Sybil attacks [201], DoS attacks [202], spoofing attacks [203], etc.

(B) Extra information-sharing

The extra information-sharing mechanism is based on exchanging additional information between

neighboring vehicles. Vehicles then use this information to detect problematic messages. It is also necessary to evaluate the legality of exchanging extra data between neighbors. Hao et al. [132] proposed a detection scheme by analyzing the logic of their own placements in relation to their neighbors locally. The assault detection is based on communication features and vehicle GPS locations, both of which are contained in the safety-related messages exchanged with neighbors broadcast on a regular basis. The neighbor lists are exchanged in a distributed, easy manner. There is another information-sharing mechanism, which is the cooperative detection and correction mechanism. In this mechanism, the vehicle calculates and sends its flow value (speed, density, flow, and position information) to the others. The rest of the vehicles also calculate the value of speed, density, flow, and position information. Each vehicle's flow is transmitted to another vehicle. Data will not be accepted with a useful traffic model if the received flow does not match the VANET model flow. This method works well against nodes that communicate incorrect location information. When a rogue node sends bogus information from several identities, honest nodes behind the malicious node disregard it because of their speed. However, this mechanism is insufficient when many attackers provide bogus information.

5. Open Issues and Discussion

Misbehavior detection is a well-studied issue that has spanned two decades of research. The first publication on identifying and rectifying fraudulent data in automotive networks was published by Golle et al. [46, 106]. This work provides an overview of existing VANET misbehavior detection technologies. For road safety and human life, identifying malicious events is critical. This article classifies misbehavior detection techniques according to their detection mode and proclivity for detecting misbehavior.

The first criterion used to classify mechanisms is node-centric or data-centric, a distinction that has been widely utilized in the literature. Data-centric processes only assess the message's credibility and consistency based on its contents. Node-centric techniques are based on a node's behavior and assign a reputation to every VANET participant in the vicinity. Most schemes have proposed combining the two approaches because data-centric and node-centric misbehavior detections are mostly inseparable. Moreover, local-based detection, cooperative detection, and global detection modes are classified in this article. Global-based detection techniques rely on the third-party system and execute detection based on previous network interaction information, which has the advantage of the following processing: using certificate revocation list or blocklist to deal with and punish malicious entities. In the event of a dense network and many honest nodes, cooperative-based detection algorithms are practical. When the frequency of contact between nodes is high, trust-based detection techniques perform well. However, global-based and local-based misbehavior detections face unique obstacles because of VANET's peculiarities. Due to various obstacles, cooperative detection technologies may not produce acceptable, adequate results. In this situation, strategies that rely on accessible information from a single node are local-based detection techniques. Local detection techniques for detecting false beacon or warning signals are globally helpful. Local node information-based detection approaches rely on a single node's information. They are efficient in terms of time because they do not rely on other nodes to identify fake messages. Accurate results for malicious information detection are not possible due to a lack of information from a single node.

Even though particular areas of misbehavior have been addressed, several unsolved problems need to be addressed.

(i) Thresholds in misbehavior detection

Many schemes reviewed in this work mentioned using a threshold concept in misbehavior detection, especially node-based detections. One of the most challenging things of any intrusion detection system is its setting and defining an exact point suitable for different scenarios. It is crucial in misbehavior detection because excessive false positive or false negative rates can create serious difficulties.

(ii) Identification in data-centric detection

Data-centric techniques better detect contradictory data and determine whether data are malicious. Although having correct data is more important than identifying attackers in many systems, data-centric detection may be unable to identify the attacker precisely.

(iii) Privacy in misbehavior detection

While the mechanisms above are essential for identifying misbehavior, they may negatively influence the users' location privacy. That vehicles communicate using short-term pseudonyms and change them frequently to safeguard privacy is a common expectation. The unlinkability between pseudonyms and real identity brings out the difficulty in misbehavior detection and extended processing time. Balancing privacy issues in tracking malicious nodes is still an open issue.

(iv) Misbehavior reporting

The reaction mechanism is absent in most of the detection schemes. However, punishing misbehavior is equally important as finding misbehavior. Reporting misbehavior to the monitoring system is vital. The added benefit of using the back-end could further be dealing with misbehavior nodes and revoking the problematic nodes' certificates. The back-end cannot receive all data received by automobiles due to bandwidth constraints. Finding a balance between transmitting suspicious behavior to the backend to increase attack detection and not wasting bandwidth is an open challenge.

6. Conclusions

This survey provides a comprehensive overview of different approaches to misbehavior detection in VANETs. After reviewing the latest VANET system model, security attributes, and existing attacks based on different targets, the concept of misbehavior and detection modes, including local, cooperative, and global detection, is introduced. Then, misbehavior detection mechanisms established in the recent decade for VANETs are collected and categorized using novel classifications. The categorization includes conventional classifications: node-centric techniques that examine sender attributes to detect malicious messages and data-centric methods that analyze received message semantics based on the detection mode. On this basis, node-centric and data-centric modes are further refined into autonomous and cooperative modes, according to the detection mode in VANET-specific situations. Finally, several remaining challenges and open issues in VANET misbehavior detection are identified, leading to a new study line. Our research serves as one step closer toward designing and constructing a secure VANET system for participants away from malicious behaviors.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partially supported by the National Key Research and Development Program of China (2020YFB1600302), Young Scientists Fund of the National Natural Science Foundation of China (52002013), and China Postdoctoral Science Foundation (BX20200036 and 2020M680298).

References

[1] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[2] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and Solutions for Cellular Based V2X Communications," *IEEE Communications Surveys & Tutorials*, vol. 23, 2020.

[3] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[4] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1–6, Tiruchengode, India, July 2013.

[5] 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, 2020.

[6] S. Gyawali and Y. Qian, "Misbehavior detection using machine learning in vehicular communication networks," in *Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, Shanghai, China, May 2019.

[7] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, 2018.

[8] Z. Yang, K. Zhang, L. Lei, and K. Zheng, "A novel classifier exploiting mobility behaviors for Sybil detection in connected vehicle systems," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2626–2636, 2018.

[9] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[10] 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.

[11] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: a comprehensive survey," *Computers & Security*, vol. 89, Article ID 101664, 2020.

[12] B. Mishra, P. Nayak, S. Behera, and D. Jena, "Security in vehicular adhoc networks: a survey," in *Proceedings of the 2011 International Conference on Communication, Computing & Security*, pp. 590–595, NY, USA, February 2011.

[13] M. S. Al-Kahtani, "Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs)," in *Proceedings of the 2012 6th international conference on signal processing and communication systems*, pp. 1–9, Gold Coast, QLD, Australia, December 2012.

[14] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[15] A. Shamir, "Identity-based cryptosystems and signature schemes," *Workshop on the Theory and Application of Cryptographic Techniques*, vol. 196, pp. 47–53, 1984.

[16] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 246–250, Phoenix, AZ, USA, April 2008.

[17] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[18] X. Yao, X. Han, and X. Du, "A light-weight certificate-less public key cryptography scheme based on ECC," in *Proceedings of the 2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, Shanghai, China, August 2014.

[19] B. Brecht and T. Hehn, "A security credential management system for V2X communications," in *Connected Vehicles: Intelligent Transportation Systems*, R. Miucic, Ed., Springer International Publishing, Cham, pp. 83–115, 2019.

[20] Y. Zhao, Y. Hou, Y. Chen, S. Kumar, and F. Deng, "An Efficient Certificateless Public Key Encryption with equality Test toward Internet of Vehicles," *Transactions on Emerging Telecommunications Technologies*, Article ID e3812, 2019.

[21] D. Rajalakshmi and K. Meena, "A Survey of intrusion detection with higher malicious misbehavior detection in Manet," *International Journal of Civil Engineering and Technology*, vol. 8, no. 10, pp. 99–110, 2017.

[22] A. Boualouache and T. Engel, "A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and beyond Vehicular Networks," 2022, https://arxiv.org/abs/2201.10500.

[23] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2020.

[24] 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.

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

[26] T. Bouali, S.-M. Senouci, and H. Sedjelmaci, "A distributed detection and prevention scheme from malicious nodes in vehicular networks," *International Journal of Communication Systems*, vol. 29, no. 10, pp. 1683–1704, 2016.

[27] S. K. Harit, G. Singh, and N. Tyagi, "Fox-hole Model for Data-Centric Misbehaviour Detection in VANETs," in *Proceedings of the 2012 Third International Conference on Computer and Communication Technology*, pp. 271–277, Allahabad, India, November 2012.

[28] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, "VeReMi extension: a dataset for comparable evaluation of misbehavior detection in VANETs," in *Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.

[29] Y. Wang and F. Li, "Vehicular ad hoc networks," in *Guide to Wireless Ad Hoc Networks*, pp. 503–525, Springer, Berlin, Germany, 2009.

[30] A.-S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, CRC Press, Boca Raton, Florida, USA, 2016.

[31] Y. Yang, Z. Yuan, J. Chen, and M. Guo, "Assessment of osculating value method based on entropy weight to transportation energy conservation and emission reduction," *Environmental Engineering & Management Journal (EEMJ)*, vol. 16, no. 10, 2017.

[32] M. S. Sheikh and J. Liang, "A Comprehensive Survey on VANET Security Services in Traffic Management System," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 2423915, 2019.

[33] J. Grover, M. S. Gaur, V. Laxmi, and R. K. Tiwari, "Detection of incorrect position information using speed and time span verification in VANET," in *Proceedings of the Fifth International Conference on Security of Information and Networks*, pp. 53–59, NY, USA, October 2012.

[34] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: specification of cooperative awareness basic service," *ETSI EN*, vol. 637, no. 2, 2014.

[35] "Intelligent transport systems; vehicular communications; basic set of applications; Part 3: specification of decentralized environmental notification basic service," *ETSI EN*, vol. 637, no. 3, 2014.

[36] R. Miucic and S. Bai, "Cooperative vehicle to pedestrian safety system," in *Connected Vehicles*, pp. 181–201, Springer, Berlin, Germany, 2019.

[37] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE communications surveys & tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[38] G. Samara, W. Alsalihy, and R. Suress, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," in *Proceedings of the 4th International Conference on New Trends in Information Science and Service Science*, Gyeongju, Korea (South), May 2010.

[39] A. Rawat, S. Sharma, and R. Sushil, "VANET: security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[40] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications*, vol. 5, no. 5, p. 95, 2013.

[41] 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.

[42] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 261–274, 2016.

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

[44] M. Abu Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, Article ID 1550147718815054, 2018.

[45] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, Article ID 101823, 2019.

[46] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 29–37, Philadelphia, PA, USA, October 2004.

[47] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[48] Z. Yuan, K. He, and Y. Yang, "A roadway safety Sustainable approach: Modeling for real-time traffic crash with limited data and its reliability verification," *Journal of Advanced Transportation*, vol. 2022, Article ID 1570521, 2022.

[49] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: its architecture, design, and characteristics," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 4, pp. 504–518, 2010.

[50] T. S. Rappaport, *Wireless communications: principles and practice*, Vol. 2, prentice hall PTR, NJ, USA, 1996.

[51] J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, pp. 894–911, IGI global, Hershey, Pennsylvania, 2011.

[52] Y. Qian and N. Moayeri, "Design of secure and application-oriented VANETs," in *Proceedings of the VTC Spring 2008-IEEE Vehicular Technology Conference*, pp. 2794–2799, Marina Bay, Singapore, May 2008.

[53] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for VANET," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1–6, NY, USA, August 2018.

[54] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," in *Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, vol. 3, pp. 261–265, Zhangjiajie, China, May 2012.

[55] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in *Proceedings of the 2012 Computing, Communications and Applications Conference*, pp. 345–350, Hong Kong, China, January 2012.

[56] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.

[57] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, 2012.

[58] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: a survey of current solutions and future research opportunities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553–2571, 2020.

[59] N. Yang, "A similarity based trust and reputation management framework for VANETs," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, pp. 25–34, 2013.

[60] 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.

[61] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in VANETs," *International Journal of Computer Theory and Engineering*, vol. 4, no. 6, p. 1007, 2012.

[62] S. Dixit, K. Joshi, and N. Joshi, "A review: black hole and gray hole attack in MANET," *International Journal of Future Generation Communication and Networking*, vol. 8, pp. 287–294, Aug. 2015.

[63] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[64] S. Benkerdagh and C. Duvallet, "Cluster-based emergency message dissemination strategy for VANET using V2V communication," *International Journal of Communication Systems*, vol. 32, no. 5, Article ID e3897, 2019.

[65] I. A. Sumra, H. B. Hasbullah, I. Ahmad, and D. M. Alghazzawi, "Classification of attacks in vehicular ad hoc network (VANET)," International Information Institute (Tokyo)," *Information*, vol. 16, no. 5, p. 2995, 2013.

[66] M. Hafiz, "A pattern language for developing privacy enhancing technologies," *Software: Practice and Experience*, vol. 43, no. 7, pp. 769–787, 2013.

[67] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle attack to the HTTPS protocol," *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78–81, 2009.

[68] B. Di Ying, D. Makrakis, and H. T. Mouftah, "Anti-traffic analysis attack for location privacy in WSNs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, pp. 1–15, 2014.

[69] S. Abbas, M. Faisal, H. Ur Rahman, M. Z. Khan, M. Merabti, and A. ur R. Khan, "Masquerading attacks detection in mobile ad hoc networks," *IEEE Access*, vol. 6, pp. 55013–55025, 2018.

[70] N.-W. Lo and H.-C. Tsai, "Illusion Attack on VANET Applications-A Message Plausibility Problem," in *Proceedings of the 2007 IEEE globecom workshops*, pp. 1–8, Washington, DC, USA, November 2007.

[71] T. Karimireddy and A. G. A. Bakshi, "A hybrid security framework for the vehicular communications in VANET," in *Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, p. 1929, Chennai, India, March 2016.

[72] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A Sybil attack detection approach using neighboring vehicles in VANET," in *Proceedings of the 4th International Conference on Security of Information and Networks*, pp. 151–158, NY, USA, November 2011.

[73] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.

[74] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[75] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, pp. 1976–1986, 2003.

[76] A. K. Mishra and A. K. Turuk, "Residual energy-based replica detection scheme for mobile wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 4, pp. 637–648, 2015.

[77] V. Manjula and C. Chellappan, "The replication attack in wireless sensor networks: analysis and defenses," in *Advances in Networks and Communications*pp. 169–178, Berlin, Heidelberg, Germany, 2011.

[78] A. M. Holkar, N. S. Holkar, and D. Nitnawwre, "Investigative analysis of repudiation attack on MANET with different routing protocols," *Int J Emerg Trends Technol Comput Sci (IJETTCS)*, vol. 2, no. 3, 2013.

[79] T. Leinmuller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," in *Proceedings of the 2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services*, pp. 84–91, Obergurgl, Austria, January 2007.

[80] M. Amoozadeh, A. Raghuramu, C. N. Chuah et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[81] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC)," in *Proceedings of the 2017 IEEE Vehicular Networking Conference (VNC)*, pp. 45–52, Turin, Italy, November 2017.

[82] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds," in *Proceedings of the 2014 IEEE world forum on internet of things (WF-IoT)*, pp. 241–246, Seoul, Korea (South), March 2014.

[83] A. M. Vegni, M. Biagi, and R. Cusani, "Smart Vehicles, Technologies and Main Applications in Vehicular Ad Hoc Networks," *Vehicular technologies-deployment and applications*, pp. 3–20, Intechopen, UK, 2013.

[84] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous VANETs," in *Proceedings of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and mobile Systems*, pp. 106–115, NY, USA, October 2009.

[85] D. A. Rivas, J. M. Barceló-Ordinas, M. G. Zapata, and J. D. Morillo-Pozo, "Security on VANETs: privacy, misbehaving nodes, false information and secure data aggregation," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1942–1955, 2011.

[86] A. K. Malhi and S. G. Batra, *A Framework for Secure Vehicular Communication Systems*, PhD Thesis, University in Patiala, Punjab, India, 2016.

[87] F. Kargl, P. Papadimitratos, L. Buttyan et al., "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.

[88] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: identity and credential management in vehicular communication systems," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63–69, 2015.

[89] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[90] I. Bilogrevic, M. H. Manshaei, M. Raya, and J.-P. Hubaux, "Optimal revocations in ephemeral networks: a game-theoretic framework," in *Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 21–30, Avignon, France, June 2010.

[91] B. Liu, J. T. Chiang, and Y.-C. Hu, "Limits on revocation in VANETs," in *Proceedings of the 8th International Conference on Applied Cryptography and Network Security*, pp. 38–52, Berlin, Heidelberg, June 2010.

[92] A. Behfarnia and A. Eslami, "Misbehavior detection in ephemeral networks: a local voting game in presence of uncertainty," *IEEE Access*, vol. 7, pp. 184629–184642, 2019.

[93] J.-P. Monteuuis, J. Petit, J. Zhang, H. Labiod, S. Mafrica, and A. Servel, "Attacker model for connected and automated vehicles," in *Proceedings of the ACM Computer Science in Car Symposium*, Munich, Germany, September 2018.

[94] J. Petit, B. Stottelaar, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," *Black Hat Europe*, vol. 13, 2015.

[95] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[96] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "DARTS: Deceiving Autonomous Cars with Toxic Signs," 2018, http://arxiv.org/abs/1802.06430.

[97] J. Petit, M. Feiri, and F. Kargl, "Revisiting attacker model for smart vehicles," in *Proceedings of the 2014 IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC 2014)*, pp. 1–5, Vancouver, BC, Canada, September 2014.

[98] M. Jedh, L. ben Othmane, N. Ahmed, and B. Bhargava, "Detection of Message Injection Attacks onto the CAN Bus Using Similarity of Successive Messages-Sequence Graphs," 2021, https://arxiv.org/abs/2104.03763.

[99] U. D. Gandhi and R. Keerthana, "Request response detection algorithm for detecting DoS attack in VANET," in *Proceedings of the 2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, pp. 192–194, Faridabad, India, February 2014.

[100] K. D. Thilak and A. Amuthan, "DoS attack on VANET routing and possible defending solutions-A survey," in *Proceedings of the 2016 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1–7, Chennai, India, February 2016.

[101] 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, Coimbatore, India, July 2020.

[102] Z. Ye, D. Zhang, and Z.-G. Wu, "Adaptive event-based tracking control of unmanned marine vehicle systems with DoS attack," *Journal of the Franklin Institute*, vol. 358, no. 3, pp. 1915–1939, 2021.

[103] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Proceedings of the 2010 Seventh International Conference on Wireless On-Demand Network Systems and Services (WONS)*, pp. 176–183, Kranjska Gora, Slovenia, February 2010.

[104] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: a survey," *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228–255, 2014.

[105] B. Ying and D. Makrakis, "Pseudonym changes scheme based on candidate-location-list in vehicular networks," in *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, pp. 7292–7297, UK, June 2015.

[106] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 29–37, NY, USA, October 2004.

[107] M. Raya, *Data-centric Trust in Ephemeral Networks*, EPFL, Lausanne, Switzerland, 2009.

[108] A. Azab, R. Layton, M. Alazab, and J. Oliver, "Mining Malware to Detect variants," in *Proceedings of the 2014 fifth Cybercrime and Trustworthy Computing Conference*, pp. 44–53, Auckland, New Zealand, November 2014.

[109] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular communications*, vol. 12, pp. 138–164, 2018.

[110] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Al-Rimy, F. Saeed, and T. Al-Hadhrami, "Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 159119–159140, 2019.

[111] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing*, vol. 75, pp. 712–727, 2019.

[112] C. Kruegel and G. Vigna, "Anomaly detection of web-based attacks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 251–261, NY, USA, October 2003.

[113] J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo, "Anomaly detection methods in wired networks: a survey and taxonomy," *Computer Communications*, vol. 27, no. 16, pp. 1569–1584, 2004.

[114] A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: a survey," in *Managing Cyber Threats*, pp. 19–78, Springer, Berlin, Germany, 2005.

[115] F. Sabahi and A. Movaghar, "Intrusion Detection: A survey," in *Proccedings of the 2008 Third International Conference on Systems and Networks Communications*, pp. 23–26, Sliema, Malta, October 2008.

[116] S. Tzeng, S. Horng, T. Li, X. Wang, P. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2015.

[117] H. Zhang, S. Dai, Y. Li, and W. Zhang, "Real-time distributed-random-forest-based network intrusion detection system using Apache spark," in *Proccedings of the 2018 IEEE 37th International Performance Computing and*

Communications Conference (IPCCC), pp. 1–7, Orlando, FL, USA, November 2018.

[118] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014.

[119] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proccedings of the 2010 IEEE International Conference on Communications Workshops*, pp. 1–5, Cape Town, South Africa., May 2010.

[120] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET," in *Proccedings of the 2009 Second International Workshop on Computer Science and Engineering*, vol. 2, pp. 160–165, Qingdao, China, October 2009.

[121] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in *Proccedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, pp. 422–432, Nice, France, September 2007.

[122] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: distributed key management for security," *2nd OLSR Interop/Workshop, Palaiseau, France*, vol. 14, pp. 1–5, 2005.

[123] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks," in *Proccedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*, pp. 1–8, PA, USA, August 2007.

[124] M. Rahbari and M. A. J. Jamali, "Efficient detection of Sybil attack based on cryptography in VANET," 2011, https://arxiv.org/abs/1112.2257.

[125] J. Soryal and T. Saadawi, "DoS attack detection in Internet-connected vehicles," in *Proccedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 7–13, Las Vegas, NV, USA, December 2013.

[126] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET," *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, 2013, http://link.springer.com/10.1007/s11277-013-1161-5.

[127] K. Verma and H. Hasbullah, "Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET," *Security and Communication Networks*, vol. 8, no. 5, pp. 864–878, 2015.

[128] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)," in *Proccedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 237–240, Chennai, India, February 2013.

[129] 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.

[130] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 377–385, 2006.

[131] B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, Los Angeles CA USA, September 2006.

[132] Y. Hao, J. Tang, and Y. Cheng, "Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs," in *Proceedings of the 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pp. 1–5, Houston, Texas, USA, December 2011.

[133] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," in *Proceedings of the MILCOM 2009 - 2009 IEEE Military Communications Conference*, pp. 1–7http://ieeexplore.ieee.org/document/5379844/, Boston, MA, USA, October 2009.

[134] H. Sedjelmaci, S. M. Senouci, and M. A. Abu-Rgheff, "An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks," *IEEE Internet of Things Journal*, vol. 1, no. 6, pp. 570–577, 2014.

[135] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: a statistical approach to rogue node detection," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, 2015.

[136] B. Lee, E. Jeong, and I. Jung, "A DTSA (detection technique against a Sybil attack) protocol using SKC (Session key based certificate) on VANET," *International Journal of Security and Its Applications*, vol. 7, no. 3, p. 10, 2013.

[137] X. Feng, C. Li, D. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, 2017.

[138] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, 2011.

[139] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613–3634, 2020.

[140] C. A. Kerrache, N. Lagraa, C. T. Ca Lafate, J. C. Ca No, and P. Manzoni, "T-VNets: a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS," *Computer Communications*, vol. 93, no. 1, pp. 68–83, 2016.

[141] 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.

[142] 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.

[143] 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. 1–17, 2018.

[144] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Countermeasures to prevent misbehaviour in VANETs," *Journal of Universal Computer Science*, vol. 18, no. 6, pp. 857–873, 2012.

[145] C. Chen, X. Wang, W. Han, and B. Zang, "A Robust detection of the Sybil attack in urban VANETs," in *Proceedings of the 2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, pp. 270–276, Montreal, Quebec, Canada, June 2009, http://ieeexplore.ieee.org/document/5158865/.

[146] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure

vehicular networks," *Computers & Electrical Engineering*, vol. 43, pp. 33–47, 2015.

[147] J. Kamel, A. Kaiser, I. Ben Jemaa, P. Cincilla, and P. Urien, "Feasibility study of misbehavior detection mechanisms in cooperative intelligent transport systems (C-its)," in *Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Porto, Portugal, June 2018.

[148] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, 2006.

[149] M. Krzysztoń and M. Marks, "Simulation of watchdog placement for cooperative anomaly detection in Bluetooth mesh intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, Article ID 102041, 2020.

[150] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pp. 255–265, Boston Massachusetts USA, August 2000.

[151] J. Baburajan and J. Prajapati, "A review paper on watchdog mechanism in wireless sensor network to eliminate false malicious node detection," *Int. J. Res. Eng. Technol*, vol. 3, no. 1, pp. 381–384, 2014.

[152] D. John and R. P. Haroon, "Selfish node Isolation & Incentivation using Progressive thresholds," *International Journal on Network Security*, vol. 5, no. 1, p. 68, 2014.

[153] S. Senthilkumar and J. William, "A survey on reputation based selfish node detection techniques in mobile Ad Hoc network," *Journal of Theoretical and Applied Information Technology*, vol. 60, no. 2, pp. 208–215, 2014.

[154] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer communications*, vol. 31, no. 12, pp. 2883–2897, 2008.

[155] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of Intelligent Transportation Systems Research*, vol. 10, no. 1, pp. 11–21, 2012.

[156] J. Zacharias and S. Fröschle, "Misbehavior Detection System in VANETs Using Local Traffic Density," in *Proceedings of the 2018 IEEE Vehicular Networking Conference (VNC)*, pp. 1–4, Taipei, Taiwan, December 2018.

[157] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Enhancing misbehavior detection in 5G vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9417–9430, Sep. 2020.

[158] L. Li, Y. Yang, Z. Yuan, and Z. Chen, "A spatial-temporal approach for traffic status analysis and prediction based on Bi-LSTM structure," *Modern Physics Letters B*, vol. 35, no. 31, Article ID 2150481, 2021.

[159] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs," *IEEE Transactions on Wireless Communications*, vol. 9, no. 5, pp. 1661–1675, 2010.

[160] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718–3731, 2016.

[161] T. C. Swetha Priya and I. R. Prakash Reddy, "channel aware detection of selective forwarding attacks in wireless sensor networks," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[162] H. Zhu, Z. Zhang, J. Du, S. Luo, and Y. Xin, "Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 11, Article ID 155014771881504, 2018.

[163] O. Puñal, A. Aguiar, and J. Gross, "VANETs we trust? characterizing RF jamming in vehicular networks," in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, pp. 83–92, New York, NY, USA, June 2012.

[164] A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of radio interference attacks in VANET," in *Proceedings of the GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*, pp. 1–5, Honolulu, HI, USA, December 2009.

[165] 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.

[166] G. S. Kasturi, A. Jain, and J. Singh, "Detection and classification of radio frequency jamming attacks using machine learning," *Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl*, vol. 11, no. 4, pp. 49–62, 2020.

[167] V. Nallarasan and K. Kottursamy, "Cognitive radio jamming attack detection using an autoencoder for CRIoT network," *Wireless Personal Communications*, pp. 1–17, 2021.

[168] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*, pp. 107–121, Springer, Berlin, Germany, 2002.

[169] G. F. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: a survey," *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 319–332, 2006.

[170] K. R. Abirami and M. G. Sumithra, "Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection," *Cluster Computing*, vol. 22, no. 6, pp. 13307–13316, 2019.

[171] T. HJ. Kim, A. Studer, R. Dubey et al., "VANET alert endorsement using multi-source filters," in *Proceedings of the Seventh ACM International Workshop on VehiculAr Inter-NETworking*, pp. 51–60, Chicago Illinois USA, September 2010.

[172] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi, and A. Perrig, "Efficient and secure threshold-based event validation for VANETs," in *Proceedings of the Fourth ACM Conference on Wireless Network Security*, pp. 163–174, Hamburg Germany, June 2011.

[173] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[174] T. Leinmueller, R. Schmidt, and A. Held, "Cooperative Position Verification - Defending against Roadside Attackers 2.0," in *Proceedings of the 17th ITS World Congress*, p. 8, Busan , Korea, South, October 2010.

[175] R. Talreja and V. Jethani, "A vote based system to detect misbehaving nodes in MANETs," in *Proceedings of the 2014 IEEE International Advance Computing Conference (IACC)*, pp. 391–394, Gurgaon, India, February 2014.

[176] M. B. Channappagoudar and P. Venkataram, "Mobile Agent Based Node Monitoring Protocol for MANETs," in *Proceedings of the 2013 National Conference on Communications (NCC)*, pp. 1–5, New Delhi, India, February 2013.

[177] L. Mendiboure, M. A. Chalouf, and F. Krief, "Survey on blockchain-based applications in internet of vehicles,"

Computers & Electrical Engineering, vol. 84, Article ID 106646, 2020.

[178] M. Al-Ali, H. Al-Mohammed, and M. Alkaeed, "Reputation Based Traffic Event Validation and Vehicle Authentication Using Blockchain Technology," in *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Doha, Qatar, February 2020.

[179] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Networks*, vol. 3, no. 4, pp. 289–302, 2010.

[180] R. W. Van der Heijden, F. Kargl, and O. M. Abu-Sharkh, "Enhanced position verification for VANETs using subjective logic," in *Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–7, Montreal, QC, Canada, September 2016.

[181] F. Cheng, C. Wang, X. Zhang, and Y. Yang, "A Local-Neighborhood Information Based Overlapping Community Detection Algorithm for Large-Scale Complex Networks," *IEEE/ACM Transactions on Networking*, vol. 29, 2020.

[182] H. Hamed, A. Keshavarz-Haddad, and S. G. Haghighi, "Sybil attack detection in urban VANETs based on RSU support," in *Proceedings of the Electrical Engineering (ICEE) Iranian Conference on*, pp. 602–606, Mashhad, Iran, May 2018.

[183] P. Sun, N. AlJeri, and A. Boukerche, "A novel passive road side unit detection scheme in vehicular networks," in *Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–5, Singapore, December 2017.

[184] S. Ruj, M. A. Cavenaghi, H. Zhen, A. Nayak, and I. Stojmenovic, "On Data-Centric Misbehavior Detection in VANETs," in *Proceedings of the Vehicular Technology Conference IEEE*, San Francisco, CA, USA, September 2011.

[185] J. Guo, X. Li, Z. Liu et al., "TROVE: a context-awareness trust model for VANETs using reinforcement learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6647–6662, 2020.

[186] N. Bißmeyer, K. H. Schröder, J. Petit, S. Mauthofer, and K. M. Bayarou, "Short Paper: Experimental Analysis of Misbehavior Detection and Prevention in VANETs," in *Proceedings of the 2013 IEEE Vehicular Networking Conference*, pp. 198–201, Boston, MA, USA, December 2013.

[187] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 1264–1276, 2020.

[188] M. Arshad, M. Khalid, N. Ahmad, W. Khalid, D. Shawar, and Y. Cao, "Beacon trust management system and fake data detection in vehicular adhoc network," *IET Intelligent Transport Systems*, vol. 13, 2018.

[189] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, M. A. Rassam, F. Saeed, and M. Alsaedi, "Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages," *Vehicular Communications*, vol. 20, Article ID 100186, Dec. 2019.

[190] A. A. Pouyan and M. Alimohammadi, "Sybil attack detection in vehicular networks," *Computer Science and Information Technology*, vol. 2, no. 4, pp. 197–202, 2014.

[191] M. Sun, M. Li, and R. Gerdes, "A data trust framework for VANETs enabling false data detection and secure vehicle tracking," in *Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, Las Vegas, NV, USA, October 2017.

[192] S. So, J. Petit, and D. Starobinski, "Physical layer plausibility checks for misbehavior detection in V2X networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 84–93, Miami Florida, May 2019.

[193] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, 2013.

[194] S. Rakhi and K. R. Shobha, "Performance analysis of an efficient data-centric misbehavior detection technique for vehicular networks," in *International Conference on Computer Networks and Communication Technologies*, S. Smys, R. Bestak, J. I.-Z. Chen, and I. Kotuliak, Eds., vol. 15, pp. 321–331, Springer, Singapore, 2019.

[195] M. Ranaweera, A. Seneviratne, D. Rey, M. Saberi, and V. V. Dixit, "Anomalous Data Detection in Vehicular Networks Using Traffic Flow Theory," in *Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–5, Honolulu, HI, USA, September 2019.

[196] Y. Yang, K. He, Y. Wang, Z. Yuan, Y. Yin, and M. Guo, "Identification of dynamic traffic crash risk for cross-area freeways based on statistical and machine learning methods," *Physica A: Statistical Mechanics and Its Applications*, vol. 595, Article ID 127083, 2022.

[197] A. Kumar, S. Mehta, and D. Vijaykeerthy, "An Introduction to Adversarial Machine Learning," *Big Data Analytics*, vol. 10721, pp. 293–299, 2017.

[198] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," 2022, http://arxiv.org/abs/1804.06701.

[199] I. Mahmoudi, J. Kamel, I. Ben-Jemaa, A. Kaiser, and P. Urien, "Towards a Reliable Machine Learning Based Global Misbehavior Detection in C-ITS: Model Evaluation Approach," 2019, https://hal.archives-ouvertes.fr/hal-02353893.

[200] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2022.

[201] J. Kamel, F. Haidar, I. B. Jemaa, A. Kaiser, B. Lonc, and P. Urien, "A misbehavior authority system for Sybil attack detection in c-its," in *Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 1117–1123, NY, USA, October 2019.

[202] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," in *Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–6, Riyadh, Saudi Arabia, May 2019.

[203] 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, Athens Greece, July 2021.