Hindawi
Scientific Programming
Volume 2020, Article ID 8831611, 21 pages
https://doi.org/10.1155/2020/8831611

Research Article

A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks

Muhammad Haleem Junejo,[1] **Ab Al-Hadi Ab Rahman**,[1] **Riaz Ahmed Shaikh**,[2] **Kamaludin Mohamad Yusof**,[1] **Imran Memon**,[3] **Hadiqua Fazal**,[3] **and Dileep Kumar**[4]

[1]*Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Skudai 81310, Johor, Malaysia*
[2]*Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[3]*Department of Computer Science, Bahria University, Karachi Campus, Sindh, Pakistan*
[4]*State Key Laboratory of Industrial Control Technology, College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China*

Correspondence should be addressed to Dileep Kumar; dk2kes21@gmail.com

Received 3 September 2020; Revised 6 November 2020; Accepted 24 November 2020; Published 11 December 2020

Academic Editor: Shah Nazir

The Internet of things (IoT) and advancements of wireless technology have evolved intelligent transport systems to integrate billion of smart objects ready to connect to the Internet. The modern era of the Internet of things (IoT) has brought significant development in vehicular ad hoc networks (VANETs) which transformed the conventional VANET into the Internet of Vehicle (IoV) to improve road safety and diminished road congestion. However, security threats are increasing due to dependency on infrastructure, computing, dynamic nature, and control technologies of VANET. The security threats of VANETs could be addressed comprehensively by increasing trustworthiness on the message received and transmitting node. Conversely, the presence of dishonest vehicles, for instance, Man in the Middle (MiTM) attackers, in the network sharing malicious content could be posed as a severe threat to VANET. Thus, increasing trustworthiness among nodes can lead to increased authenticity, privacy, accuracy, security, and trusted information sharing in the VANET. In this paper, a lightweight trust model is proposed, presented model identifying dishonest nodes and revoking its credential in the MiTM attack scenario. Furthermore, addressing the privacy and security requirement, the pseudonym scheme is used. All nodes in the VANET established trust provided by initially RSU, which is a trusted source in the network. Extensive experiments are conducted based on a variety of network scenarios to evaluate the accuracy and performance of the presented lightweight trust model. In terms of recall, precision, and *F*-score, our presented model significantly outperformed compared to MARINE. The simulation results have validated that the proposed lightweight model realized a high trust level with 40% of MiTM attackers and in terms of *F*-score 95%, whereas the MARINE model has 90%, which leads to the model to attain high detection accuracy.

1. Introduction

In our daily lives, the transport system plays an undeniable role. It is projected that this increasing number of vehicles on roads reaches up to 2 billion or more in the coming decades [1]. As a consequence, we encounter an unfortunate rise in accidents, traffic jams, congestion, pollution, and so forth. The World Health Organization (WHO) has released a report of 1.35 million deaths due to road accidents [2, 3]. To improve transport efficiency and security, the vehicular ad hoc networks (VANETs) present the foundation of the smart city paradigm and Intelligent Transportation Systems (ITSs) [4–6]. The Internet of things (IoT) is a novel concept in the current era that is evolved to integrate billion of smart objects ready to connect to the Internet [7]. The newest technologies have enabled smart object, remote devices, and wireless and wired networks to be part of IoT. The IoT combines all electronic, mechanical, and computing devices

to part of the Internet. The vehicular ad hoc networks (VANETs) connected to IoT bring the concept of the Internet of Vehicles (IoV) [8–10]. Internet of VANET is application of IoT to improve the urban transport system, reduce accidents, and enhance the traffic monitoring system [10]. The main features of IoV are high creditability, controllability, manageability, and operationalization efficiency [7, 11]. The VANETs are considered as subclasses of Mobile Ad Hoc Networks (MANETs) [12–14]. Under the umbrella of VANET, vehicles are capable of communicating with other vehicles and the roadside units by dedicated short-range communication (DSRC) radiofrequency. Particularly, in VANET, two types of communication are established. Firstly, it is among vehicle-to-vehicle (V2V) communication and secondly, in between vehicles-to-infrastructure (V2I) communication. The primary nodes in VANETs are smart vehicles and Road Side Units (RSU) that are communicating among each other to exchange safety, security, and infotainment information.

In a situation where the exchanged information is incorrect, it leads to some counterproductive; consequently, accidents and traffic congestion would increase. Over the last decade, promising advancements have been made in the field of VANET [15]. Accordingly, the scientific community has contributed a lot to overcome the challenges in the scope of security, safety, and engineering design. In the context of effectively using the VANETs, the most important aspect is to deal with the safety, security, and privacy parameters.

To that respect, several solutions have been proposed by the research community to foster security in VANETs [16–20]. In those solutions, the authors suggested, as a solution, the use of traditional cryptography which utilizes the Public Key Infrastructure (PKI) and certificates to achieve security in the network. However, these solutions suffer from several factors that reduce network efficiency in VANETs. These factors include

(i) The mobility of vehicles randomly dispersed throughout a network with low- and high-speed vehicles

(ii) The presence of a roadside unit or network infrastructure in a rural area is not assured all the time

(iii) The propagation of untrusted messages in VANET in case of an inside attack is a result of a compromised cryptographic solution

The cryptographic-based solution can protect VANETs from outside attacks. However, it is incapable of assuring message reliability and quality, which may lead to undesirable consequences. This leads to the emergence of trust-based solutions, which aim to protect VANETs from inside attacks [21–24].

Trust, in the VANET, is described as the confidence of one (vehicle) to the other for performing a requirement or a set of conditions [19, 20]. In VANET, the trust is created between two or more vehicles based on the intercommunication. Once the message is received, the assessor node computes the trust based on numerous factors, which are the vehicle's previous communication, reputation in the network, and neighbors' recommendations regarding a specific vehicle.

It must be noted that, due to extremely mobile and randomly distributed vehicles, the trust was established for a short duration [12, 25, 26]. Therefore, it is challenging to creating, calculating, quantifying, and assessing the trust in received messages based on varied factors in a limited time. The trust, as a method to attain security in VANETs, is in its early stages of development. The trust models (TM) are fixed within vehicles to assess the reliability, accuracy, and authenticity of received messages. The TMs confirm the broadcast of trusted information in the network by retracting both dishonest nodes and malicious messages.

These challenges are imposed because of the ephemeral nature of VANETs [27]. In the literature, most of the existing trust models did not properly address security control to countermeasure the security vulnerability and attacks in VANET. To cover this gap, the trust metric value should be taken into account for multiple factors and for protection against the attacks. The recently designed architecture of VANET trust models encompasses the key new features to reduce the effect of security attacks, which are the ability to configure, control, and combine security services. Vehicles, RSU, and other node parts of the VANET network should be trusted and reliable. To identify the malicious, misbehaving, and compromised node in the VANET network is challenging due to the aforementioned points. Furthermore, it is an open issue to evaluate the trustworthiness of a node. The safety of human lives can be lost in case of any sort of miscommunication in VANET. Several parameters need to be considered before trusting the received message from another node based on the following questions:

(1) What is the reliability of a node before transmitting a critical message?

(2) How criteria are defined on the basis of that the trustworthiness of the node?

(3) How to detect the misbehavior in calculating the trustworthiness of a vehicle?

To address the security challenges required by VANETs are availability, authentication, confidentiality, integrity, privacy, nonrepudiation, and others. The security threats of VANETs could be addressed comprehensively by increasing trustworthiness on the message received and transmitting node. In this paper, we propose a trust management model for vehicular ad hoc networks. The presented model consists of two main blocks: Trust Estimation Model and Decision Model.

(i) The trust estimation in the proposed model is based on five parameters, namely, Location Closeness, Data Integrity, Authentication, Time Stamp Verification, and Peer Alert Message. The trust estimation part calculates the threshold value on the data received from all of five parameters.

(ii) The decision model received the trust value from the trust estimation block to decide whether to process the message or discard it on the basis of the threshold

value. If the trust value is less than the threshold value a TRUE message is generated, and the decision box accepts the value send an update to a database and takes an application-specific decision. In case, if the threshold value exceeds, the threshold value message is discarded and the FALSE message is generated. On the basis of false generated message value, invoke/revoke procedure decide to invoke or revoke the message.

The main contribution of our presented model is as follows:

(1) An attack-resistant trust model for VANETs that efficiently addresses the privacy issue by using the pseudonym scheme

(2) Propose a trust model, identifying dishonest nodes and revoking its credential in a MiTM attack scenario

(3) The RSU is a trusted source in the network, RSU assigns an initial trusted value in the coverage area and based on the presented scenario generates a peer alert message to inform vehicle in the coverage area about the presence of a malicious vehicle.

This paper is organized as follows. In Section 2, related work is presented. Section 3 discusses the architecture of VANET and security threats. Section 4 represents the trust model in detail, and in Section 5, we present the evaluation of the presented trust model in the presence of four variant of MiTM attacks scenario. In Section 6, conclusion of the paper is demonstrated.

2. Related Work

The trust established between the nodes can be classified into two:

(1) Infrastructure based

(2) Self-organizing

Infrastructure trust is based on the certificates carried by each vehicle in the network, while the self-organizing as the term is quite self-explanatory. Meaning that the self-organizing is based on the trust that is directly between two nodes, indirect between the nodes, and a combination of direct and indirect is termed as a hybrid. In VANET, the trust is calculated on a node or the received message. The trust calculation can be centralized or distributed based on the environment and the infrastructure used.

In VANET, the TMs are divided into three distinct classes:

(1) Data-oriented

(2) Entity-oriented

(3) Hybrid

The purpose of entity-oriented (EO) is to remove dishonest vehicles by assessing the reliability of the node. The data-oriented (DO) evaluates the trust in the received messages (data). And, finally, the hybrid trust models (HTM) calculation is based on both vehicle and data for the trust creation.

2.1. Data-Oriented Trust Model. In recent studies, few trust models are proposed for data-oriented trust calculation. In DO, the calculation of trust is performed on the trustworthiness of the received messages.

A framework proposed by [28] on data-centric trust creation is based on location and time. The authors' approach is based on the evaluator node (EV) that initially receives data from vehicles in the area and then allocates weights to each received data based on two factors: location and time. The proposed frame is not well suited to dynamic and sparse environments as trust is computed all the way, and data is received at a node. In his approach, the author utilized several decision logics, specifically weighted voting, Bayesian inference, and Dempster–Shafer Theory. He concludes that Bayesian inference achieved better results the Dempster–Shafer based on multiple events. The shortcoming of the proposed scheme that it is appropriate only in a condition when there is adequate evidence is available in favor or against a given scenario for a particular event [29].

Gurung et al. [30], in their proposed trust model, evaluate the trustworthiness of the message based on multiple factors such as context similarity, content conflict, and routine similarity. In their conclusion of the paper, the author concluded that the proposed trust model meets the requirements of the dynamic of VANETs nature. The shortcoming of work proposed by the author is that the model contains real-time confirmation of received messages which is not possible in high mobility and scant situation.

Shaikh and Alzahrani [21], in their work, proposed a trust model based on the timing and fake location attacks. The trust model is decentralized and suitable for real-time application in VANETs as it introduces linear time complexity and simple. Moreover, the trust model proposed method detects the false location, time, and robustness. The computation of the trustworthiness of the message is based on previous information on node holds. Furthermore, the trust value of the event decides to accept or reject the value.

Mármol and Pérez [22] proposed a trust model, namely, TRIP. In the work introduced by authors, computation of trust of node is based on three factors. First, direct experiences based on previous interaction with node; second, interactive communication with surrounding nodes and their recommendations; and third, the communication between RSU and central authority and central authority send recommendations. Computation of reputation score map all three values received from conditions 1, 2, and three based on fuzzy sets that are ((One) trust; (Two) not trust; and (Three) +/− trust)). In three conditions of trust to accept or discarded, first, if the score is placed in "not trust," discard the message, and the presence of the dishonest node is sent to infrastructure. In other cases, if the score is placed in "trust," then the message is accepted and forwarded to other vehicles in the network. In the last condition, if the reputation score is computed as "+/− trust," the message is processed as reliable with the condition of tunable

probability; furthermore, it is not forwarded to nodes in the network. We find that the proposed assumption is not realistic. In addition to this, to build a history and reputation of the received message of vehicles, in this scenario, the actual identities of vehicles should be known.

Patwardhan et al. [31] proposed the Data Intensive Reputation Management model. The protocol integrates reputation and agreement to guarantee the reliability of data and kindle proactive collaboration. Furthermore, in their model, they exercise multiple factors such as frequency of encounters, persistent identities, and a known set of trustworthy sources for creating trust relationships among existing unknown devices. The trustworthiness of data depends upon majority consensus among peers or in case it is received from trustworthy sources. In addition to this, the authors supposed that each node must have a unique persistent identity, and this assumption violates identity privacy.

Chen et al. [32] proposed a trust model framework for evaluation and message propagation. In their trust model, the authors used experience-based trust, trust opinions, and role-based trust models to model the quality of information shared between nodes. The model is based on a binary operation that is either to (trust) or (not trust) information. This binary condition limits the situation based on incomplete information or in other cases are in uncertain situations. Moreover, in their work, the key important features such as privacy and robustness are not widely addressed.

Lo and Tsai [33] have proposed a trust modeling framework based on Traffic Safety Event. In their method, specifically, the event-based Reputation System (ERS) is used to stop the nodes to broadcast compromised, untrustworthy, and malicious warning messages. Furthermore, the method uses a cooperative-event observation and reputation adaptation schemes, with two types of thresholds, event confidence and event reputation, to calculate the event intensity and event reliability simultaneously. The major shortcoming of the proposed model is the time taken to share the trusted information with peers in time.

Liu et al. [24] have proposed a trust model, namely, LSOT in VANETs, based on two types of evaluation methods: certificate-based and recommendation-based trust. In their work, authors address the high mobility and random distribution dynamics of VANETs. Furthermore, the LSOT model operates in a fully distributed environment. To the calculation of trust, the three weight factors were used, which are number, time decay, and context to accurately determine overall trust. The main drawbacks of this model are that the authors failed to differentiate between the message and trust of the node.

2.2. Entity-Oriented Trust Model. The entity-oriented (EO) aims to remove dishonest vehicles by assessing the reliability of the node. The EO evaluates the trust on the node and identifies the presence of a malicious vehicle in the network. There is a considerable amount of literature work carried out by several authors on data-oriented trustworthiness.

Mármol and Pérez [22] have presented a trust scheme based on reputation infrastructure, for vehicular ad hoc networks. In their work, the authors are considering three different types of information to calculating the reputation score for every node in the network. The three estimating parameters are direct interaction with the previous vehicle, suggestions, and recommendations from nearby vehicles in the network and central authority recommendations. To accept or reject them based on the three conditions after the trust score is generated if the generated trust score is found as "not trust," the message is dropped and the presence of the dishonest node is sent to infrastructure. In other cases, if the trust value is calculated as "trust," then the message is accepted. In the last condition, if the trust value is calculated as "+/– trust," the message is accepted, and it is not forwarded to nodes in the network. Furthermore, in their model, trust establishment is connected to the node verification of trustworthiness of the node. The main shortcoming of the proposed trust model is that multiple senders will send the reputation of the sender, and this will generate additional overhead.

Khan et al. [34] have proposed a trust model DMN in Vehicular Ad Hoc Networks based on cluster-based mechanisms. The Cluster Head (CH) is responsible to calculate the trust and forward it to a Trusted Authority (TA). Furthermore, the TA is responsible to remove a malicious node from a network based on information received from CH. The main drawback of the proposed approach is that this approach is high overgenerated due to continuous reporting, which reduces network efficiency. Moreover, the network communication detail between CH, TA, and vehicles is missing.

Gerlach [35] developed a preliminary method in which each vehicle builds a profile of another vehicle when other vehicles come in contact. The proposed TM is sociological trust and based on the principle of confidence tagging and trust. The evaluation of trustworthiness is based on the interaction between vehicle profile histories. The EO model approach has serious weaknesses. First, VANET is highly dynamic, and interaction between the vehicles is for a limited time; this leads to difficulty in collecting enough evidence to calculate trust. Second, in case the vehicle itself is trustworthy, however, the message sent by the vehicle is either correct or not. In conclusion, the author presents a method of trust tagging exercising probabilities for representing trust and a trust model for vehicular applications for trust and applications. The shortcoming of Gerlach's proposed trust model is that it does not include the formalization of the architecture. Furthermore, their work failed to address a combination of the different types of trust together.

Minhas et al. [23], in their work, proposed role-based trust and experience-based trust as the evaluation method metric for the integrated reliability of nodes. This model also permits a vehicular entity to vigorously investigate about an event by sending requests to other entities but restricts the received number of reports. The multifaceted trust management model of the author has combined role based and experience based that are incorporated into the priority-based model, the two factors used to choose proper advisers.

The advisors are using the majority-opinion method to receive feedback. Furthermore, based on feedback aggregation received from advisors, two more factors were also considered: time and location closeness. The authors, further in their work, suppose that authorities predefined the roles and are assumed to behave in a certain way. The shortcoming of the work is that the robustness has not been addressed widely.

Yang [36] proposed a trust model based on Reputation Management for VANETs. The author used a similarity mining approach to calculate the trustworthiness of the vehicle. Furthermore, the reputations of recommenders are exercised as weights for calculating a full reputation for the message generator. The main drawback of the approach used by the author is that it proposed TM based on Euclidean distance between two vehicles as this contrast global information on the similarity of the generated message.

Jesudoss et al. [37] proposed a trust model scheme based on the reputation and election of CH. Authors in the scheme utilize the truth-telling approach to propagate true content to receive a better reputation. Moreover, the election is held among nodes to elect as CH. Furthermore, in election, nodes assign incentives in the form of weights. Higher the weight is, the more trusted the node by CH. Although this approach is interesting, it suffers from a rural scenario and highly mobile where only a few numbers of vehicle participates in election.

Haddadou et al. [38] proposed an economic incentive-based trust model. The authors used a distinct approach in which the credit value is assigned in a distributed manner. The credit value can be increased and decreased based on node behavior in the network. Furthermore, the credit value decreases each time in case an attack occurs in a network.

Zhang et al. [39] have proposed a trust scheme based on the Chinese remainder theorem (CRT). The authors work based on securing nodes privacy and offer authentication. Their scheme is based on tamper-proof device (TPD) identity, RSUs, and TAs. The shortcoming of the proposed scheme is that it is fully centralized, depends on RSUs and TAs, and is not applicable in rural areas where the VANET infrastructure is not available.

Guleng et al. [40] have proposed a trust scheme based on fuzzy logic to evaluate direct trust on the node. The author utilized honestness, cooperativeness, and responsibility factors in their approach based on fuzzy logic. The main shortcoming of this approach is the limitation of coverage area as the scheme is fully decentralized.

2.3. Hybrid Trust Models. Hybrid rust models combined the properties of both entity-centric and data-centric trust model scheme. Recently, in the literature, several studies have been conducted on the trust established based on hybrid trust models. A hybrid trust model has evaluated the trustworthiness of peers and utilizing modeling outcomes to calculate the reliability and trustworthiness of data.

Sedjelmaci and Senouci [41] have proposed a trust model based on the mobility and accuracy of VANET. The author claims that the trust model addresses the basic characteristics of a network for instance node's mobility and rapid topology change. The authors claim that the proposed lightweight model will adversary address the most dangerous attacks such as a black-hole attack, wormhole attack, and Sybil attacks by using a watchdog mechanism. Furthermore, the proposed solution is divided into two level intrusion detection systems. The first part is based on collaborative detection, whereas the second part of the framework deals with a global detection system that was processed by RSU. The main shortcoming of the proposed solution is that time to elect the cluster head will pose a delay in the network and time-consuming process.

Dhurandher et al. [42] proposed a framework, a Reputation and Plausibility Checks-based approach, by transmitting safety and security-related messages. The authors work based on the Vehicular Security throw reputation and plausibility check (VSRP) mechanism which utilizes three terminologies in the algorithms, and they are event modification message, data grouping, and false event generation. The main drawback of the proposed solution is that the detection range is very short that is 50 meters. Furthermore, detection is based on the vehicles' embedded sensors.

Abdelaziz et al. [43] proposed a trust-based scheme for VANETs, namely, Trust Model with Delayed Verification for Message Relay. The authors divided data traffic into four distinct classes specifically based on the priority given to safety-related messages from high to low as follows: (1) background traffic, (2) best-effort traffic, (3) video traffic, and (4) voice traffic. The main drawback of the proposed trust model is that author assumes that a dishonest vehicle will behave constantly all over to their journey in the network; this approach is invalid in the VANET.

Dotzeret et al. [44] proposed a trust scheme that is based on a distributed reputation model piggybacking opinion approach. In this approach, every forwarding node adds its own opinion regarding the trustworthiness of data. The trustworthiness algorithm is based on multiple trust factors that include direct and indirect trust, sender base reputation, and geo-situation orientation.

The main drawbacks of the scheme provider by authors are that they failed to provide sufficient and complete details about the approach. Moreover, the author mentioned that, in algorithm, sender-based information is managed; however, it failed to provide about how reputed information in TM will be updated.

Chen et al. [25] proposed a framework based on the message propagation and evaluation framework. The framework is based on trustworthiness message propagation in a distributed and collaborative fashion. The authors in their model address basic characteristics of VANETs; they are network scalability and system effectiveness. Moreover, those two characteristics include the addition of information evaluation based on the pervasive presence of false information in a network.

Rai et al. [3] proposed a hybrid VANET-based trust scheme, namely, a hybrid dual-mode trust management scheme for vehicular networks. The author's scheme is dual applicable for urban and rural based. Their scheme is based on the crediting technique. The credit value is obtained by

looking at sender node history and validation of the message received. The main shortcoming of the approach is the missing of central authority and infrastructure of VANET.

2.4. Authentication Schemes Based on a Pseudonym. The key requirements of privacy in VANETs are the unlinkability and the secrecy of the message. The safety-related beacons are broadcasted every 300 ms in a vehicle-to-vehicle communication. This phenomenon can lead to potential endangers the privacy of drivers by tracking the mobility pattern of the targeted driver. The main motive of attacks on privacy is to get sensitive information about vehicles and drivers [45]. A pseudonym scheme facilitates hiding the identity of a vehicle and addresses the privacy and security requirements of the system [46]. Furthermore, a pseudonym is a temporary certificate assigned to a vehicle to hide its real identity [14, 46–50]. In the literature, a range of pseudonym schemes is proposed to provide privacy protection and changing pseudonyms periodically.

Buttyán et al. [47] proposed a scheme, namely, SLOW: a practical pseudonym changing scheme for location privacy in VANETs. In their scheme, the authors proposed that the vehicle must not send beacons in case its speed is reduced below a given threshold. Furthermore, a vehicle must change a pseudonym for the duration of such a silent period.

In [49, 51, 52], the pseudonym of vehicle changes in case it enters the social spot and mix zone. In [53], the authors put forward a cooperative pseudonym change method among its neighbors. In [47, 54], once a pseudonym is changed then the vehicle will keep communication silent. The assure legitimacy and integrity of message authentication are indispensable. Various approaches have been proposed in [49, 55], and with these approaches, the authors developed the methods of verifying the certificate and message. These approaches can authenticate the legitimacy of the sender and validity of a message without revealing the vehicle identity. The main weaknesses in their approaches are the trustworthiness of received messages.

3. Architecture of Internet of VANETs

The main components of VANETs are vehicles embedded with OBU, RSU a communication component consist of RF antennas and process unit, and telecommunication network, for example, satellite communication. There are mainly three types of communication modes:

(1) Intervehicle communication (V2V)

(2) Vehicle-to-roadside communication (V2I)

(3) Interroadside communication (I2I)

(a) Intervehicle communication (V2V): in this mode of communication, vehicles communicate with another vehicle with the help of OBU embedded in every vehicle. In this communication mode, vehicle to vehicle communicates with each other with wireless technology. Furthermore, the message transmitted among the vehicle is broadcast so all vehicles in the coverage area received the transmitted information, as shown in Figure 1.

(b) Vehicle-to-roadside communication (V2I): in this mode of communication, vehicles will communicate with roadsides communication equipment Roadside Unit (RSU). Furthermore, in this mode, a direct wireless communication link is established between vehicle and infrastructure units located around the road [56].

(c) Interroadside communication (I2I): in this mode, communication RSU communicates with another RSU and core network, for example, 5G, satellite, or wired telecommunication system.

(d) Trusted authority: trusted authority (TA) is the heart of the VANET system. The primary responsibility is registering the RSUs, OBUs, and vehicles. The secondary responsibility includes assuring security management by verifying authentication of vehicle, user identification, and OBU identification to secure the vehicle from attack.

(e) Roadside units (RSU): these are communication based units installed near highways, which transmit useful information to vehicles that came in the radio range of RSU. They are connected to a central network with means of wired or wireless.

(f) Vehicles: vehicles are the basic units of VANET; they are equipped with the computing device installed on it called the On-Board Unit (OBU). The main responsibility of OBU to communicate with neighboring OBU installed on the vehicle as well as RSU. TA sends multiple pseudonyms to registered vehicles in the network.

(g) Legitimate nodes trust variation: in this section, legitimacy and dishonesties of TM will be measured in the presence of an attacker. Furthermore, compromised messages and trust rating was shared by an attacker.

(h) Malicious nodes trust variation: in this section, we define the ability of TM to implement the lowest level for the attackers.

(i) Centralized reputation serve (CRS): it assigns an initial reputation value for each registered vehicle in the network. CRS is responsible for managing and updating reputation. In case the reputation value is less than the threshold, CRS revokes the vehicle from the network.

(j) Pseudonyms: these are identities that are assigned to nodes in the network and only once used. The basic functionality is to maintain the privacy of nodes. Central authority keeps changing assigned pseudonyms periodically. A pseudonym is a temporary certificate assigned to a vehicle to hide its real identity.

(k) Mix zone: this is the coverage area in the VANET that is not under the surveillance range of the dishonest attacker. This is suitable for a node to change their pseudonym to prevent tracking.

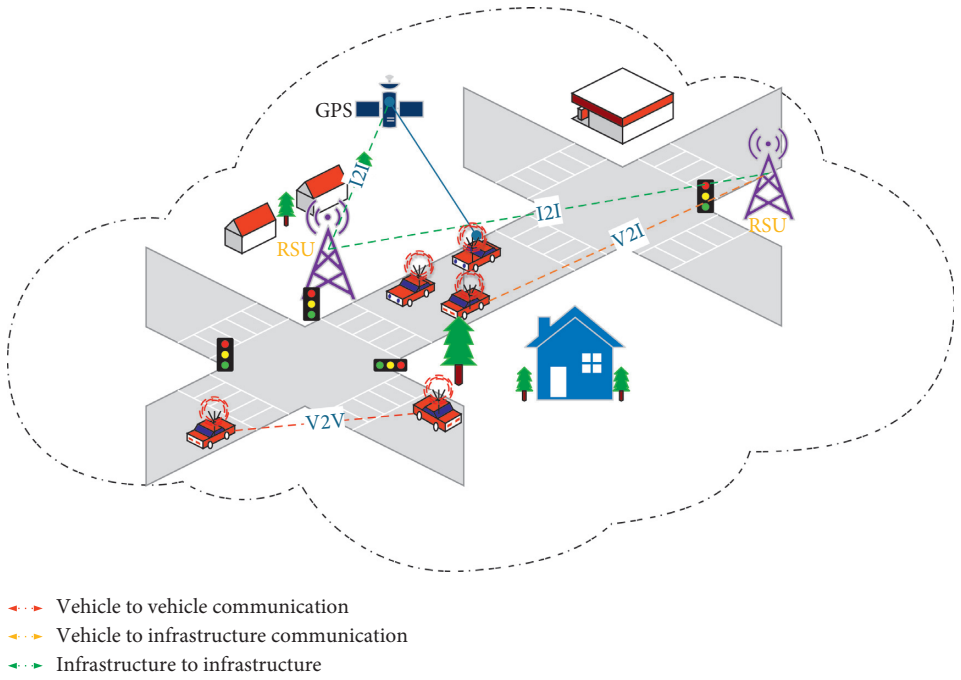

Figure 1: Internet of vehicular ad hoc network architecture.

Furthermore, in this coverage area, multiple nodes exist simultaneously, and this makes the attacker difficult to track the node.

3.1. VANET Challenges in a Road Network. Modeling of VANET trustworthiness peers in road network faces enormous challenges [14]. The key challenges that encounter by VANET can be categorized into two major conditions. Firstly, vehicles are continuously moving in the network and are extremely dynamic [57–59]. The speed of a vehicle is on the highway typically between 80 and 120 km/h. Furthermore, at this high speed on the road, to respond to a forthcoming event is critical in real time, and peers must be able to validate incoming information [12, 29]. Secondly, it may be expected that the number of vehicles in the network can increase in any instance. For example, in urban areas, for all the time, ten thousand peers are always in the network, and during peak rush hours, it will increase dramatically to a higher number. This leads to congestions in the network which poses several issues. Moreover, the VANET is a shared channel network; during rush hour, peers received a lot of information from other peers in a network; this results in information overload [60]. Consequently, there is a great need for intelligent vehicle communication systems that potentially respond to hazardous conditions by efficiently deciding with which peers communicate in a network [61, 62].

A third key challenge is related to modeling trust in the VANET environment as it is a decentralized and open system; this means that no centralized infrastructure exists in the VANET [63]. Furthermore, the vehicle at any time joins or leaves the network, and it may be not guaranteed that, in future, interaction with the same vehicle will happen. Therefore, practically it is not worth to rely on a mechanism which utilizes a centralized system, for example, using Central Certificate Authority and Trusted Third Party or to create long-term relationship depends on a social network.

3.2. VANET Security. It is well known that VANET security is a complex issue with several challenges. These challenges are given, in detail, below. To address these challenges, different requirements must be taken into account. These requirements, for simplicity, can be classified into six main categories, i.e., Availability, Authentication, Confidentiality, Integrity, Privacy, and Nonrepudiation. These requirements, for simplicity, can be classified into six main categories, i.e.,

(1) Availability
(2) Authentication
(3) Confidentiality
(4) Integrity
(5) Privacy
(6) Nonrepudiation

3.2.1. Availability. This requirement is quite self-explanatory, meaning that the VANET ad hoc network must be available all the time to ensure the safety of vehicles. The unavailability could be possible by the DOS attack, as mentioned in [64]. To ensure availability, high connectivity and bandwidth must be disposable. That is, the network must be available all the time, and, at times, it must have a fast response time to some specific applications. A delay, or even milliseconds, could make the message futile, as highlighted in [65–67]. In addition to the aforementioned safety

aspects, security is also highly linked with the availability of the network. In a way, availability is a prerequisite to the overall security of the system [68].

3.2.2. Authenticity. Authentication is one of the major security aspects and plays an important role in VANETs. It is crucial for verifying the claim of authenticity, that is, verifying the identity of a vehicle, and differentiates the legitimate vehicles from the malicious ones. Otherwise, it may lead to serious safety issues, such as human injuries, traffic disruptions, and, in some extreme cases, it may lead to human loss. The process of authentication in VANETs includes three major parameters, i.e., identification, access control, and authentication. This can be achieved by acquiring security certificates and signatures. Specifically, cryptographic mechanisms are used to achieve authentication in VANETs, as it represents the first line of defense against any sort of external danger.

3.2.3. Confidentiality. The confidentiality in VANET plays an important role in maintaining users' privacy by safeguarding the content of information transmitted between two users. Confidentiality is achieved by using shared public keys and certificates in peer-to-peer communication. The cryptography mechanism is exercised to persuade confidentiality in VANET.

3.2.4. Integrity. In VANET, the Integrity assures that the message communicated between two nodes has not been altered, modified, and/or changed during the transmission. The Integrity in VANET could be achieved by cryptography as well as by the Trust. In cryptography, the public key and revocation methods are used to ensure Integrity [68, 69]. The received message, at the end node, could be trusted if it is free from alteration, modification, and change [68, 70–72].

3.2.5. Nonrepudiation. In VANET, the nonrepudiation requirement ensures that the sending node cannot deny a send message. The nonrepudiation matches the nodes' identification with the messages received. This is achieved by utilizing cryptographic approaches to meet certain requirements of nonrepudiation in VANET [69].

3.2.6. Privacy. Privacy is the foremost key requirement in VANET. The major sensitive information related to the nodes is Vehicle location, Identification of vehicle, identification of the driver, and details of the traffic route to be followed by the vehicle. While the communication in VANET is broadcasted, the attacker could take advantage of tacking the vehicle identity and location. Therefore, to ensure the privacy of the vehicle, cryptography and the Trust methods can be exercised in VANET.

3.3. Attacks in VANET. This section lists the common threats faced by VANET [29, 32, 68, 70–72].

(1) Certificate Replication Attack: in this attack, the certificate is replicated multiple times.

(2) Eavesdropping Attack: attacker intercept transmitted the communication to gain access or password.

(3) Tracking Tracing Attack: trace or track the correct position of device and vehicle.

(4) Denial of Service Attack (DoS): this attack is caused by preventing accessing the network from functioning properly and timely manner. This causes a legitimate vehicle not to access the application or services.

(5) Jamming Attack: this attack is almost the same as a DoS attack, but this time the shared bandwidth among the nodes or network is jammed.

(6) Coalition and Platooning Attack: this attack works in a group, where multiple dishonest vehicles collaborate to perform malicious activities such as bandwidth usage or stopping any services.

(7) Betrayal Attack: this attack occurs when an honest vehicle becomes dishonest during transmission.

(8) Replayed, Altered, and Injected Message Attack: this attack altered or modified the information during messages transmission. This will cause to send multiple erroneous messages.

(9) Illusion Attack: typically, this attack is related to hardware component, for example, wrong sensor reading, and incorrect messages are sent to other vehicles.

(10) Masquerading Attack: this attack is caused by a dishonest vehicle wearing a legitimate certificate by disturbing and doing malicious activities.

(11) Impersonation Attack: a dishonest node assumes to be another node by using the wrong identity.

(12) Sybil Attack: a dishonest node transmits multiple fabricated message IDs to the legitimate node, where the legitimate nodes assume that they are dealing with multiple devices.

(13) GPS Position Faking Attack: falsified positioning based on geographical coordinates.

(14) Timing Attack: the dishonest node adds the delay between the packets, which cause unforeseen incidents.

(15) Blackhole Attack: a dishonest node transmits a false reply message to the other vehicle that the dishonest host is optimal route information to the destination.

(16) Grayhole Attack: a dishonest host drops the packet of the particular vehicle in the network and transmits other packets to its destination.

3.4. Identity and Location Privacy Protection in VANET. In VANET, through a continuous exchange of Safety Beacon Messages (SBMs), all peers in the network would receive safety-related information in well time and help peers to be

aware of incidents happening in the surrounding, for example, traffic congestion, accidents on road, and updated traffic flows. The SBM includes major information is speed, location, vehicular identity content of a request, and others. In VANET, information regarding location and identity is most important [51, 73, 74]. Moreover, vehicular identity information is usually protected by utilizing a pseudonym, which is produced by the Central Authority (CA) in the traditional approach used in VANET. In the case, if CA is compromised, this leads to threatening the privacy of the vehicle. SBMs are produced according to location information. The traditional encryption process is used to protect location information which helps that location information during transmission will not be leaked or stolen. However, this approach does not assure that the information in CA or another related server in a centralized structure will not be lost or leaked. The users nowadays are more curious about their private information, so the system must be robust to protect the vehicular location and identity. Privacy protection is the utmost basic requirement of VANETs. Moreover, to protect the information of users, pseudonym technique is used commonly. This strategy helps vehicles to amend pseudonym periodically to avoid being tracked in the system [49]. As a result, the attack on the privacy of the vehicle is the motive of an attacker to get access to sensitive data of the vehicle. Pseudonym schemes are developed to address privacy, security, and system requirement in VANET. To protect the real identity of a vehicle, a temporary certificate is issued, and this terminology is termed as a pseudonym. The authors in [50, 75, 76], when vehicles enter a range of mix-zone or social spot, amend its pseudonym.

4. System Model

This section describes the proposed Lightweight Trust Model (TM), in terms of lightweight, fewer arithmetic operations are used to reduce the complexity, such as square root log and complex geometry of the model. Trustworthiness involves several steps to calculate trust from received information from the sender. Our proposed model is hybrid, which calculates trust in data and node based on V2V and V2I communication. The proposed model comprises of the following two key components:

(1) Trust Estimation Model

(2) Decision Model

4.1. Trust Estimation Model. The trust estimation is performed based on five parameters: Location closeness, Data Integrity, Authentication, Time Stamp verification, and Peer Alert Message. The trust value is calculated based on the value generated by each of the five parameters. The vehicle received a message from another vehicle V2V or Roadside unit V2I.

The TM, in the initial following parameter, can be used, and the parameters may be changed depending on the simulation results and performance of TM, as shown in Figure 2.

4.1.1. Vehicle Location. A vehicle may provide incorrect location information during network interaction. Thus, the trust model should be able to detect the correct location. This parameter is either calculated or assumed to be shared between peers. When the model detects false location information of a vehicle, it will be discarded.

Vehicular Network System comprises of several vehicles. Every vehicle can communicate with other vehicles by using short radio signals dedicated to short-range communication DSRC (5.9 GHz), within a 1-kilometer range area. The communication between each vehicle is an Ad Hoc communication that means each connected node can move freely; usually, in a VANET, each node is supposed to have an onboard unit (OBU). The OBU enables vehicles to share messages with another vehicle in a prescribed coverage area. The coverage area is based on multiple factors, and they are the position and height of the transmitting antenna. Based on coverage, we present validation mechanisms to provide location closeness in VANET. In our approach, we use four different methods to calculate the location closeness. The trusted zone consists of the Road Side Trust Zone coverage area $\mathrm{RSU}_{\mathrm{TZ}}$, vehicle trust zone coverage area V_{TZ}, and vehicle zone coverage area $V_Z(V_r, V_s)$ for the sender and receiver vehicle:

$$L_C = \begin{cases} 1 & \text{if } V_L \in \left|\mathrm{RSU}_{\mathrm{TZ}}\right| \cap \left|V_{\mathrm{TZ}}\right| \\ \dfrac{2}{3} + \dfrac{1}{\left|\mathrm{Send}_{\mathrm{loc}} - \mathrm{Recv}_{\mathrm{loc}}\right|} & \text{if } V_L \in \dfrac{|\mathrm{RSU}|}{\left|V_{\mathrm{TZ}}\right|} \\ \dfrac{1}{3} + \dfrac{1+\gamma}{\left|\mathrm{Send}_{\mathrm{loc}} - \mathrm{Recv}_{\mathrm{loc}}\right|} & \text{if } V_L \in \dfrac{\left|V_Z\right|}{|\mathrm{RSU}|} \\ 0 & \text{if } V_L \notin \dfrac{\left|V_{\mathrm{TZ}}\right|}{\left|\mathrm{RSU}_{\mathrm{TZ}}\right|} \end{cases}. \tag{1}$$

The equation shows that the vehicle received a message from several sources, and based on the received message, calculate L_C to trust the message or discard it. We assume four different cases to calculate location closeness, the distance between the two nodes, the distance between the sender and RSU, and location closeness based on L_C. Here, in our scenario, we assume the coverage area of RSU is (50, 50), whereas the radius is 25.

4.1.2. Integrity. Data integrity ensures the genuineness of a message in terms of modification. The message exchange is one of the essential services of VANET applications. A message should be delivered timely, and accurate information for drivers should be provided to assure safety and enhance travel experiences. Due to the distributed, wireless, and open nature of the vehicular network, it faces serious security challenges. This may lead to a need for common security metrics to quantify the efficacy of VANET security measures. Here, we are using the WAVE (Wireless Access in

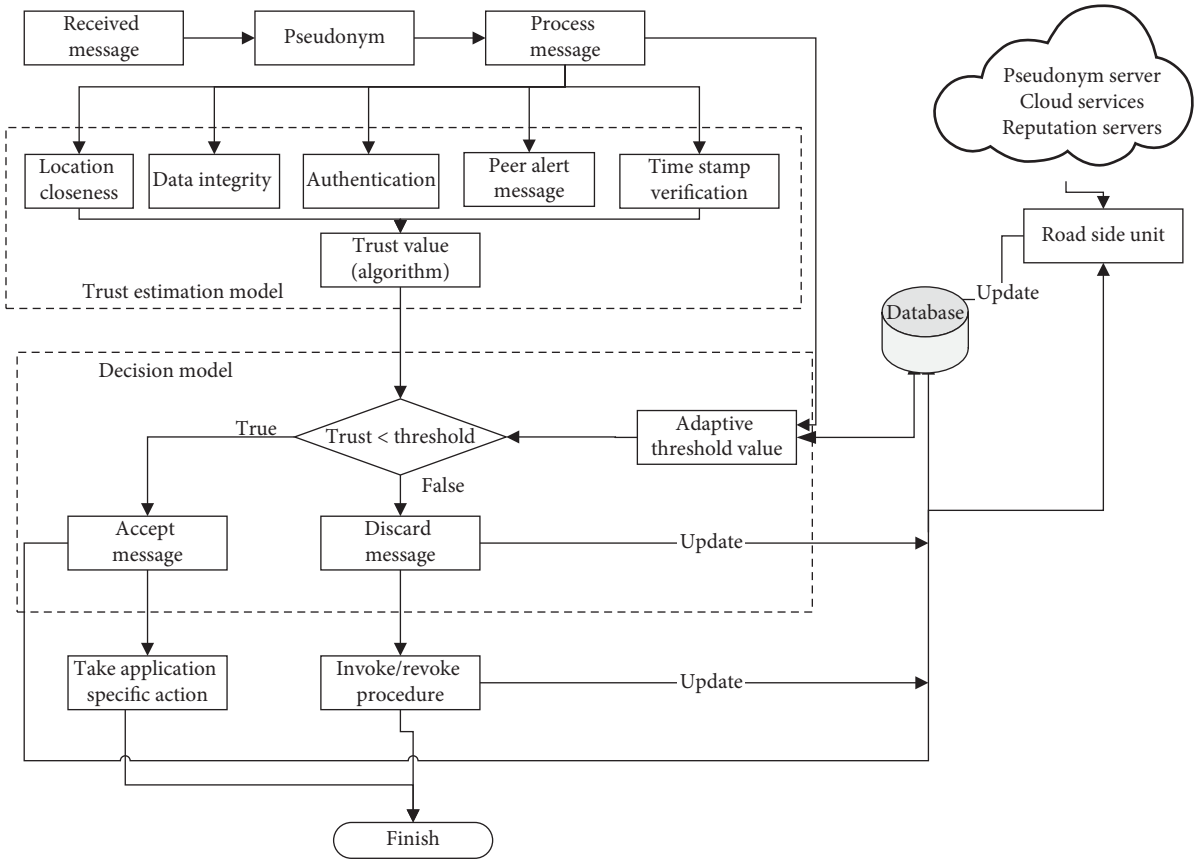

Figure 2: Proposed trust model.

Vehicular Environments) application to secure the content. WAVE specifications can assist V2V and V2I wireless communications, and these functionalities can be utilized to improve vehicle operational safety. Integrity prevents the unauthorized modification of messages in the transmission of the message between V2V. The integrity of considered applications is violated when the correctness and appropriateness of the content of a message are modified, destroyed, or deleted. Data integrity is assured that the message from a sender is protected by the hashing algorithm. To address any security limitations which are inherent mostly in wireless communications, the WAVE standard aims to enhance vehicle safety, to lessen traffic congestion, to activate services for vehicle maintenance, and to provide the potential for new commercial services. The hash algorithm SHA-256 will be used for integrity, as shown in Figure 3.

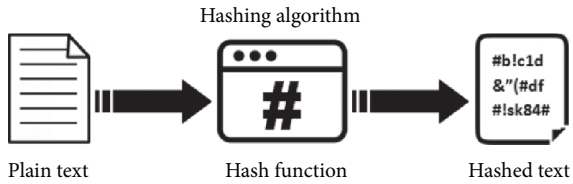

Figure 3: Data integrity hashing algorithm.

4.1.3. Authentication. Authentication is the process of proving something to be true, genuine, or valid. It is compulsory to identify a vehicle that sorts out the genuine sender and receiver. This ensures the identity first to kick out intruders and lower the chance of information loss [77]. The receiver vehicle must be able to verify whether the message is transmitted by a true sender vehicle [78].

WAVE security approaches use a Public Key Infrastructure (PKI) [79]. Here, in our TM, we use Public Key Infrastructure (PKI) scheme for authentication. The V2V and V2I communication in both cases is authenticated. The PKI scheme is scalable [8]. The nature of VANET is that some vehicles are moving quickly and changing the coverage area of one TM to another TM [80, 81]. A huge number of keys are required so that if the numbers of vehicles are increased in the TM area, all vehicles will receive keys. When certificates become invalid for any reason, that certificate will be revoked and updated information will be sent to the database. The revoked information is communicated by RSU in the trust area to other vehicles by generating Peer Alert Message. In our TM public key, cryptography confirms authenticity, integrity, confidentiality, and nonrepudiation [82]. In the scheme, if both vehicles wanted to interact, they have to exchange their public keys authentically, and the process requires the preliminary distribution of public keys. On the contrary, the private key is held only by other vehicles. Here, in our scenario, Public keys are generated by the

RSU and distributed through a secured channel to the vehicles. The Distribution of key comprises the initialization process, registration process, certification, and key updating in the case required [83]. All keys used have a validity date which is updated based on usage. RSU is hosting the public keys as well as the Certificate Revocation List (CRL). Furthermore, it is connected with a centralized database, in distributed manners, as shown in Figure 2.

4.1.4. Peer Alert Message. Message received from peers shares information regarding road condition or safety, and other options regarding the information can be trusted [32].

Peers (vehicles) in a VANET interact with each other by sharing road condition and safety information, to improve passenger and road safety and to effectively route traffic through dense urban areas. These systems concentrate primarily on ensuring the reliable delivery of messages among peers. Here, in our scenario, RSU generates peer alert message to inform vehicle in the coverage area about the safety and untrusted vehicle in the coverage area of the RSU trust zone.

The peer message is generated to inform about the critical condition of the situation regarding safety and security. Figure 4 shows if the peer alert message generated our TM model, we assign the higher wait regarding other parameters used in the TM.

4.1.5. Time Stamp Verification. VANET applications are time critical, and the safety messages are received from the neighboring nodes. Disseminating incorrect time information in the safety message has a severe impact on the security of VANET applications, time verification, and correctness in the VANET.

VANET applications are time critical, and the safety messages are received from the neighboring nodes. Disseminating incorrect time information in the safety message has a severe impact on the security of VANET applications.

4.1.6. Time Stamp Verification Algorithm (Packet)

t_{pkt} = fetch – timestamp (pkt)

Calculate $t_e = t_r - ((\text{dist}(V_1; V_2))/C)$

C = Speed of light
V_1 = Vehicle one
V_2 = Vehicle second
t_e = Event time
t_r = Received time

if ($t_e == t_{pkt}$)
return 1
else
return 0;

The algorithm of Time Stamp Verification explains that time is verified by comparing the Event time received in a packet and current time. The Event time we are calculating here is the current time minus distance of Vehicle 1 to Vehicle 2 divided by the speed of light [21].

4.2. Decision Model Process. The decision model in our model received as the trust value from TM to decide whether to process the message or discard it based on a threshold value. If the trust value is less than the threshold value, a TRUE message is generated, and the decision box accepts the value, sends an update to a database, and takes an application-specific decision. Our TM is for two types of applications that are safety and traffic efficiency. If the threshold value exceeds, the threshold value message is discarded and the FALSE message is generated. False generated message is sent to discard, and update is sent to the database. On the basis of false generated message value, invoke/revoke procedure decides to invoke or revoke the message. Road Side Unit (RSU) is the trusted unit in the model. RSU will provide the initial trust value to all vehicles in the region of interest. All vehicles will have a unique ID in the region. RSU generated an alert message to inform about the malicious vehicle in the region of interest, and this alert message helps vehicles in the region not trust the information received from the malicious node. The decision model in our model received a trust value from TM to decide whether to process the message or discard it depending on the threshold value. If the trust value is less than the threshold value, a TRUE message is generated, and the decision box accepts the value, sends an update to a database, and takes an application-specific decision. Our TM is for two types of applications, which are safety and traffic efficiency.

(1) If the threshold value exceeds, the threshold value message is discarded and the FALSE message is generated.

(2) False generated message is sendt to discard and update is sent to the database. On the basis of false generated message value, invoke/revoke procedure decides to invoke or revoke the message.

(3) Road Side Unit (RSU) is the trusted unit in the model. RSU will provide the initial trust value to all vehicles in the region of interest. All vehicles will have a unique ID in the region. RSU generated an alert message to inform about a malicious vehicle in the region of interest, and this alert message helps vehicles in the region not trust the information received from the malicious node.

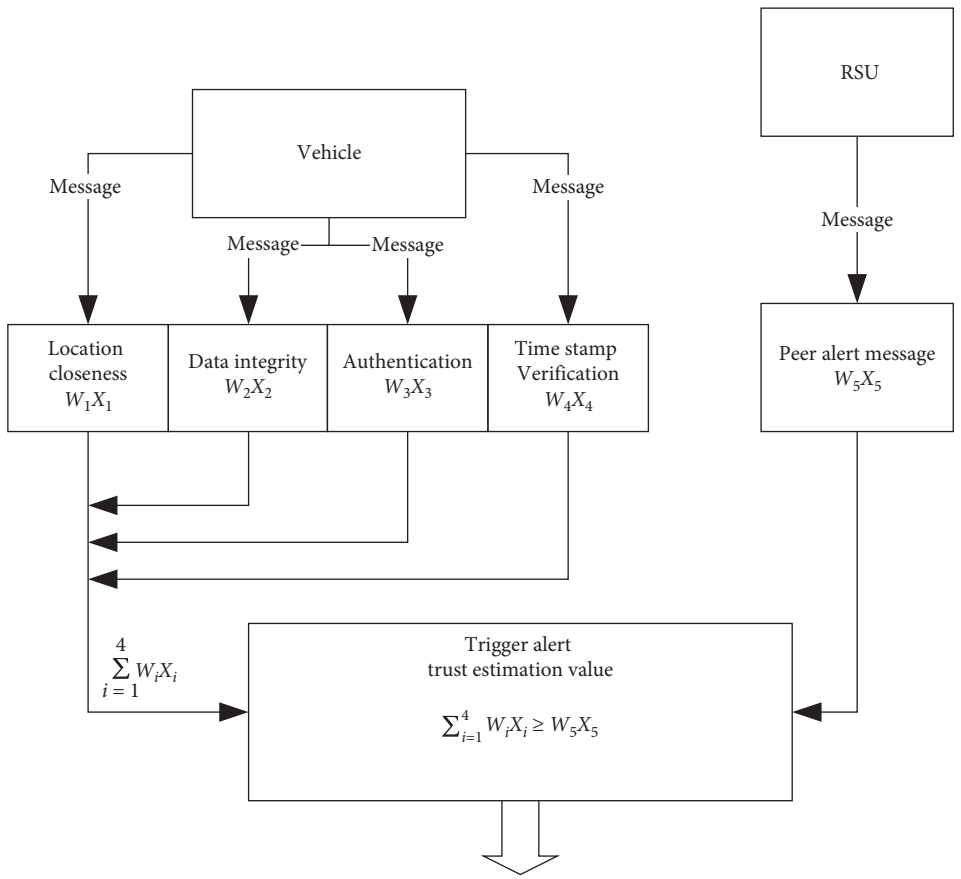

Figure 4: Peer alert message flow diagram.

4.2.1. Trust Calculation Algorithms

w_5P_R = Initial Trust value provided by RSU

```
#   Trust model
(1)   If L_C = 0 || T_S = 0 || AU = 0 ||DI = 0      # P_1 = L_C (Location closeness)
                                                    # P_2 = T_S (Timestamp)
                                                    # P_3 = AU (Authentication)
                                                    # P_4 = DI (Data integrity)
(2)   Trust = 0
(3)   Else
(4)       If Peer Recommendation available
(5)
      Trust = ((∑_{i=0}^{4} w_iP_i + w_5P_R)/5)
(6)   else
(7)
      Trust = ((∑_{i=0}^{4} w_iP_i)/4)
(8)   Endif
(9)       Endif
      # Decision model
(10)  ð = calculate threshold (s, r, A_U)         #s = sender
                                                  #r = receiver
                                                  #Au = authentication
(11)  if    trust < ð
(12)  accept message
(13)  else
(14)  discard message
(15)  Invoke-revoke procedure (s, r, T, ð)        T = Trust, ð = threshold
(16)  endif
```

5. Evaluations

In this section, the proposed lightweight trust model is evaluated based on the IEEE 802.11p standard. To evaluate the performance of the lightweight TM, the weighted voting method is used which is universally used in trust management schemes for wireless and vehicular networks [84–86]. The performance lightweight TM is evaluated against the MARINE [87] trust management scheme. Furthermore, the performance of our trust model is evaluated in the presence of four variants of Man in the Middle (MiTM) attacker. Moreover, the efficiency of the model is compared to a MARINE trust model based on the weighted voting method. In scientific research, the facility to use computer models and simulator programs to simulate a nearly real-world scenario facilitates a rapid and comparatively inexpensive study of complex real-time issues. Furthermore, than time and cost, simulation using computing resources can enable a view into experimentation. VANET research computer simulation permits research to build up applications and models for utilizing in real life before applying to cars and drivers. To deliver practical usable and realistic scenario-based results, the simulated system must be an accurate representation of real-road infrastructure. To present the real-world scenario-based simulation, in this study, we use UTM as the reference map to simulate the traffic pattern. Figure 5 shows the selected

Figure 5: Traffic map based on simulation.

Figure 6: Traffic (vehicles) movement.

area on which we will run the different simulations by changing and varying different traffic-based patterns.

Map 1, shown in Figure 5, will import in SUMO to simulate the traffic patterns. The map has some roads: one-way, single line, double line, two ways, number of signals, speed breakers, and bridges.

Figure 6 shows the movement of the vehicle inside the area, and every vehicle has a unique vehicle ID.

Table 1 provides details of the simulation values, which we will use in our simulation scenario. Road traffic simulation is performed by SUMO such as road length, several lanes, and speed of vehicles, and other details are listed in Table 1. Physical network communication of vehicles and RSU will be performed by using OMNET++ such as Frequency, packet size, and transmission rate, and transmission power. VEINS will integrate the physical and network structure scenarios. According to [88], most of the vehicles in the VANET are legitimate and behave honestly in the network. Consequently, to investigate the behavior of TM, the number of malicious nodes in the different network simulation scenarios will be varied from 10% to 50% in OpenStreetMap [89–91]. To evaluate and assess the TM the well-known machine learning evaluation parameters are used are Precision (P), Recall (R), and F-score. The Precision (P), Recall (R), and F-score are defined as follows:

Precision (P): the term Precision (P) is defined as the ability of TM to precisely forecast the trustworthiness of an event. Let P_M = number of real malicious nodes caught probability and P_U = total number of untrustworthy nodes caught probability. So,

$$\text{Precision } (P): \frac{P_M}{P_U}. \tag{2}$$

Recall (R): the term Recall (R) is described as the capability of TM to predict absolute malicious content disseminating by the nodes. Let P_M = number of real malicious nodes caught probability and P_T = total number of truly malicious nodes:

$$\text{Recall } (R): \frac{P_M}{P_T}. \tag{3}$$

F-Score: the term F-Score is described as the weighted average of Precision (P) and Recall (R). Moreover, accuracy of TM depends on F-Score. The higher F-Score values correspond more accurately TM. F-Score is defined as

$$F - \text{Score} = 2^* \frac{(P)^* (R)}{(P) + (R)}. \tag{4}$$

Trust variation metrics: in the paper, trust-related metrics is also considered, which illustrates the capability of TM and its efficiency to forego real events in a vehicular network [92]. In particular, to check, given three terms are described.

5.1. Attacker Scenario 1: Identity and Content Tempering. The graph in Figure 7 depicts the accuracy of the trust model on the base of attacker model 1. The two important considerations here are that the attacker is changing the content of safety messages and his identity; furthermore, the adversary tempering trust rating is within the coverage area. The precision and recall of the trust model are illustrated in Figures 8 and 9, and it can be drawn that the smaller number of MiTM attackers achieved high precision as well as recall. Moreover, in this case, if the number of MiTM attackers is increased holding tempering capability, this will result in decreasing corresponding precision and recall. Increasing MiTM attackers in the coverage area generates a high volume of compromised messages, resulting in limiting the ability of a vehicle to distinguish between legitimate and malicious messages. The presented trust model achieved high accuracy in term of F-score by comparing with MARINE, as shown in Figure 7. Furthermore, in terms of tempering ability, our model is more accurate compared to MARINE and assures accuracy around 88% with 11% MiTM attackers, whereas MARINE has 77% accuracy in terms of F-score.

Table 1: Simulation detailed parameters.

Parameters	Value approximation	Values used in simulation
Road length	1300–1400 meters	1400 meter
Number of road lanes	According to map	According to map
A frequency of vehicles entering per hour	0 to 4000 per hour	3000 per hour
Desired speed	10–70 km/hour	40 km/hour
Number of signals	0 to 2	1
Speed at signal	0 to 10 km/hr	0 when signal red 5 km/hr when a signal is orange 10 km/hr signal is green
Frequency	5.9 GHz for V2V	5.9 GHz for V2V
Transmission propagation vehicle	0 to 25 meters	0 to 25 meters
Transmission propagation RSU	0 to 50 meters	0 to 50 meters
Packet size	44 to 1000 bytes	200 bytes
Transmission rate	4–6 Mbps	6 Mbps
Transmission power	17–20 dBm EIRP	18 dBm EIRP
MAC protocol	IEEE 802.11p	IEEE 802.11p
Network protocol	IEEE 1609.4	IEEE 1609.4

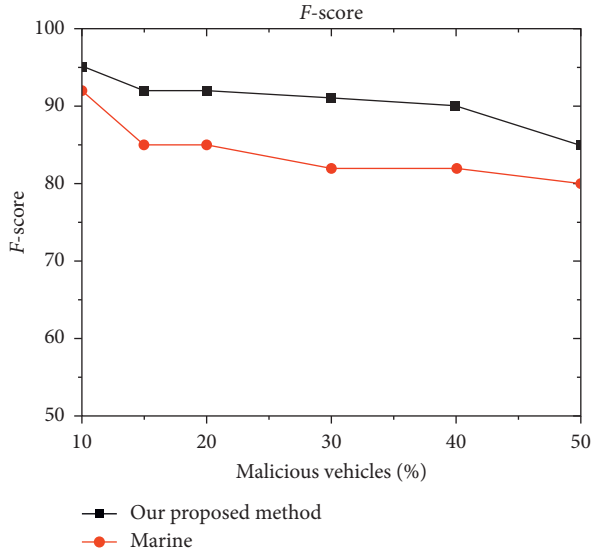

Figure 7: *F*-score attacker-1.

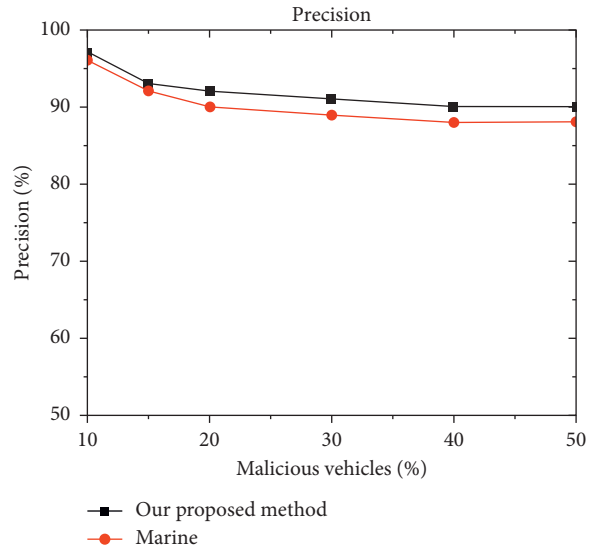

Figure 8: Precision based on attack-1.

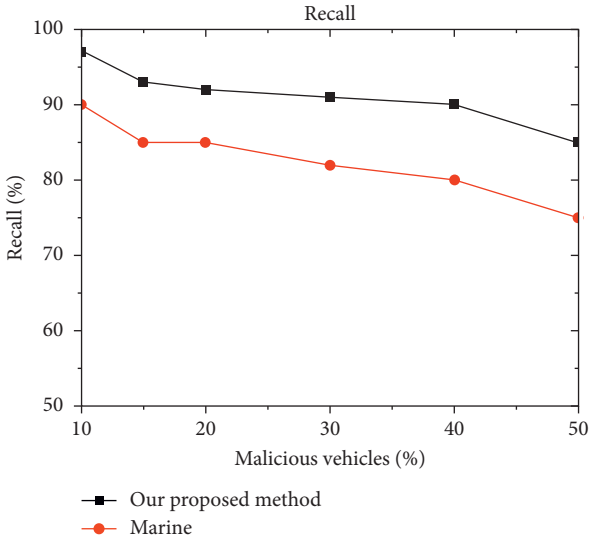

Figure 9: Recall based on attack 1.

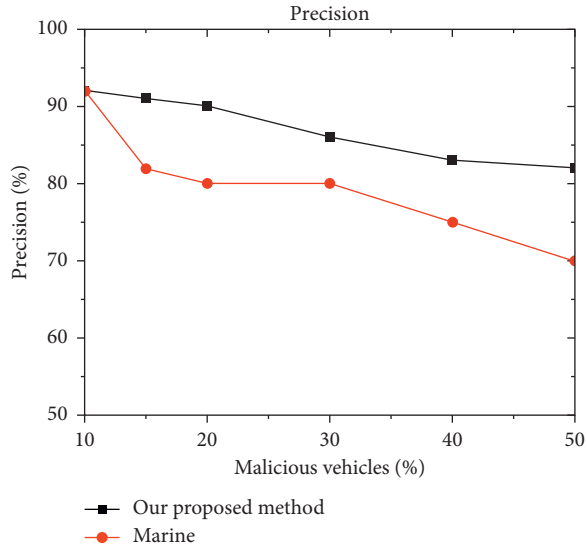

Figure 10: Precision attack 2.

5.2. Attacker Model-2 Is Based on Dropping and Delaying Messages. In this attacker model, the accuracy is measured based on precision, recall, and *F*-score. The malicious node in the coverage area is deliberately delaying and dropping the messages. Delaying and dropping of messages will delay the significant information received in time. Figures 10–12 highlighted the impact of delaying and dropping messages as the number increased the precision and *F*-score and recall decreased. Our trust model is efficient in finding such an attacker reason that the lower layer of the node detects the vehicle applying MiTM attacks. In the case of coverage area based on the high volume of MiTM attackers, 25% our proposed model assured around 82% of recall and 87% of precision values. This significantly concludes that our model is efficient in terms of identifying a malicious node in a network.

On the contrary, Figure 12 shows the accuracy in terms of *F*-score, and our trust model has high accuracy compared to MARINE. The percentage of malicious vehicles increased from 5 to 50 than the accuracy, which also decreased from 92% to 83% almost as compare to MARINE. The MARINE accuracy ranges in the same scenario from 91.5% to 72%. In this attack scenario, it concluded that our trust model is attack resistant to MiTM attacks. Furthermore, the trust model assures to disseminate trusted messages in the case high volume of malicious nodes.

5.3. Advance Zig-Zag Attack. To test the trust model at high-efficiency, several experiments are conducted which are reflected in Figure 13. MiTM attackers perform intelligently throughout the network to deceive legitimate nodes with disseminate tempered information and propagate compromised messages. The introduction of advanced zig-zag attack patterns has a drastic impact and reduced significantly precision and recall, and this is given in Figures 14 and 15. This advanced zig-zag attack will

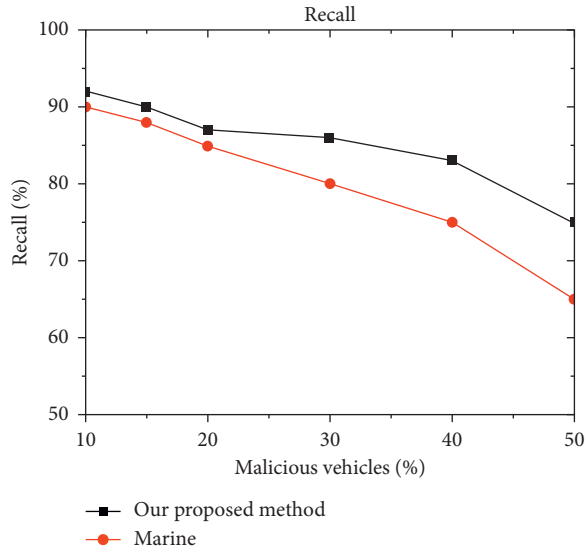

Figure 11: Recall attack 2.

help attackers to deceive legitimate vehicle to identify the attacker. In this case, our trust model helps the node to detect such an attacker with the zig-zag attack pattern. The following reasons explained trust model detection capability. Primarily, the trust establishment at lower layers helps early detection of MiTM attackers in a node-centric scenario. Secondary, Figure 13 reflects the *F*-score of the trust model used to measure the accuracy of the proposed method in identifying malicious content and detecting MiTM attackers. Finally, the overall performance notably decreased by varying the MiTM attackers' pattern in the network. Furthermore, changing the attack pattern will considerably reduce recall and precision. In this attack scenario, the accuracy of the trust model is more accurate as compared to MARINE in terms of *F*-score. Furthermore, in an attack scenario where 35% of vehicles are

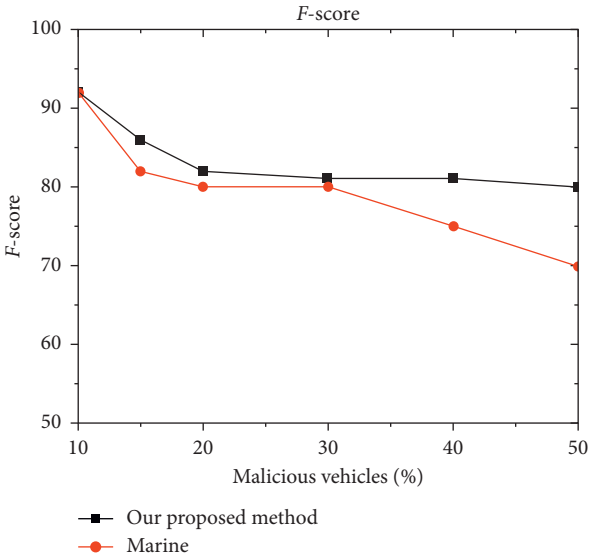

Figure 12: *F*-score attack-2.

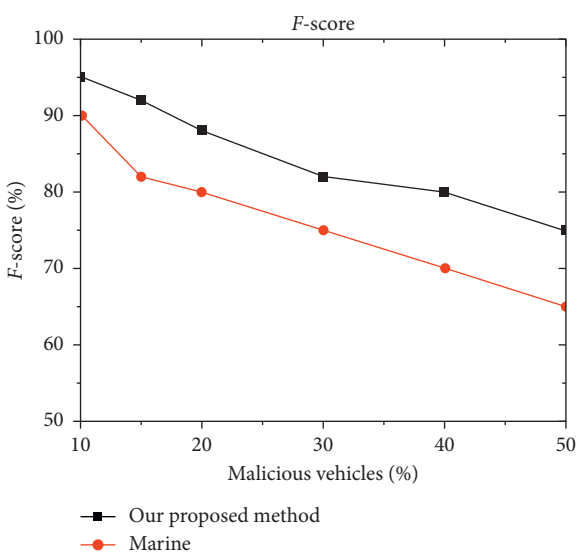

Figure 13: *F*-score attack-3.

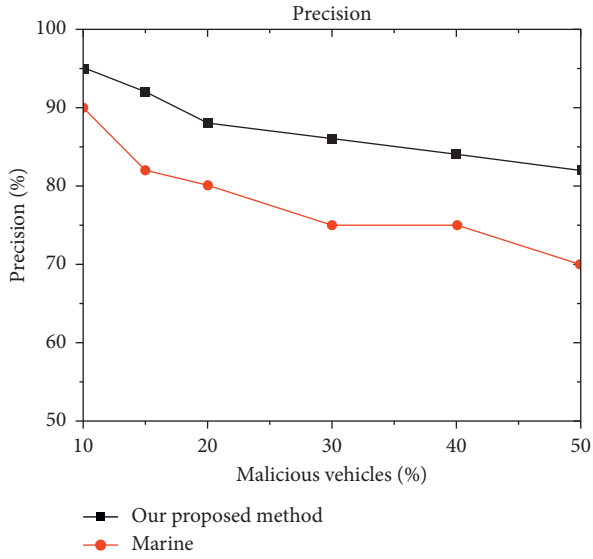

Figure 14: Precision attack-3.

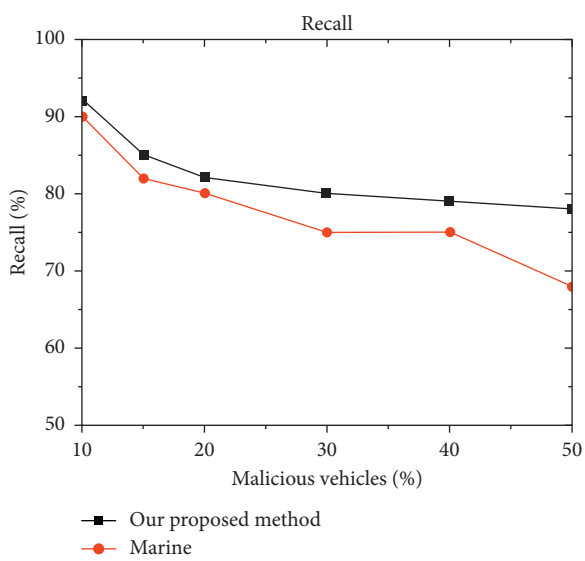

Figure 15: Recall attack 3.

malicious, the accuracy of the model is around 82%, whereas the MARINE was approximately 66%.

5.4. Trust Perspective Measurement. The trust establishment is a key parameter which enhances the security of nodes against inside attackers. The presented trust model in Figure 16 shows efficiency to classify and identify malicious content concerning the trust. In this scenario, a MiTM attack is generated in the VANET, and the trust of the network is decreased by increasing the malicious content in the network. The main reason behind trust decrease is that increasing malicious content in the network limits the ability of a legitimate vehicle to classify legitimate messages received. The presented trust model is capable of classifying and identifying legitimate nodes in the presence of attackers. The key factors for this are, primarily, presented the trust model which intelligently classify malicious messages as well as identify malicious nodes at lower layers. Secondarily, the presence of a role-oriented evaluator node in the network is to help the legitimate vehicle to process and true events. Finally, the evaluator node based on the abovementioned points will distinguish between an attacker and a legitimate node. In the current scenario, with 40% of MiTM attackers, the presented trust model achieves 86% of the trust level, now, as compared to MARINE, and it was 83%. Figures 16 and 17 describe the trust for both legitimate and untrustworthy nodes correspondingly. The given metrics are foremost important as they play an important role in the measurement of efficiency of the presented trust model

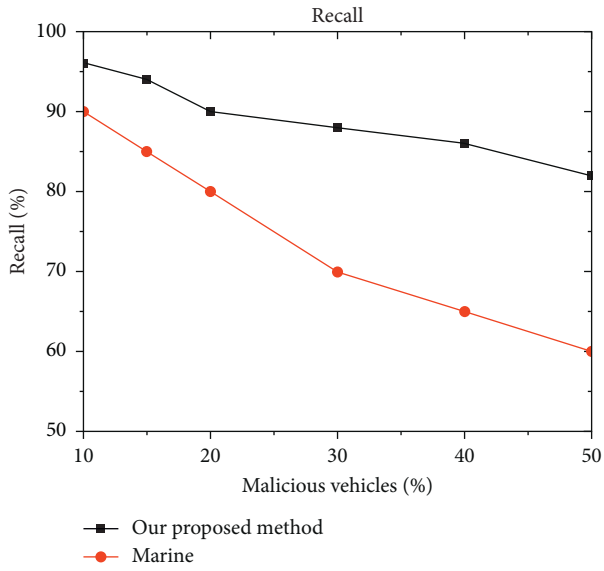

Figure 16: Recall attack 4.

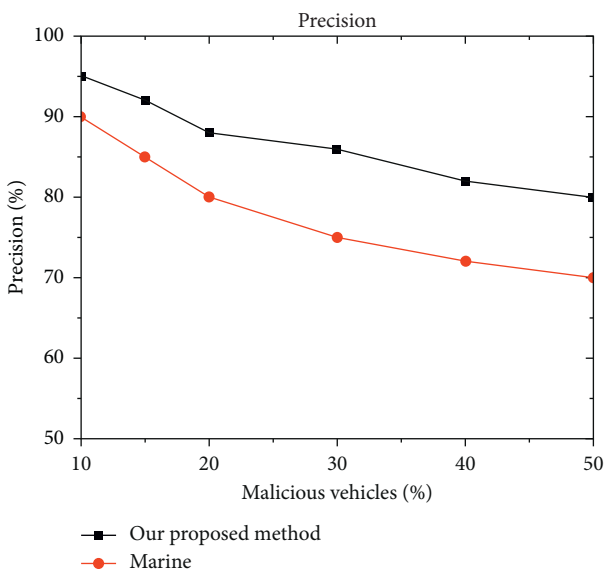

Figure 17: Precision attack 4.

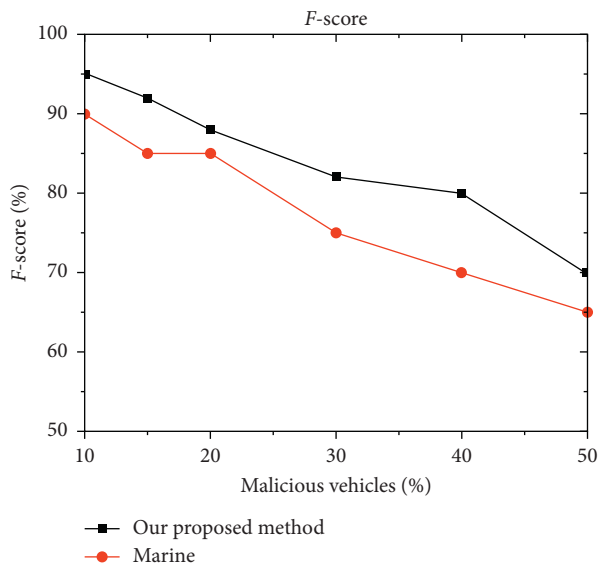

Figure 18: *F*-score attack-4.

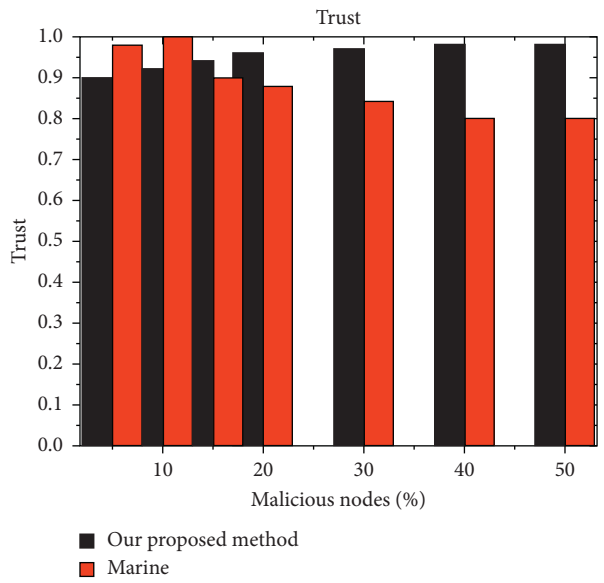

Figure 19: Impact of trust metric.

for evaluating trust in the received content. The presented trust model is a higher trust comparing MARINE, and the mentioned points below further elaborate it. The information in Figure 18 describes that the trust value within the legitimate vehicle is always more than the threshold value; here, in the presented trust model case, it is 0.5 even though if a high volume of MiTM attackers are present in the network. In this regard, it can be said that the presented trust model experiences a small number of false positive in the VANET. Furthermore, in Figure 19, trust between the MiTM vehicles is considerably lower than a threshold value, and this is because a very small number of false negative are generated by the presented model.

6. Conclusion

A privacy-preserving attack-resistant lightweight trust model is proposed to increase Internet of vehicles (IoV) security by promptly identifying dishonest nodes and revoking its credential in the MiTM attack scenario. Besides, for the trust model in terms of lightweight, fewer arithmetic operations are used to reduce the complexity, such as square root log and complex geometry of the model. The performance of the trust model is measured in the presence of four variants of Man in the Middle (MiTM) attacker and compared with a MARINE trust model based on the weighted voting method. Furthermore, for addressing the privacy and security requirement, pseudonym scheme is used. All nodes in the VANET established trust provided by RSU initially,

which is a trusted source in the network; once the trustworthiness of the sender is verified then the content can be processed. The results have validated the lightweight features of the trust model such as less arithmetic complexity, and low memory consumption leads the model to attain high detection accuracy in MiTM attacks. It has also manifested that the proposed model outperforms in terms of *F*-score, recall, and precision as compared to the MARINE model. Moreover, the proposed model has achieved a high trust level with 40% of MiTM attackers, and in terms of F-score 95%, whereas the MARINE model has 90%, which leads to the model to attain high detection accuracy. Despite the fact, the privacy-preserving attack-resistant trust model due to lightweight enables the participating nodes to hastily identify dishonest nodes and prevent them to poison the network from malicious content, and it also remains stable even when the number of malicious vehicles is increasing.

Data Availability

The data used to support this study are available at https://www.openstreetmap.org/#map=15/1.5645/103.6403.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Latif, S. Mahfooz, B. Jan et al., "Multicriteria based next forwarder selection for data dissemination in vehicular ad hoc networks using analytical network process," *Mathematical Problems in Engineering*, vol. 2017, Article ID 4671892, 18 pages, 2017.

[2] World Health Organization, "Global status report on road safety 2018: summary," World Health Organization, Geneva, Switzerland, 2018.

[3] I. A. Rai, R. A. Shaikh, and S. R. Hassan, "A hybrid dual-mode trust management scheme for vehicular networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 7, 2020.

[4] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, and A. Teles, "Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET," *Future Internet*, vol. 12, no. 4, p. 63, 2020.

[5] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: an overview," *Computers & Electrical Engineering*, vol. 87, p. 106776, 2020.

[6] M. Balta and İ. Özçelik, "A 3-stage fuzzy-decision tree model for traffic signal optimization in urban city via a SDN based VANET architecture," *Future Generation Computer Systems*, vol. 104, pp. 142–158, 2020.

[7] A. Bhargava, S. Verma, B. K. Chaurasia, and G. S. Tomar, "Computational trust model for internet of vehicles," in *Proceedings of the 2017 Conference on Information and Communication Technology (CICT)*, pp. 1–5, Gwalior, India, November 2017.

[8] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of vehicles: factors, challenges, blockchain, and fog solutions," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, 2019.

[9] I. A. Sumra and A. N. Akhtar, "Applications of internet of vehicle (IoV): a survey," *LGURJCSIT*, vol. 4, no. 2, pp. 59–70, 2020.

[10] M. K. Priyan and G. U. Devi, "A survey on internet of vehicles: applications, technologies, challenges and opportunities," *International Journal of Advanced Intelligence Paradigms*, vol. 12, no. 1-2, pp. 98–119, 2019.

[11] T. Halabi and M. Zulkernine, "Trust-based cooperative game model for secure collaboration in the internet of vehicles," in *Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, Shanghai, China, May 2019.

[12] R. A. Shaikh and A. S. Alzahrani, "Trust management method for vehicular ad hoc networks," in *Proceedings of the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pp. 801–815, Noida, India, January 2013.

[13] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust management problem in distributed wireless sensor networks," in *Proceedings of the 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06)*, pp. 411–414, Sydney, Australia, August 2006.

[14] I. Memon and H. T. Mirza, "MADPTM: mix zones and dynamic pseudonym trust management system for location privacy," *International Journal of Communication Systems*, vol. 31, no. 17, p. e3795, 2018.

[15] E. R. Cavalcanti, J. A. R. de Souza, M. A. Spohn, R. C. d. M. Gomes, and A. F. B. F. d. Costa, "VANETs' research over the past decade," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 2, pp. 31–39, 2018.

[16] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs," in *Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–3, Sydney, Australia, November 2018.

[17] S. Sakhreliya and N. Pandya, "Public key infrastructure (PKI) using symmetric key cryptography (SC) in VANETs," *International Journal of Computer Science and Information Technologies*, vol. 5, pp. 3556–3561, 2014.

[18] A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, "The case for dynamic key distribution for PKI-based VANETS," 2016, https://arxiv.org/abs/1605.04696.

[19] A. Hesham, A. Abdel-Hamid, and M. Abou El-Nasr, "A dynamic key distribution protocol for PKI-based VANETs," in *Proceedings of the 2011 IFIP Wireless Days (WD)*, pp. 1–3, Niagara Falls, ON, USA, 2011.

[20] S. A. Thileeban, C. S. Narayan, J. Bhuvana, and V. Balasubramanian, "PKI model optimisation in VANET with clustering and polling," in *Proceedings of the International Conference on Innovations In Bio-Inspired Computing and Applications*, pp. 321–329, Kochi, India, December 2018.

[21] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks," *Security and Communication Networks*, vol. 7, no. 11, pp. 1652–1669, 2014.

[22] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[23] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Transactions on Systems, Man, and*

Cybernetics, Part C (Applications and Reviews), vol. 41, no. 3, pp. 407–420, 2011.

[24] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: a lightweight self-organized trust model in VANETs," *Mobile Information Systems*, vol. 2016, Article ID 7628231, 15 pages, 2016.

[25] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust-based message propagation and evaluation framework in Vanets," in *Proceedings of the 2010 2nd International Conference on Information Technology Convergence and Services*, Cebu, Phillippines, August 2010.

[26] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[27] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for VANETs," in *Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology*, pp. 832–837, Bradford, UK, June 2010.

[28] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proceedings of the 2008 Proceedings IEEE INFOCOM-The 27th Conference on Computer Communications*, pp. 1238–1246, IEEE, Phoenix, AZ, USA, April 2008.

[29] J. Zhang, "A survey on trust management for Vanets," in *Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications*, pp. 105–112, Singapore, March 2011.

[30] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proceedings of the International Conference on Network and System Security*, pp. 94–108, Madrid, Spain, June 2013.

[31] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proceedings of the 2006 3rd Annual International Conference on Mobile and Ubiquitous Systems-Workshops*, pp. 1–8, San Jose, CA, USA, July 2006.

[32] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in VANETs," in *Proceedings of the 2010 2nd International Conference on Information Technology Convergence and Services*, pp. 1–8, Cebu, Phillippines, August 2010.

[33] N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, Article ID 125348, 2009.

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

[35] M. Gerlach, "Trust for vehicular applications," in *Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07)*, pp. 295–304, Sedona, AZ, USA, March 2007.

[36] 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.

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

[38] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach," in *Proceedings of the ComComAP'2013*, pp. 13–18, Hong Kong, China, April 2013.

[39] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[40] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized trust evaluation in vehicular internet of things," *IEEE Access*, vol. 7, pp. 15980–15988, 2019.

[41] 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.

[42] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing vehicular networks: a reputation and plausibility checks-based approach," in *Proceedings of the GLOBECOM Workshops (GC Wkshps)*, pp. 1550–1554, IEEE, Miami, FL, USA, December 2010.

[43] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs," in *Proceedings of the 2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 700–705, Nicosia, Cyprus, August 2014.

[44] F. Dotzer, L. Fischer, and P. Magiera, "Vars: a vehicle ad-hoc network reputation system," in *Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, pp. 454–456, Taormina-Giardini Naxos, Italy, June 2005.

[45] 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, PA, USA, 2011.

[46] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1, pp. 228–255, 2014.

[47] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: a practical pseudonym changing scheme for location privacy in VANETS," in *Proceedings of the 2009 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, Tokyo, Japan, October 2009.

[48] D. Förster, F. Kargl, and H. Löhr, "PUCA: a pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 37, pp. 122–132, 2016.

[49] S. Wang and N. Yao, "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs," *Wireless Networks*, vol. 25, no. 3, pp. 1099–1115, 2019.

[50] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in vanets," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2011.

[51] D. Liao, G. Sun, M. Zhang, V. Chang, and H. Li, "Towards location and trajectory privacy preservation in 5G vehicular social network," in *Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 2, pp. 63–69, Guangzhou, China, July 2017.

[52] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: a robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs," *International Journal of*

Distributed Sensor Networks, vol. 12, no. 3, Article ID 6138251, 2016.

[53] 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.

[54] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," 2016, https://arxiv.org/abs/1607.07656.

[55] B. Mishra, S. K. Panigrahy, T. C. Tripathy, D. Jena, and S. K. Jena, "A secure and efficient message authentication protocol for VANETs with privacy preservation," in *Proceedings of the 2011 World Congress on Information and Communication Technologies*, pp. 880–885, Mumbai, India, December 2011.

[56] J. A. Guerrero-Ibáñez, C. Flores-Cortés, and S. Zeadally, "Vehicular Ad-Hoc networks (Vanets): architecture, protocols and applications," in *Next-Generation Wireless Technologies*, pp. 49–70, Springer, Berlin, Germany, 2013.

[57] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4255–4271, 2016.

[58] A. Agrawal, A. Garg, N. Chaudhiri, S. Gupta, D. Pandey, and T. Roy, "Security on vehicular ad hoc networks (VANET): a review paper," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 1, pp. 231–235, 2013.

[59] P. Fabian, A. Rachedi, and C. Guéguen, "Programmable objective function for data transportation in the Internet of Vehicles," *Technologies for Emerging Future Wireless Networks*, vol. 31, no. 5, p. e3882, 2020.

[60] W. Li, W. Song, Q. Lu, and C. Yue, "Reliable congestion control mechanism for safety applications in urban VANETs," *Ad Hoc Networks*, vol. 98, Article ID 102033, 2020.

[61] I. Memon, "A secure and efficient communication scheme with authenticated key establishment protocol for road networks," *Wireless Personal Communications*, vol. 85, no. 3, pp. 1167–1191, 2015.

[62] I. Memon and Q. A. Arain, "Dynamic path privacy protection framework for continuous query service over road networks," *World Wide Web*, vol. 20, no. 4, pp. 639–672, 2017.

[63] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Transactions on Emerging Topics in Computing*, vol. 2020, 2020.

[64] J. S. Sengar, "SURVEY: reputation and trust management in VANETs," *International Journal of Grid and Distributed Computing*, vol. 8, no. 4, pp. 301–306, 2015.

[65] G. Samara and Y. Al-Raba'nah, "Security issues in vehicular ad hoc networks (VANET): a survey," 2017, https://arxiv.org/abs/1712.04263.

[66] M. A. H. Al Junaid, A. A. Syed, M. N. M. Warip, K. N. F. K. Azir, and N. H. Romli, "Classification of security attacks in VANET: a review of requirements and perspectives," *MATEC Web of Conferences*, vol. 150, p. 6038, 2018.

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

[68] 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, 23 pages, 2019.

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

[70] 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.

[71] 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, Australia, December 2012.

[72] 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.

[73] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, "Location and trajectory privacy preservation in 5G-Enabled vehicle social network services," *Journal of Network and Computer Applications*, vol. 110, pp. 108–118, 2018.

[74] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: an architecture for identity and location privacy protection in VANET," *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1178–1193, 2019.

[75] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su, "Mix-zones optimal deployment for protecting location privacy in VANET," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1108–1121, 2015.

[76] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5631–5641, 2015.

[77] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead," *Journal of Sensors*, vol. 2018, Article ID 6576841, 17 pages, 2018.

[78] A. Mondal and S. Mitra, "TDMAC: a timestamp defined message authentication code for secure data dissemination in VANET," in *Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, Bangalore, India, November 2016.

[79] J.-H. Kang, S.-J. Ok, J. Y. Kim, and E.-G. Kim, "Software implementation of wave security algorithms," *Journal of the Korea Academia-Industrial Cooperation Society*, vol. 15, no. 3, pp. 1691–1699, 2014.

[80] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[81] S. Shrivastava, "V2V vehicle safety communication," in *Connected Vehicles*, pp. 117–155, Springer, Berlin, Germany, 2019.

[82] H. Zhao, D. Sun, H. Yue, M. Zhao, and S. Cheng, "Dynamic trust model for vehicular cyber-physical systems," *International Journal of Network Security*, vol. 20, no. 1, pp. 157–167, 2018.

[83] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in VANET," *Wireless Networks*, vol. 25, no. 8, pp. 4639–4661, 2018.

[84] J.-M. Chen, T.-T. Li, and J. Panneerselvam, "TMEC: a trust management based on evidence combination on attack-

resistant and collaborative internet of vehicles," *IEEE Access*, vol. 7, pp. 148913–148922, 2018.

[85] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[86] M. A. Azad, S. Bag, S. Parkinson, and F. Hao, "TrustVote: privacy-preserving node ranking in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5878–5891, 2018.

[87] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.

[88] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV)*, pp. 1–6, College Park, MD, USA, November 2005.

[89] D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner, "SUMO (simulation of urban mobility)-an open-source traffic simulation," in *Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM20002)*, pp. 183–187, Sharjah, UAE, 2002.

[90] M. Haklay and P. Weber, "Openstreetmap: user-generated street maps," *IEEE Pervasive Computing*, vol. 7, no. 4, pp. 12–18, 2008.

[91] Veins, Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework, http://veins.car2x.org.

[92] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A comparative analysis of trust models for safety applications in IOT-enabled vehicular networks," in *Proceedings of the 2019 Wireless Days (WD)*, pp. 1–8, Manchester, UK, February 2019.