Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 5129620, 25 pages
https://doi.org/10.1155/2020/5129620

Review Article

Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey

Muhammad Sameer Sheikh,[1,2] **Jun Liang**,[2] **and Wensong Wang**[3]

[1]*School of Automotive and Traffic Engineering, Jiangsu University, Zhenjiang 212013, China*
[2]*Department of Automotive and Transportation Engineering, Automotive Engineering Research Institute, Jiangsu University, Zhenjiang 212013, China*
[3]*School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore*

Correspondence should be addressed to Muhammad Sameer Sheikh; sameer@ujs.edu.cn and Jun Liang; liangjun@ujs.edu.cn

Received 30 June 2019; Revised 4 November 2019; Accepted 27 December 2019; Published 17 January 2020

Academic Editor: Antonio Guerrieri

Vehicular networks are becoming a prominent research field in the intelligent transportation system (ITS) due to the nature and characteristics of providing high-level road safety and optimized traffic management. Vehicles are equipped with the heavy communication equipment which requires a high power supply, on-board computing device, and data storage devices. Many wireless communication technologies are deployed to maintain and enhance the traffic management system. The ITS is capable of providing services to the traffic authorities and precautionary measures to the drivers and passengers. Several methods have been proposed for discussing the security and privacy issues for the vehicular ad hoc networks (VANETs) and vehicular cloud computing (VCC). They receive a great deal of attention from researchers around the world since they are new technologies, and they can improve road safety and enhance traffic flow by utilizing the vehicles resources and communication system. Firstly, the VANETs are presented, including the basic overview, characteristics, threats, and attacks. The location privacy methodologies are elaborated, which can protect the confidential information of the vehicle, such as the location detail and driver information. Secondly, the trust management models in the VANETs are comprehensively discussed, followed by the comparison of the cryptography and trust models in terms of different kinds of attacks. Then, the simulation tools and applications of the VANETs are discussed, and the evolution is presented from the VANETs to VCC in the vehicular network. Thirdly, the VCC is discussed from its architecture and the security and privacy issues. Finally, several research challenges on the VANETs and VCC are presented. In sum, this survey comprehensively covers the location privacy and trust management models of the VANETs and discusses the security and privacy issues in the VCC, which fills the gap of existing surveys. Also, it indicates the research challenges in the VANETs and VCC.

1. Introduction

The intelligent transportation system (ITS) is an important part to revolutionize the traditional vehicle into the digital automated vehicle, which can limit and control the unpleasant events caused by traffic incidents, bottlenecks, and severe accidents. The ITS platform integrates the communication technologies with the vehicle networks to improve the transportation safety and management system. It provides traffic safety and comfort to the traveler and optimizes traffic flow to reduce the traffic congestions [1]. On the other hand, more deaths for the traffic incident in the urban traffic environment are caused by the fatal injuries and severe accidents. The traffic incidents and accidents will become the major reason of the death by 2030 [2].

VANETs are the type of mobile ad hoc network (MANET), which can provide the communication between the vehicles and infrastructures [3, 4]. The vehicle manufacturer and telecommunication industries are cooperating together to assemble each vehicle with the on-board unit (OBU) communication device, which are able to communicate with other vehicles by using the vehicle-to-vehicle

(V2V) technique and simultaneously with the infrastructures by using the vehicle-to-infrastructure (V2I) technique. The VANETs provides many advantages in terms of reducing road accidents, comfortable and pleasant driving, car parking, etc. Furthermore, it can serve the driver and passenger with the weather information, music, infotainment, etc. [5]. The VANETs provides robust solutions in terms of road and vehicle safeties and improves the traffic flow and efficiency [6]. It also provides the fast convergence of vehicular network with the ITS to explore the advanced development of the intelligent vehicular network [7]. These advancements are expected to transform driving features and experiences by creating a secure traffic environment including the city traffic and highway traffic. The vehicular network provides the infotainment services and enhances the efficiency of the ITS. Many contributions have been made to obtain these goals. However, the demerits of VANETs also appear, such as the transmission overhead caused by the high-mobility vehicles [8]. Secure communication in VANETs is challenging due to different kinds of threats and attacks [9]. Recently, research works have been done to overcome these issues and provide security solutions to tackle these attacks. In the VANETs, many existing security solutions related to the cryptography technique provide the secure communication by using different security certificates [10], public key infrastructures (PKIs) [11], signatures [12], and trusted third parties [13]. In contrast, some high-mobility scenarios cannot be performed well without the infrastructure; thus, the cryptography solution is limited which is not able to provide secure communication in the VANETs. When a trustworthy user becomes a malicious node or more vulnerable to be attacked, then the higher probability of cryptography solution is being compromised and may be overtaken [14]. In the VANETs, the trust management is based on the direct interactions and indirect recommendation between vehicles. Therefore, the evaluation of trust depends on the current situation in terms of data exchanges [14]. Trust models in the VANETs are classified into three types: entity-oriented model, data-oriented model, and hybrid trust model [15]. The trust model is capable of dealing with the inside attackers where the cryptography is unable to handle these attacks in the VANETs. However, the cryptography is able to handle outside unauthorized attacks.

Recent development and advances in the vehicular technology provide many resources such as storage devices, radio network, robust computational power, and different kinds of vehicle sensors. Challenges and benefits in the ITS have motivated the researchers to introduce and promote the vehicular cloud computing (VCC) [16]. It aims to provide the services to the drivers, improve the traffic flow, reduce the traffic congestion and accident, and ensure the usage of the real-time software and infrastructure with the quality of service (QoS) to drivers [17]. Specifically, the VCC can be the platform for the convergence of the ITS and the computing and storage capabilities of the mobile cloud computing (MCC). Moreover, the VCC can incorporate the features of ITS, WSN, and MCC for providing a better road safety, improving the driving conditions and the secured traffic management system [18].

Several surveys have been presented for VANETs [19–21]. Most of them provide the cryptography-based solutions to tackle the threats and attacks of the VANETs. Also, these research works focus on the security services without considering the VANETs requirements into the practical applications. In [22], Tangade and Manvi discussed the security attacks that confront with the VANETs and present the trust management solutions in the VANETs. Al-Sultan et al. launched a comprehensive survey which covered the VANETs architecture, protocols, simulations, and its applications [6]. However, they did not discuss the threats and attacks of the VANETs. In [1], Nidhal Mejri et al. launched a survey on VANETs security and its cryptography solutions to tackle the threats and attacks. However, it did not cover the trust-based model to handle VANETs threats and attacks. Furthermore, Whaiduzzaman et al. [17] launched a comprehensive survey on the VCC by covering its architecture, security, and privacy issues. Also, it discussed open research challenges and future directions. By utilizing the trust management, Patel and Jhaveri [23] launched a survey for securing routing protocol based on the trust management. In [24], Sharma and Kaur presented a survey of the VCC, in which they have discussed security threats and attacks and corresponding countermeasures to ensure the secure communication.

Few surveys related to the trust management for VANETs are reported [14, 15, 25, 26]. Reference [15] discussed the revocation target which covered the entity-oriented, data-oriented, and hybrid trust models. This work performs the trust management in a different way, without acknowledging where to apply trust model instead of the cryptography technique. Solyemani et al. [25] launched a survey which described the comprehensive literature review for trust concepts, problems, and solutions in the VANETs. Karn and Gupta [27] discussed the cryptography solution, only specifying the VANETs threats and describing the Sybil attacks and its possible solutions. Azees et al. [28] focused on the security challenges, threats, and attacks in the VANETs and also covered authentication schemes with privacy-preservation. In [14], Kerrache et al. launched a comprehensive survey on the trust management models for VANETs and also discussed the comparison of the existing solutions between the cryptography and trust models. It covered the specific trust model while did not cover the whole trust management system. Gillani et al. [26] launched a survey on trust management techniques for routing protocol. It focused on the trust management schemes which were applicable for the release of useful information for real-time applications. Then, they presented a categorical overview of trust management schemes and identified some open research challenges. Mekki et al. [29] launched a comprehensive survey on the vehicular cloud by presenting architecture, challenges, and security issues of vehicular cloud (VC). In particular, it discussed the challenges related to the VC design and did not cover the security and privacy challenges in VCC comprehensively. Moreover, in [30], Boukerche and De Grande presented the VCC architectures,

mobility, and applications. They discussed the recent state-of-the-art methods and the solutions for the VC, and traffic models that allow the VC to work in the dynamic environment. In [31], Sakiz and Sen discussed the security attacks in VANETs and the corresponding detection mechanisms and then presented the solutions. Hasrouny et al. [32] launched a survey on VANETs security challenges and solutions. They discussed VANETs characteristics and security and privacy challenges and requirements and then presented different kinds of attacks in VANETs and their corresponding solutions. Boualouache et al. [33] presented a comprehensive survey and classification of pseudonym changing strategies in VANETs. Then, they discussed and compared them with respect to some relevant criteria. Finally, they highlighted some open research challenges in VANETs along with the future research direction. Boussoufa-Lahlah et al. [34] launched a survey related to geographic routing protocols for VANETs. The authors discussed the recent state-of-the-art methods of the routing protocols of VANETs based on the geographical location of vehicles. Then, they highlighted some future research directions in the domain of routing protocols of VANETs. In [35], Muhammad and Safdar launched a survey which comprehensively covered the security and privacy issues for the cellular-based V2X communication, where it covered the security requirements, services, and authentication schemes related to the V2X communication. Sharma and Kaul [36] introduced a survey on intrusion detection system (IDS) and security mechanism in a vehicular network, i.e., VANETs and VANET cloud, which is used to handle the security threats. It discussed the challenging issues for using the IDS in the vehicular network especially for VANETs. In [37], Lu et al. presented a comprehensive survey, which discusses the architecture, security, privacy, and trust management system in the VANETs. Furthermore, it also discussed the network simulators and integrated simulator, but still with less coverage on the privacy and security in the VANETs. Kalaiarasy et al. [38] proposed a survey on location privacy in the VANETs using mix zones. They have reviewed several techniques for pseudonym strategy and mix zone schemes for privacy-preserving in the VANETs. Kouser and Manikandan [39] presented a survey on VCC services, which comprehensively covered the services and vehicle resource scheduling in the V2V communication. They highlighted the existing issues associated with the V2V communication and possible solutions. Alrehan and Alhaidari [40] launched a survey for the detection of distributed denial of service (DDoS) attack on VANETs based on machine learning techniques. They also discussed the machine learning algorithms applied to handle different kinds of attacks in the VANETs. Ali et al. [41] presented a survey on the authentication and privacy schemes for vehicular networks such as VANETs. The model classification, requirements, and threats and attacks were explained. Also, they discussed some open issues for VANETs security services. In [42], Hussain et al. presented a survey of integration of 5G network security with VANETs. They comprehensively conducted a study in terms of existing security issues, standards, and solutions used in vehicular networks. Then, they classified the security issues in existing VANETs security schemes. Second, the authors presented VANETs security standards to secure the VANETs applications as well as some open research challenges and future research directions for 5G-based vehicular networks. In [43], Arif et al. launched a survey on security attacks in VANETs. They investigated the communication protocols for each network layer in terms of relevant attacks that occurred at each layer. Then, they discussed the challenges and application in VANETs along with some open research challenges in VANETs. Sheikh and Liang [44] presented a comprehensive survey on VANETs security services. The authors discussed the VANETs architecture and security and privacy challenges in VANETs. Then, they presented the authentication schemes, which could protect the VANETs from malicious nodes.

As the whole communication take place in an open-access environment in VANETs, they are more vulnerable to be attacked, and the attackers can inject, modify, and delete messages, thereby subsequently causing the traffic accidents, traffic congestions, etc. Several research solutions have been proposed on the privacy and authentication schemes for VANETs. This survey is motivated from different surveys related to the VANETs security and privacy issues and challenges [14, 35–37, 41, 43, 44]. The previous surveys covered most of the security challenges which are relevant to the vehicular network and discussed a brief overview of the threats and attacks, the security and privacy issues, and the authentication schemes. However, there is still a great need for a comprehensive survey that analyzes VANETs security and privacy challenges from different perspectives.

The objective of this survey is to provide comprehensive analyses and understand threats and attacks and trust management for ensuring the secure communication in the VANETs. This survey is different from previous surveys in terms of location privacy, trust management, comparison of the cryptography, and trust models in terms of different kinds of attacks, VCC architecture, security and privacy challenges in VCC, and open research challenges in the VANETs and VCC. First, we presented the brief overview of the VANETs and its characteristics. Then, we discussed the potential applications, which are affected by the threats and attacks in VANETs. Second, we elaborated the location privacy methodologies, which can protect the confidential information of the vehicle, such as location details and driver information. Lu et al. [37] discussed the location privacy in detail while the rest of the previous surveys did not cover the location privacy. Then, we presented the comprehensive analysis of different trust management models in the VANETs, followed by the comparison of the cryptography and trust models in terms of different kinds of attacks, while the previous surveys did not discuss the trust management models in detail. Third, the simulation tools and applications of VANETs are explained while most of the previous surveys did not discuss them. Finally, we have covered the VCC by discussing its architecture and security and privacy issues, followed by open research challenges in the VANETs and VCC, while most of the previous surveys did not discuss the

VCC architecture, security and privacy issues, and open research challenges in the VANETs and VCC.

This survey is structured as follows. We have explained the overview of the VANETs along with the VANETs security services, and threats and attacks in Section 2. Section 3 presents the location privacy in VANETs. Section 4 presents the trust management models of VANETs. Simulation tools and applications of VANETs are discussed in Sections 5 and 6, respectively. We discuss the evolution from the VANETs to the VCC in Section 7. Section 8 presents the security and privacy issues in the VCC. Open research challenges in VANETs and VCC are explained in Section 9. Finally, Section 10 concludes the review.

2. VANETs Overview

The VANETs architecture consists of the OBU, roadside unit (RSU), and trusted authority (TA). There are two communication patterns, V2V and V2I communications, as shown in Figure 1. In the V2V communication, the vehicle can communicate with each other to exchange the traffic-related information within the wireless range. For instance, when an incident occurs on the road, the vehicle can immediately send the traffic information to the other vehicles nearby, suggesting them to avoid that area. In the V2I communication, the vehicle can exchange the safety information with the infrastructure such as RSUs which are deployed on the road. The V2I communication aims to avoid the crashes and severe incidents and provide multiple safety measures and precautions to the vehicles.

In the VANETs, the TA is responsible for the registration of the RSU and the OBU, which is used to maintain and manage the network system. The RSU is placed on the road which is used to communicate between the TA and the OBU for authentication. The OBU is equipped in each vehicle, which is able to send the traffic information to the neighboring vehicles and RSU by using dedicated short range communication (DSRC) [45].

2.1. VANETs Characteristics. The VANETs are highly dynamic ad hoc networks with high reliability, offering multiple services, but have limited accesses to the network infrastructure. VANETs have characteristics of high mobility and frequent change in topology as compared to the MANETs [1, 46], and can be further categorized into the network topology and communication mode as well as the vehicle and driver mode. The characteristics of the VANETs are as follows:

(i) High mobility: VANETs have high mobility as compared with the MANETs. The high mobility is one of the main features and plays a very important role in the modeling of VANET protocol. Every node in the VANET moves on very high speed. Therefore, the high mobility of nodes reduces the communication time in the network [5, 47].

(ii) Driver safety: VANETs can improve the driver safety, enhance the passenger comfort, and improve the traffic flow. The main advantage of VANETs is that the vehicles can communicate directly with each other. It allows a number of applications to communicate among different nodes such as the RSUs and OBU.

(iii) Dynamic network topology: the topology of VANETs varies rapidly based on the vehicle speed and high mobility. The rapid changes in vehicle mobility make VANETs more vulnerable to attacks and also very difficult to recognize the suspected vehicles.

(iv) Frequent network disconnection: the frequent disconnection of the VANETs are due to the high-speed movement among vehicles and other issues such as the weather condition. A large number of vehicles on the road can also lead to the recurrent disconnection.

(v) Transmission medium: the transmission medium is the air in the VANETs, and the universal availability of the wireless medium can be a robust advantage in the intervehicle communication (IVC), but there still are some security problems which depend on the nature of transmission and the security of communication by using an open support [1].

(vi) No power constraints: there is no power constraint in VANETs as compared to MANETs; thus, the vehicle provides continuous power to the OBU through the long-lasting battery [48, 49].

(vii) Limitation of transmission power: the transmission power is constrained in the wireless access of vehicular environment (WAVE) which ranges from 0 to 28.8 dBm with the associated coverage distance ranges from 10 m to 1 km. Thus, the limited power transmission can affect the coverage distance of VANETs [45, 50].

(viii) Network strength: the strength of the network in VANETs depends on the flow of the traffic on the street. In case of traffic jam, it can be very high and can be low when there is no traffic on the road.

(ix) Large network: the network can be larger in the downtown areas, highways, and also entry and exit locations of the city [48, 51].

(x) Wireless transmission attenuation: the performance of DSRC wireless communication has a limitation which is associated to the digital transmission with such frequencies band because of diffraction, reflection, dispersion, refraction, and scattering in the urban area [52].

(xi) Large computational processing: as the nodes in VANETs are vehicles which can be embedded with the sensors and other computational devices such as processors, global positioning system (GPS), and antenna. These resources require a large amount of computational capacity of node and lead to provide better and reliable wireless communication to obtain the exact information such as its existing position, speed, and direction [53, 54].

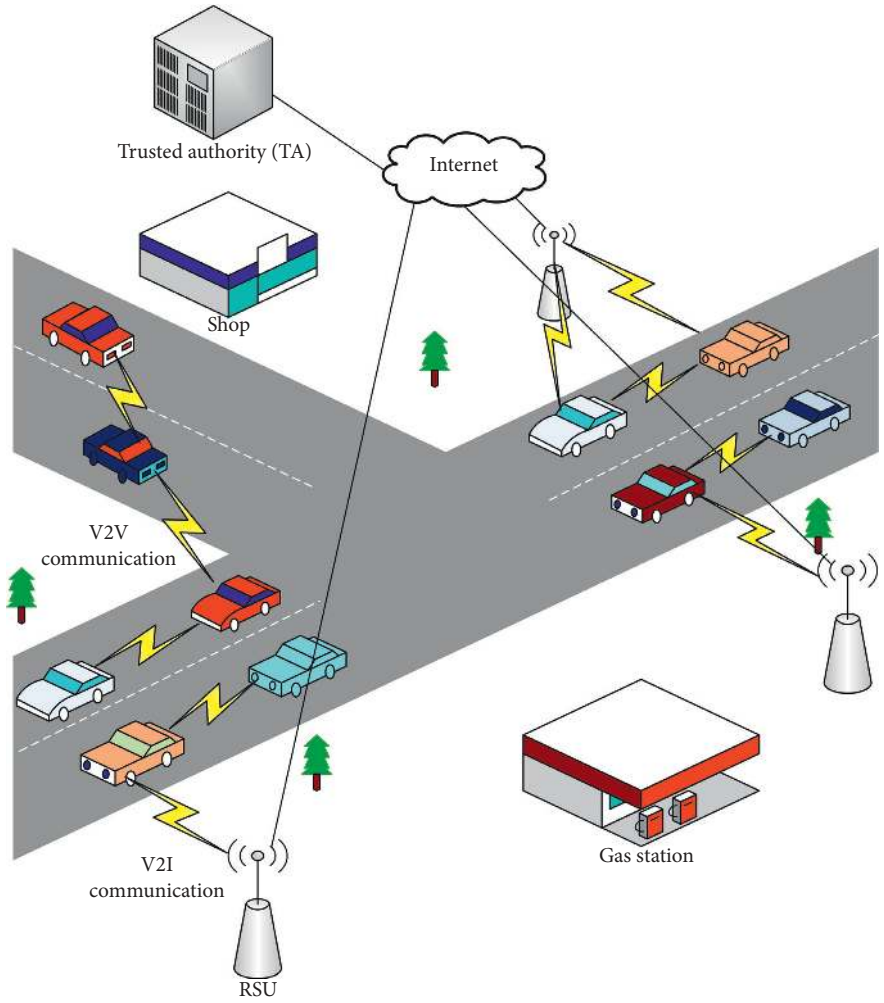

Figure 1: VANET system.

2.2. VANETs Security Services. The security of VANETs is a critical issue for providing safeties to the passengers and drivers. It is necessary to design significant algorithms to ensure the safety level. The security services are availability, confidentiality, authentication, data integrity, and nonrepudiation [55].

2.2.1. Availability. Availability plays a crucial role in the VANETs security since it ensures that the network remains functional in case of faulty and malicious conditions [56]. The availability is more vulnerable to dangerous attacks as compared to other security services. Therefore, trust-based and cryptography techniques can secure VANETs from these attacks.

2.2.2. Confidentiality. Confidentiality ensures that the data can be accessed only by the designated user while the outside users cannot access the confidential information that relates to a designated user.

2.2.3. Authentication. The authentication plays a vital role to ensure the safety of the VANET by preventing them from malicious entities in the network. In order to prevent the network from dangerous attacks, the authentication of users and messages which pass through the network is required [21].

2.2.4. Data Integrity. Data integrity ensures that the message content is not altered or modified during the transmission process. The task can be done by the public key infrastructure and cryptography revocation mechanism [14].

2.2.5. Nonrepudiation. The nonrepudiation ensures that the sending and receiving entity cannot deny its transmission and reception in case of dispute.

2.3. Threats and Attack of VANETs. The VANETs suffer from different kinds of threats and attacks, and damage caused by these attacks can malfunction the other applications. Also, the negative impact of these attacks influences many applications such as safety, security, comfort, and infotainment applications [14].

2.3.1. Attack on Communication. In VANETs, achieving secure communication is a critical issue because the VANET security suffers from many threats such as certificate replication attack, eavesdropping attack, and location privacy attack.

(i) Certificate replication attack: in the attack, the attacker uses fake certificates and keys of the other users as a proof of authentication without being tracked by the TA. The aim of the attack is to create the ambiguity to the TAs and make harder for TA to identify the malicious vehicle.

(ii) Eavesdropping attack: the attack obtains the confidential information when a nonregistered vehicle uses a valid certificate to gather the useful information of the vehicles such as user ID, location, etc.

(iii) Privacy attack: this attack comprises of different kinds of attacks on privacy-preserving schemes which include tracking vehicle. The attacker can use the target vehicle location, ID, key, and certificate to initiate another attack without being tracked [14].

2.3.2. Attack on Safety Applications. The attacks are related to the channel allocation, as discussed below:

(i) Denial of service attacks: the attack is one of the common attacks in VANETs, the attack occurs when the dishonest vehicle sends multiple messages which blocks all possible ways of communication. The attack can be performed by many attackers concurrently in the distributed way which is called distributed denial of service (DDoS) (see Figure 2) [57].

(ii) Jamming attack: it is one of the dangerous attacks in VANETs security application and happens when the untrustworthy vehicle tries to disrupt the broadcasting communication through different techniques such as consuming heavy power with equivalent frequency range and alert injection (see Figure 2) [58].

(iii) Platooning attack: it occurs when the number of untrustworthy vehicles locate in the same zone or move forward together with the aim of causing disturbance and removing trustworthy nodes from the network operation and restricted them for using bandwidth, etc., as shown in Figure 2 [14].

(iv) Betrayal attack: It happens when a trustworthy vehicle enters in the malicious node and starts to send fake messages [14].

2.3.3. Attack on Infotainment Applications. These attacks discuss the issues related to the comfort and safety of the passengers.

(i) Illusion attack: it is associated with the hardware component which is caused by receiving data from the antenna, and data are collected by the sensor for warning messages of the road conditions which create the illusion to the vehicles nearby [59].

(ii) Inject message attack: it occurs when the untrustworthy vehicle makes many duplicate copies of the same messages or creates a new message by injecting some malicious information and modifying the original messages in the network while behaving like a master node for the intervehicle communication network as shown in Figure 2.

3. Location Privacy in VANETs

The vehicle can be protected to avoid surveillance cameras and monitoring by sending frequent MAC-layer safety messages and accessing location-based service (LBS) application [60]. Generally, without any privacy preservation and wireless eavesdropper, a malicious vehicle can track any specific vehicle by its origin and termination coordinates with work and home addresses by using map database such as Google map, Baidu map, etc. [60]. In the beacon message, any kind of attack such as private, commercial, and criminal attacks can create comprehensive location details and driver profiles [61].

The sensitive and confidential information in the beacon message may lead to reveal the location details of a vehicle. Vehicles are more vulnerable to attack as compared to mobile phones. Firstly, a vehicle should broadcast beacon messages. Secondly, a false measurement cannot be acceptable in beacon messages and, finally, limited traffic rules and regulations and streets for the movement of the vehicles. Based on the beacon messages, the attacker can initiate the attack to acquire the confidential information of the vehicle.

3.1. Threat Model. The ITS is more likely to combine the air traffic control system like LBS system which is referred as traffic management systems (TMSs). By using this technique, the traffic manager can guide the drivers or unmanned vehicles based on their vehicle and traffic conditions [60]. As shown in Figure 3, the global passive adversary (GPA) is used to obtain access to the LBS application data, RSU information, data of cameras, and license plate reader. It also has knowledge of the road maps, road structures, traffic conditions, and name of homeowners with addresses and geographical coordinates. Moreover, the action of GPA is assumed to be passive, which can eavesdrop only and may not alter the data which is to be transmitted. Generally, the attack is a global attack, and the GPA may have access to the data over a large area, in which the whole area is covered by the TMS. The scope of action may be temporary, and GPA may eavesdrop for hours, days, months, or longer period [60]. At last, the main role of the GPA is to find out whether a specific vehicle is at the given place and time in order to target accurately.

3.2. Tracking Attack. Tracking a vehicle is regarded as a multiple target tracking (MTT) issue which considers the sets of observations detected by a sensing device periodically under the specific interval called a scan. The main objective is

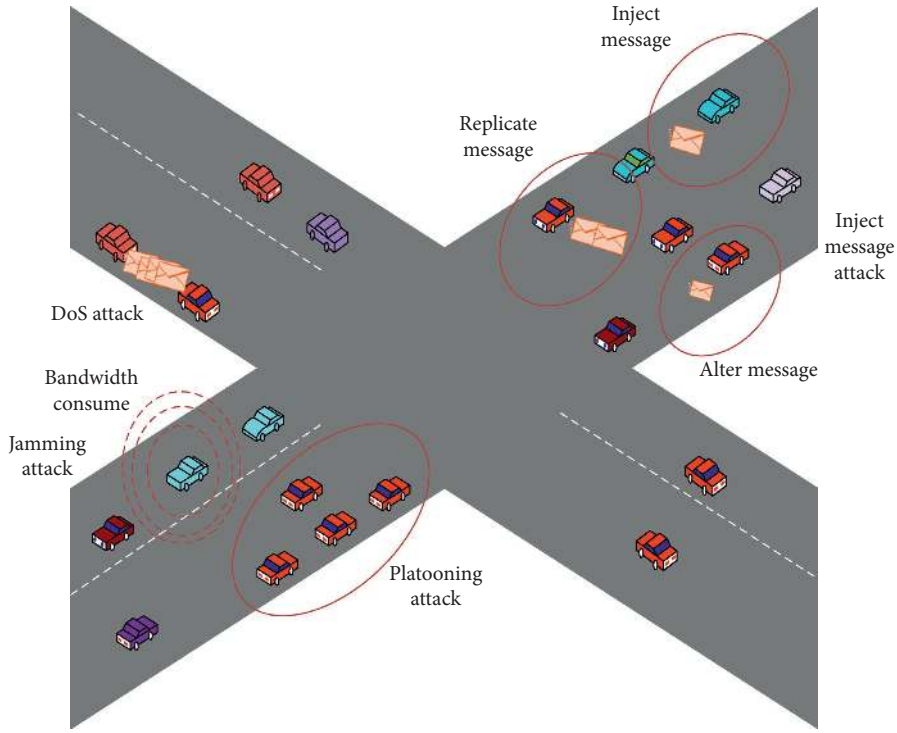

Figure 2: VANETs security attacks.

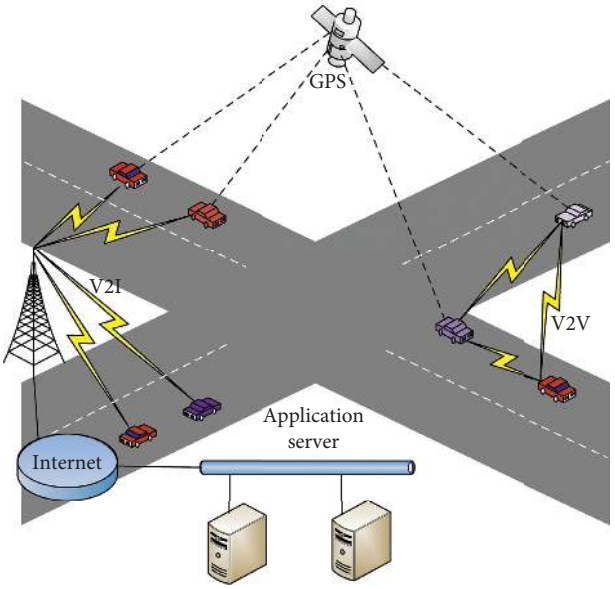

Figure 3: Vehicle diagram for GPA.

to estimate the accurate target and the probability associated with the target in each scan [62].

Figure 4 shows the block diagram of MTT, which consists of gating, state estimation, data association, and track maintenance. These parameters are discussed below:

(i) State estimation: it is important to include some parameters such as position, velocity, and acceleration in the state estimation. It is very difficult to find out the accurate state of the vehicle because the GPS receiver and speedometer are unable to determine the accurate parameters [62]. To track a vehicle with distorted instruments, the exact state assessment of the vehicle is required and can be determined by the state estimation filter [63].

(ii) Gating: in tracking attack, data association is applied to assign each measurement to the accurate target vehicle. Due to high traffic density, a gating should be done prior to state estimation to reduce large computation process. The common gating approach is an ellipsoidal gate. The main objective of the gating is to remove the measurements which unlikely transmit from the target vehicle to minimize the computational consumption of data process [37].

(iii) Data association: it is possible to have measurements in more than one gate. Specifically, the accuracy of data association is suffered due to the distance between vehicles and beacon time interval. Furthermore, the vehicles which require large space and shorter beacon time can create instability in the data association [62].

(iv) Track maintenance: once the measurement is received and does not allocate the previous track, a trial version of a new track is launched until it establishes in subsequent scans [62]. In contrast, if a track is not updated in a short time, then it must be deleted to consume any large amount of computational overhead.

3.3. Protection Technique Against Tracking Attack. A large distorted measurement noise and a longer beacon message

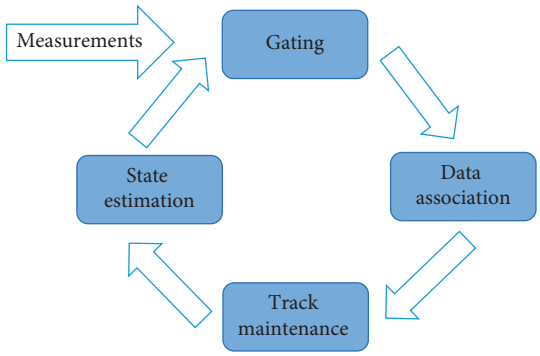

Figure 4: Multiple target tracking component (MTT).

interval cause the tracking attack more complex. The features of LBSs are very crucial to safety applications which require frequent vehicle status to be updated. In order to design and evaluate the privacy protection step, it considers the trade-off between the location privacy and the LBSs quality [64].

In the tracking attack, an attacker should trace the target vehicle apart from other vehicles which exit the same path, and it may cause difficulty if the path has higher traffic flow. Therefore, it is recommended to construct the zones in urban cities that can lead to protect the vehicles from tracked [37]. The efficiency of the mix-zone depends on the number of vehicles entering the zones and changing its pseudonyms. We may face challenges when deploying mix zones in big cities [65]. In 2016, Yu et al. [66] introduced a new privacy scheme named as MixGroup. Its construct extended pseudonyms-changing region in which the vehicles are allowed to successively exchange their pseudonyms. However, it may cause the uncertainty of pseudonyms mixture to be enlarged. Reference [67] indicates that minimizing the accuracy of location information can prevent the location privacy of the vehicles because several LBSs do not require exact information to provide sufficient quality of service to the vehicles.

Emara et al. [64] presented a method to estimate the protection level of privacy and its influence on safety applications by evaluating the correct probability of particular application using Monte Carlo analysis. Additionally, the obfuscation privacy technique is introduced which disturbs position and beacon frequency. The experimental results indicated that it can protect location privacy as compared to mix-zone in terms of increasing tracker confusion; thus, it may cause a negative impact on the safety application. In 2017, Takbiri et al. [68] proposed a method by integrating the major tool to achieve the location privacy by utilizing the obfuscation and anonymization techniques.

4. Trust Management for VANETs

In the VANET, trust management is considered a serious issue. Several authentication methods have been done to ensure that the messages are transmitted from authorized vehicles. VANETs have a decentralized open system and characteristics. Therefore, designing trust in VANETs is a challenging issue. If a peer interacts with the vehicle, there is no guarantee that a peer can interact with the same vehicle in the near future [69]. Thus, we cannot rely on the trusted third party (TTP) to establish a long-term relationship. Specifically, the main function of trust management has to decide whether to trust or not the information declared by authorized users. However, it cannot protect a registered vehicle to send false or bogus messages. Consequently, these messages may cause the delay in the traffic management system and decrease traffic efficiency. In addition to these, it can cause an accident that can threaten human life [70].

Figure 5 illustrates trust schemes model for the VANET to evaluate the degree of trustworthiness of each node and verification of the message authenticity.

4.1. Effective Trust Management Properties. To overcome the challenges of trust management in the VANET, we discuss the desirable properties for the trust management which should be incorporated in the VANETs system.

(i) Decentralized trust establishment: it is appropriate for VANETs because of its dynamic environment. A key infrastructure is used to verify the roles of each vehicle drivers in a distributed way. The reliability of vehicle is evaluated by using V2V interaction or relying on the actual driver's condition [37].

(ii) Scalability: it is a vital part of the trust management; during the peak hours, a large number of vehicles passing through the network may be higher. In case of emergency situations, a peer needs to take the decision very fast. To fulfill this requirement, each peer can only accept information from trustworthy peers, and established trust in the VANET should be scalable.

(iii) Privacy: it is a challenging part for the trust management, revealing a vehicle owner ID, such as owner home address, may cause any malicious user to attack and create the damage. The trust management can use public key infrastructure which can allow nodes to authenticate each other.

(iv) Robustness: the trust management can improve peers collaboration and detect malicious nodes. However, sometimes the trust management becomes the target of attacks and compromised [69]. The trust distortion can misguide the trusted network operations by misleading the reliable computation, and also, the reliability of another node maybe distorted [71].

(v) Information sparsity: in the trust management, the information sparsity is dominated in VANETs and the data might be termed valuable. The information which is received directly has an important value, and the weightage of this information must be increased in trust calculation mechanism.

4.2. Model for Trust Management in VANETs. Recently, several methods have been proposed based on the third party [72–74]. Li et al. [72] proposed an announcement scheme for

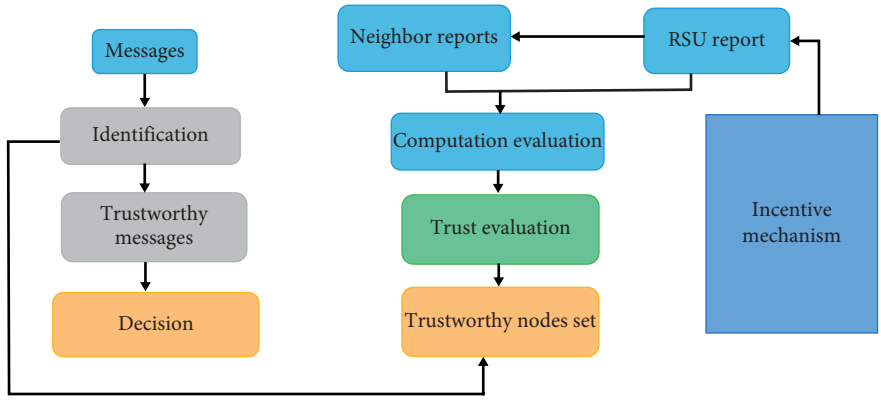

Figure 5: Trust management schemes in VANETs.

VANETs based on the reputation system, which can evaluate the message reliability. In the case of unavailability of the central server, this method relied on fault tolerance and robustness. Li et al. [73] proposed a reputation-based global trust establishment (RGTE). By applying statistical laws, it can share trust information in VANET safely. Therefore, this method achieved a more efficient and accurate way to develop trust in the changing environment. Bißmeyer et al. [74] introduced a central technique, which uses the reliable information provided in misbehavior reports to ensure the safety and functionality of the network in the VANETs. Recently, some existing works have been utilized based on different architectures in which some are RSU-based technique, and other methods which can deal with the privacy of trust management. Furthermore, in recent years, many research works consider official vehicles such as police cars and ambulances and many work use private vehicles such as cars and taxis.

Specifically, existing trust models are categorized based on the network topology and vehicles orientation: (i) internal cluster communication, a vehicle decision depends on the opinion of the clustering member, (ii) smooth communication in which all the vehicles behaves autonomously, and (iii) vehicles within the vicinity of RSU and act as sinking handle all communication [14]. Recently, a cluster-based approach is used to established trust management in VANETs [75–78]. Wahab et al. [75] introduced a new method, in which they address the problem of identifying misbehaving vehicles in VANETs by using the Quality of Service-Optimized Link State Routing (QoS-OLSR). This technique utilized the phase modeling to encourage nodes to behave mannerly during the cluster formation process, and it can also detect malicious users once clusters are established. Sedjelmaci and Senouci [76] introduced an accurate and lightweight intrusion detection method called AECFV, which aimed to prevent VANETs against possible severe attacks that may happen frequently. AECFV is suitable for high node mobility and rapid topology change. In this scheme, stable clusters are formed with sufficient connectivity, and then the cluster-heads (CH) are elected based on vehicle mobility and trust level.

Yang et al. [77] proposed a method which utilized RSU to develop a cluster-based trust management. In this scheme, V2V- and V2I-based CH is generated which is also responsible for the cluster management. Ltifi et al. [78] proposed a Petri Net to design smart vehicles which is responsible to take decision based on the reliability of messages. These methods are very robust which enhance the communication between vehicles in the VANETs by constructing a cluster and electing CH based on algorithm [37]. The major drawback of trust-based management comes from the VANETs because of its ephemeral characteristics. The correctness of CHs decision relies on the cluster scale, which indicates that it might be possible that cluster-based methods can fail in the area where vehicle flow is lower. Additionally, it is a very critical issue to maintain stable cluster for trust management [37].

In [79], Mehdi et al. presented a game theory-based trust model for VANETs. In this scheme, an attacker and defender security game was responsible for the detection of malicious nodes. The results obtained from the simulation revealed that the presented method obtained better performance in terms of throughput and data drop rate of different attackers as compared with other methods. In [80], Goli-Bidgoli and Movahhedinia introduced an effective trust management system for cognitive radio VANET (CR-VANET). This technique relies on the birth and death process (BDP) to evaluate the average delay influenced by the decision-making process. The proposed method obtained a better accuracy of event detection and also significantly reduced the complexity of the decision-making process. However, it required a large amount of computational time to process each event. Ahmad et al. [81] presented a trust evaluation and management (TEAM) framework for designing, evaluating, and managing trusted models in the presence of malicious nodes. The proposed framework was tested with different trusted models (i.e., data-oriented, entity-oriented, and hybrid) in terms of four different VANETs contexts based on the mobility of honest and malicious vehicles. Mehmood et al. [82] proposed a hybrid trust management technique to identify malicious vehicles. This scheme utilized a composite metric assigned to vehicles which coupled with available resources for a selection of cluster head and proxy head selection through an intermittent election. This method produced a trustworthy and efficient vehicle network. The decentralization trust models do not rely on static

infrastructure. These models are further categorized into three types: entity-oriented trust model, data-oriented trust model, and hybrid trust model.

4.2.1. Entity-Oriented Trust Model. The entity-oriented trust model ensures the trustworthiness of the vehicles [25]. Recently, a new method to evaluate the distrust level has been proposed for each neighbor, which acts as a black hole via the watchdog technique. In this approach, the distrust level will be forwarded to the regional cluster head and then delivered to the trusted party that may cancel the certificates of attackers [83]. This scheme did not discuss the steps which were involved during the communication process and its computational overhead. Kerrache et al. [84] introduced a trust-based routing protocol for vehicle urban environment called TROUVE. This scheme used to find the shortest and very reliable path to the destination by considering the real traffic information and malicious nodes in the network. Minhas et al. [85] developed a multifaceted trust modeling technique to obtain useful and trustworthy information. They incorporated integrated roles, experience, and majority-based trust to provide a real-time decision. It also integrates different dimensions of trust which can be effectively applied in V2V communication through intelligent agents. Haddadou et al. [86] introduced a new method based on a distributed trust model (DTM^2) to overcome the presence of malicious nodes that circulate the wrong information and forged data, and it can also handle selfish nodes which are only cooperating for their own benefit. In this scheme, based on nodes' behaviors, DTM^2 requires the cost sending by utilizing the signaling values. Therefore, the sending cost is higher which can affect the participation of nodes in the network. In [87], Kerrache et al. introduced risk-aware trust-based architecture (RITA) to evaluate the trust among vehicles for an independent period. This scheme utilizes a multihop broadcast communication technique for V2V and V2I message communication that could ensure efficient dissemination of safety messages. However, the proposed technique introduced a new risk evaluation metrics to trust-based metric.

(1) Entity-Oriented Trust Model based on Weight. In several trust models, the trust value depends on the direct trust and the recommendation [88, 89]. The weight notion is used to indicate the different kinds of applications and users to assess the direct trust and recommendations [90]. The trustworthiness of a node is associated with the application data and the node authority level. These weights are defined, respectively.

Traffic safety data play an important role to ensure the safety of travelers. Three different kinds of application data with A, E, and O, respectively. Specifically, the requirements of security analysis and three different kinds of application data, which influence the traffic safety, are written as follows:

$$W(y) = \begin{cases} 1, & y = A, \\ 0.8, & y = E, \\ 0.5, & y = O, \end{cases} \tag{1}$$

where $W(y)$ is the weight of application data and y indicates the number of application data.

(2) Node Weight. Nodes in VANETs contain different types of vehicles such as an emergency vehicle, ambulance, private cars, ride-sharing vehicles, and roadside units. The nodes are classified into three different types in the VANET such as high-level nodes, middle-level nodes, and low-level nodes. Specifically, the information reported by the high-level nodes has higher trustworthiness as compared with the other levels nodes. In the entity-oriented trust model, a node-level is associated with the trust value.

$$W_n(y) = \begin{cases} 1, & y = H_n, \\ 0.7, & y = M_n, \\ 0.5, & y = L_n, \end{cases} \tag{2}$$

where H_n, M_n, and L_n are the high-level nodes, middle-level nodes, and low-level nodes, respectively. In the entity-oriented model, the nodes' weight indicates the data trustworthiness up to some level.

(3) Comprehensive Trust. The comprehensive trust is the combination of direct trust and recommendation. The direct trust must not be fixed and can be changed with the node:

$$\gamma = \begin{cases} 1, & D_t \in (0.7,\ 1] \text{ or } D_t \in [0,\ 0.2) \text{ or } W_n = 1, \\ D_t, & D_t \in [0.5,\ 0.7), \\ W_n \cdot D_t, & D_t \in [0.3,\ 0.5). \end{cases} \tag{3}$$

From equation (3), we can see that γ changes with D_t and W_n. These two parameters are responsible to maintain the balance between recommendation and direct trust in order to provide cost efficient solution:

$$T_a = \gamma \cdot D_t + (1 - \gamma) RT_a. \tag{4}$$

Based on the weight, the dynamic trust model is represented in equation (4), and the weight of T_a between 0 and 1.

4.2.2. Data-Oriented Trust Model. The data-oriented trust model can easily recognize the fastest trustworthiness evaluation, when the node R receives the data report μ generated from node q, so the data trustworthiness is evaluated by

$$B_\mu^q = 0.7 T_r^q M(\tau(q),\ \tau(\mu)) + 0.15\,\beta_1\ (q,\ \mu) + 0.15 + \beta_1\,(q,\ \mu). \tag{5}$$

For the same event, several trust values of the same event from different reporters can be used as the final trust value [90].

The main aim of the data-oriented trust model is to focus on the evaluation of the trustworthiness of the received data [25]. This model requires detailed information from various sources such as RSUs and vehicles to verify the received data. To overcome the limitations of several methods that measure

trust in the history of interaction and the infeasibility for VANETs due to its ephemeral nature, Shaikh and Alzahrani [91] presented a new trust management technique to identify the anonymous vehicle, and it can also detect the false location and vehicle information. This scheme achieved high accuracy, but it may introduce a large delay which is not acceptable for VANETs safety applications.

Huang et al. [92] introduced the implementation of cascading and oversampling to the VANETs and developed the voting system, in which each vehicle had assigned different weights that depend on its distance from the event. In case, a vehicle closer with the event contains a higher weight. Gurung et al. [93] introduced a method that can directly evaluate the trustworthiness of message contents received from vehicles. In the scheme, a model was designed by considering several factors such as content similarity and route similarity. Hussain et al. [94] proposed a method that addressed the trust management problem in the vehicular social network (VSN). Therefore, the problem is overcome by using two trust establishment and management solutions in terms of email and social network-based trust to develop a trust level. In [95], Kerrache et al. introduced a trust-routing protocol based on the intrusion detection system (IDS) and data-centric verification framework. This scheme can prevent VANETs from DDoS attacks and also enhance the intervehicle communication. The proposed method obtained better detection of malicious nodes and messages which are either send by trusty or untrustworthy vehicle. However, the authors did not provide many details about the detection algorithm. In particular, the main disadvantages of data-oriented models are sparsity and latency, respectively, because data acquired from different sources contain redundant information which can result in larger latency [37].

4.2.3. Hybrid Trust Model. The hybrid trust model is used to assess the level of trust and also analysis the trustworthiness of vehicle data [96]. To handle with the black holes and the gray holes procedure, in recent years, several works have been proposed on hybrid trust models [76, 86]. Sedjelmaci and Senouci [76] introduced the two-level intrusion system, in which the first system is based on the collaboration of in-cluster detection, and the second system relies on the detection process by the RSU globally. The main disadvantage of this technique is that it is associated with the large computational time for selecting the cluster head. Li and Song [97] introduced an attack-resistant trust management (ART) scheme which could detect and cope with the malicious attacks that are often influenced by dishonest vehicle in the VANET. Firstly, this method determined the trustworthiness of the data which are gathered from different vehicles, and node trust is evaluated based on the functional trust and recommendation trust. The proposed method did not consider the data sparse and privacy which are necessary for trust management in the VANET. Hasrouny et al. [98] proposed a security mechanism based on vehicle behavior analysis. This technique utilized the hybrid trust model (HTM) and the misbehavior detection system, in which the trust metric is dedicated to each vehicle depending on its behavior. By selecting the trustworthy node as a group leader, the HTM ensures secure communication between the vehicles and the back-end system. Then, vehicles and a group leader can cooperate with each other to detect the malicious nodes in VANETs and to notify them to the network authority. The proposed scheme obtained better efficiency in terms of selecting trustworthy vehicles and to monitor their behaviors. However, the proposed method did not consider the trust level, which could ensure communication in VANETs.

4.2.4. Different Trust Establishment Model. In recent years, some of the works do not specify any category of the model, nor does it indicate any types of attacks. However, these works can be classified under trust establishment related to intervehicular communication. Jesudoss et al. [99] method falls in the entity-oriented category. This method proposed a payment punishment scheme (PPS) integrated with different models to evaluate the trustworthiness in the election process of the nodes in a cluster. In this approach, each node in a cluster cooperates with other nodes to acknowledge the exchange of communication between nodes and clusters. This method does not provide indirect and direct trust metrics which may lead to decrease the performance in case of high mobility. Chen and Wei [100] presented a trust scheme based on beacon mechanism to improve the location privacy in VANETs. In this scheme, the vehicle can utilize indirect and direct messages to develop trustworthy relationship, which then subsequently leads to differentiation between trustworthy and untrustworthy messages. This method can significantly protect the location privacy, but cannot evaluate different kinds of messages and is unable to detect any attack in high mobility, upper layers, etc. Gerlach [101] introduced construction of the trust model based on node reputation which is able to provide secured communication and protect the location privacy of the registered vehicles. In this approach, belief trust is evaluated by using three different metrics. The demerits of this method are that it exchanges traffic information with limited information. Rostamzadeh et al. [102] introduced a trust-based framework to broadcasting safe information in VANETs. This method introduced two-layer trust dissemination called FACT, which is used to maintain the trust value. It makes sure that the message broadcasting from trustworthy nodes and the content is valid and then selects the best path to deliver the message to the receiving nodes. This method required large amount of computational time because of checking the authenticity of message content. He et al. [103] proposed a unified trust management scheme for dealing with spectrum sensing and data transmission process in cognitive radio VANETs. In this method, the weighted consensus spectrum is applied to protect the sensing process and also improve the security of data transmission process by utilizing the trust value in CR-VANETs. This scheme did not cover comprehensive trust management and security performance of VANETs.

4.3. Comparison of Cryptographic from Trust Management. Trust management is regarded as a security to indicate the limitations of cryptography solutions, and it requires valid

certificates to tackle inside attackers. For the security of the VANET network, the trust and cryptography are able to tackle a single or a group attacker inside the network. The trust and cryptography cannot prevent from inside attackers, while both of them can handle active attackers alone, but are unable to detect the passive attackers since they did not perform any malicious activity [14].

Table 1 shows the comparisons between cryptography and trust management in terms of VANET security services targeted by each attack. It identifies which category, i.e., trust or cryptography is better to deal with these attacks.

5. Trust Management Simulation Tools of VANETs

In order to evaluate the performance of existing trust models of VANETs, it is necessary to design the simulation tools to simulate these trust models. This task can be accomplished by using the simulation tools that provide the closest results of a particular model. Different types of simulation tools have been used to evaluate the performance of these models, such as the network simulator NS-2 [104], NS-3 [105], and Matlab [106]. Furthermore, several approaches utilize other simulation tools such as TRMSIM-V2V [107], TraNS [108], VanetMobisim [109], and Veins [110] to evaluate the performance of their trust models. Also, some authors simulate their trust model by developing their own simulation tools to evaluate the performance of their proposed models instead of using simulation tools which are built from C++ and Java programming languages.

Figure 6 shows the VANETs trust management tools which are used to evaluate the performance of trust models. Evaluation of trust models can be performed by several ways such as simulation tools, theoretical and analysis approach, and analytical method, respectively.

In VANETs, mobility models determine the movement of nodes which is further connected with the simulator. This connection enables the simulator to generate random topology depending on the condition of each node in the vehicular network [6]. The challenges arise due to the unique characteristics of VANETs as compared to other network. The mobility model contains two patterns: traffic pattern and motion pattern. Motion pattern relates to the movement of drivers which creates vehicle movement along with the pedestrians and the surrounding vehicles. Traffic generator provides geographical maps and topologies and evaluates the vehicle behavior depending on the road environment [6]. The performance of the vehicular network depends on the mobility model. In past, several methods have used the mobility pattern to obtain the reliable vehicle mobility for simulating VANETs.

6. Applications of VANETs

The main objective of VANETs is to facilitate and coordinate with other vehicles. VANETs safety application includes collision prevention system, lane-changing notification, and road bottleneck notification in case of emergency and traffic incident. Comfort applications provide infotainment, Internet, online gaming, and music to the passengers. VANETs applications are further classified into several other categories depending on the traffic event and conditions [1]. In the past, several methods classified VANETs applications into two types: safety and comfort applications [55, 111]. In [112], the authors described VANETs application more deeply by classifying into traffic efficiency, road safety, and entertainment applications. Ducourthial and El Ali [113] further extended the classification of VANETs, which include driver and vehicle applications, as shown in Figure 7.

6.1. Driver Application. This application helps drivers to guide and assist them on the road in case of any road bottlenecks, collision, traffic incident, traffic congestion, accident, etc. And, this application provides parking guidance and notification and toll booths collection [19].

6.2. Safety Application. This application is used to enhance the travel safety to avoid any severe incidents. Communications between V2V and V2I are used to improve traffic safety by providing traffic safety warning, lane-changing warning, collision warning, etc. This application ensures the safety of passengers, pedestrians, and drivers [49].

6.3. Comfort Application. This application provides comfort to the drivers and passengers with different types of entertainment services such as music, messaging, online games, communication between vehicles, and Internet access [49].

6.4. Vehicle Application. This application allows the driver to provide information for their vehicle to improve vehicle safety, improve the vehicle automation system, and enhance the vehicle safety on the road [1].

7. Evolution from VANETs to VCC

The VCC has been an emerging paradigm, evolved from VANETs. It has been receiving significant attention from the research community due to its features and ability to support many computing applications. This great development in the vehicular network technology has produced significant improvement and growth to the vehicles in terms of vehicle resources, computing, and storage capacity [114]. A new technological shift from the VANETs to VCC utilizes the benefits from the cloud computing technology to enhance the safety of the travelers and driving experiences of the VANET drivers. The main aims of VCCs are to provide various computing services to the drivers at low costs, such as reducing traffic congestion, improving traffic flow, reducing number of incidents, improving traffic environment, and enhancing road safety.

Figure 8 shows the paradigm evolution to the VCC in which the existing techniques are outline. These techniques are the integration of vehicular network and cloud computing, as shown in Figure 8. The VANETs are an extension of MANETs, in which the communication is between nodes

Table 1: Security services target and solutions.

Name of attack	Service	Trust-based	Cryptography-based
Betrayal attack	Authenticity, availability, integrity	×	—
Replayed, altered, and injected message attack	Authenticity, availability, integrity	×	×
Illusion attack	Integrity	×	—
Masquerading attack	Authenticity	×	—
Impersonation attack	Authenticity, nonrepudiation	×	×
Sybil attack	Authenticity, nonrepudiation	×	×
GPS position fake attack	Authenticity, nonrepudiation	×	—
Timing attack	Availability	×	×
Black hole attack	Availability	×	×
Gray hole attack	Availability	×	×
Certificate replication attack	Authenticity	—	×
Eavesdropping attack	Confidentiality, privacy	×	×
Tracking/tracing attacks	Privacy	—	×
Denial of service attack	Availability	×	×
Jamming attack	Availability	×	×
Coalition and platooning attack	Availability, privacy	×	—

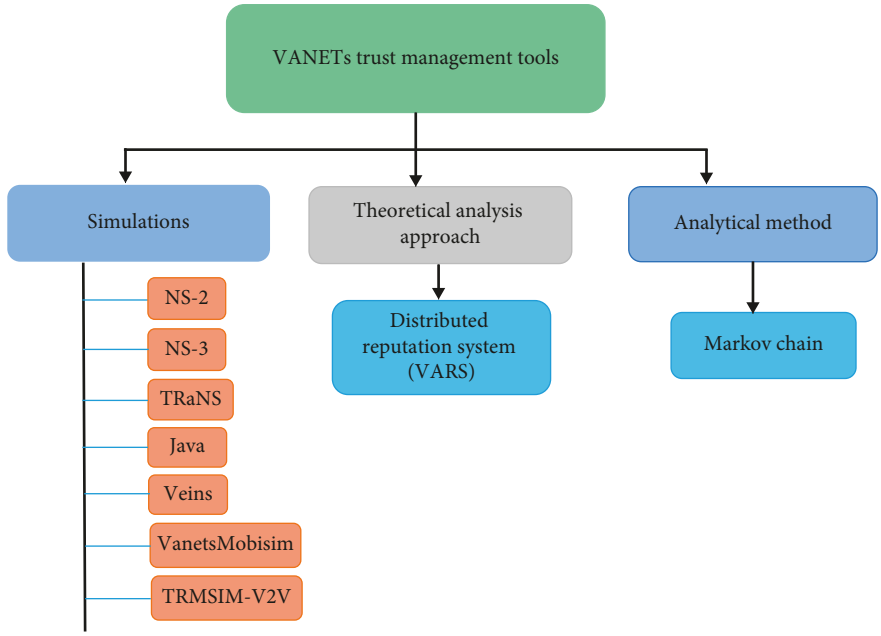

Figure 6: Simulation tools for trust management in VANETs.

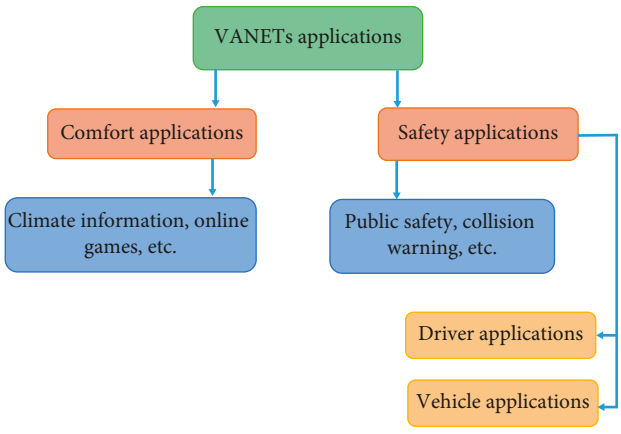

Figure 7: The VANET applications.

in single-hop and multihop. Based on the vehicular network, the VCC has emerged, which is an extension of mobile cloud computing (MCC) [29].

7.1. Vehicular Cloud Computing. In recent years, the vehicle industry has achieved a significant development to design smart vehicles, which consists of robust computing, communication module, and storage and energy resources. VCC exploits vehicle resources, in which the vehicle acts as a cloudlet to the other devices. These resources brought benefits to the vehicle industry by performing different services. However, these resources are not efficiently utilized. On the other hand, many vehicle resources remain in the idle stage for a longer time when the vehicles are in the parking area or in the congested areas. In other words, some vehicle

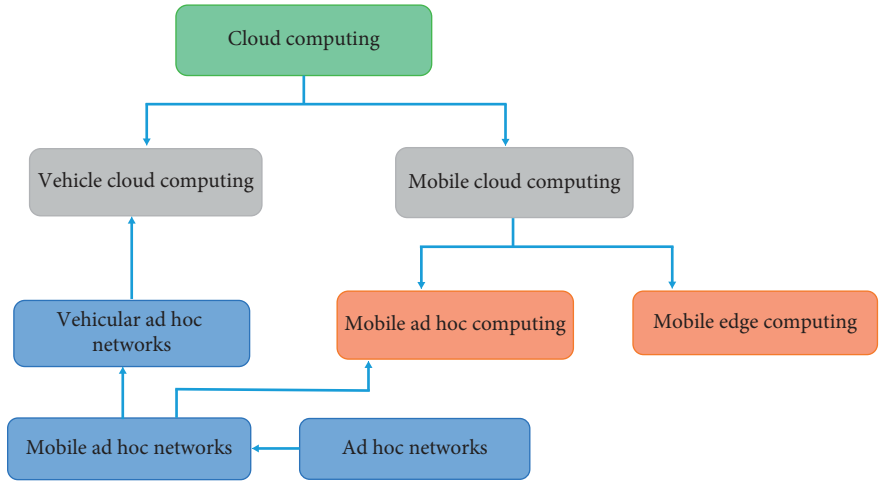

Figure 8: Paradigm to VCC.

does not have the capability to run some resources, such as downloading media applications, while some vehicles can use the available resources.

The VCC is the combination of cloud computing (CC) and VANETs. The VCC forms a cloud with the nearby vehicles on the road to perform the assigned task and other services; the vehicle can be a user or resource service provider similar to MCC, and the roadside infrastructure, such as RSU can be a part of the VC [115]. Several research works outline the VCC overview and architecture and discuss the design requirement of VCC [16, 116]. These schemes presented the VCC structure, which aims to gather, allocate, and utilize the available resources on the vehicles. These resources have capability such as processing, storage, communication, and sensor, which can be significantly harvested in a group of vehicles legitimately. More specifically, the drivers, passengers, traffic authorities, and cloud users can get the benefits from the aggregations of these resources and make them available as the cloud services in open-access [30].

In the VCC, a group of vehicles can communicate and share resources through the vehicle-to-everything (V2X) i.e., V2V and V2I communications. Vehicular cloud network is illustrated in Figure 9, in which vehicles can communicate with the cloud data center by using RSUs and the other vehicles can access the cloud when they are in need. Due to the wireless characteristics, it is very unlikely to develop secured communication between the vehicles and RSUs.

7.2. Vehicular Cloud Architecture. The vehicular cloud can be accomplished by several ways such as on-demand cloud, permanent cloud, and/or combination of both clouds. On-demand cloud is formed as a temporary purpose, which can be accessed by registered members or nearby users. Permanent cloud can be accessed in any form such as the vehicles can communicate with the cloud by using RSUs or directly through the 3 G/4 G links. To analyze the selection criteria of cloud services, vehicular cloud architectures can be classified into three different categories, as shown in Figure 9 [29].

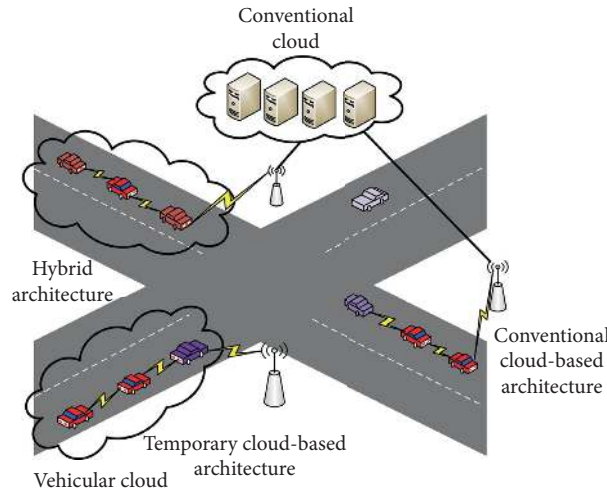

Figure 9: Vehicular cloud network.

(i) Temporary cloud architecture: in the temporary-based architecture, the moving vehicle can act as an infrastructure temporarily to accomplish the task. On the other hand, the vehicle can also accomplish this task by sharing resources such as downloading contents from the Internet. In some cases, depending on the traffic scenarios and conditions, the integration of infrastructure is not always required [29].

(ii) Permanent cloud architecture: in permanent-based architecture, only the vehicles which formed the vehicular network can get the access to the cloud data centers by using wireless and satellite communications. Vehicles can share information between each other and with the cloud data center [29].

(iii) Hybrid architecture: the hybrid architecture is the combination of the temporary cloud architecture and permanent cloud architecture. To accomplish any task, vehicles can get access to the permanent cloud by forming a temporary cloud [29].

8. Security and Privacy in VCC

8.1. Privacy and Security Issues. The VC is affected by the security and privacy issues of the vehicular network [21] and cloud computing [117]. There are many security issues in the VC, which consists of unregistered and malicious nodes, vehicle locations, vehicle privacy, and trustworthiness between the VC members. Generally speaking, the security and privacy are the major issues for the VC due to utilization of the wireless network, which allow users to share the same resources [17].

8.1.1. Vehicle Privacy. In vehicular communication, users' information such as vehicle location and identity are disclosed. Unregistered vehicles can track the vehicle's location, which may threat the vehicle privacy [29]. Pseudonyms are used to protect from privacy attacks. In recent years, several works regarding pseudonyms have been proposed, which ensured the vehicle privacy and discussed different mechanisms to maintain the conditional privacy of users [118, 119]. Pseudonyms are able to protect the vehicle privacy. However, it is affected in the absence of trust between the cloud members [29].

8.1.2. Trustworthiness between VC Members. The trust between vehicles plays an important role to ensure the secured communication in the VC. The vehicles form a collaboration to perform several tasks, which are required to evaluate the trustworthiness of vehicles. An attacker can be a cloud member which can attack the user, i.e., in the traffic safety and management applications. To overcome this issue several works have been proposed in VANETs [120, 121]. The main aim of VC is established, in which the member can join and leave the cloud anytime in the dynamic trustworthiness mechanism [29].

8.1.3. Malicious Nodes. Malicious nodes refer to the nodes which affect the performance of the vehicular network such as VANETs and VC. In the VANETs, several research works have been proposed to deal with these issues [86, 121]. Also, several methods are proposed to detect the malicious node in the VC [122, 123].

Figure 10 shows the security and privacy issues of VC, such as security services, threats, and challenges. It is vital to indicate the security requirements where the system must be in-line with the network operation in order to provide secure communication in VC. In security threats, several issues threatening the security of VC are illustrated.

8.2. Vehicular Cloud Threats. In recent years, the demand of using VC significantly increases the chances of various security and privacy issues [124]. These issues threat the security of the vehicular cloud computing. VCC security threats can be categorized into several groups, which are discussed below:

(i) Denial of service (DoS): the denial of service is a very common attack on the vehicular cloud, which aims to attack the VC in order to make the resources unavailable to the other cloud users [125].

(ii) Identity spoofing: this attack allows a malicious user or application to misuse other registered user identity and security credential [126].

(iii) Message tampering: this attack normally occurs when the attacker modifies or alters recent message data to be transmitted [127]. For instance, if the route is congested, the attacker alters the data to clear the road which can influence the users to alter their driving paths.

(iv) Information disclosure: this attack occurs by obtaining the useful information of the system in the absence of data privacy.

(v) Sybil attack: this attacker can manipulate the other vehicle behavior, and the receiving vehicle thinks that the messages are transmitting from the different vehicles. Thus, the vehicle may feel that there is a congestion on the road, so they enforce vehicles to alter their paths and leave the road clear.

8.3. Vehicular Cloud Security Services. There are several security requirements where the system must be matched with the cloud computing network. They are categorized into five main domains:

(i) Confidentiality: it ensures that confidential data should not be disclosed to the outside nodes.

(ii) Integrity: it ensures that the message contents are not modified during communication process, and the message must be valid.

(iii) Availability: data resources must be available whenever it is required by the vehicles.

(iv) Authentication: it protects the VC against suspected nodes in the network by verifying the user identity and sender address before allowing them to access VC.

(v) Privacy: it is used to protect sensitive and confidential information of the vehicles or passengers from the attackers.

8.4. Vehicular Cloud Security Challenges. There are many security challenges in the VC which occurred due to high mobility of nodes such as node authentication, localization, access control, data security, secure vehicular communication, and certificate revocation [17].

8.4.1. Node Authentication. The authentication plays a very important role in the VC which verifies the user authentication and message integrity before allowing vehicles to access the vehicular network. In the vehicular network, anonymous authentication is a very common approach [128]. In the past, many authors utilize the pseudonym-based approach which is able to protect the vehicle security

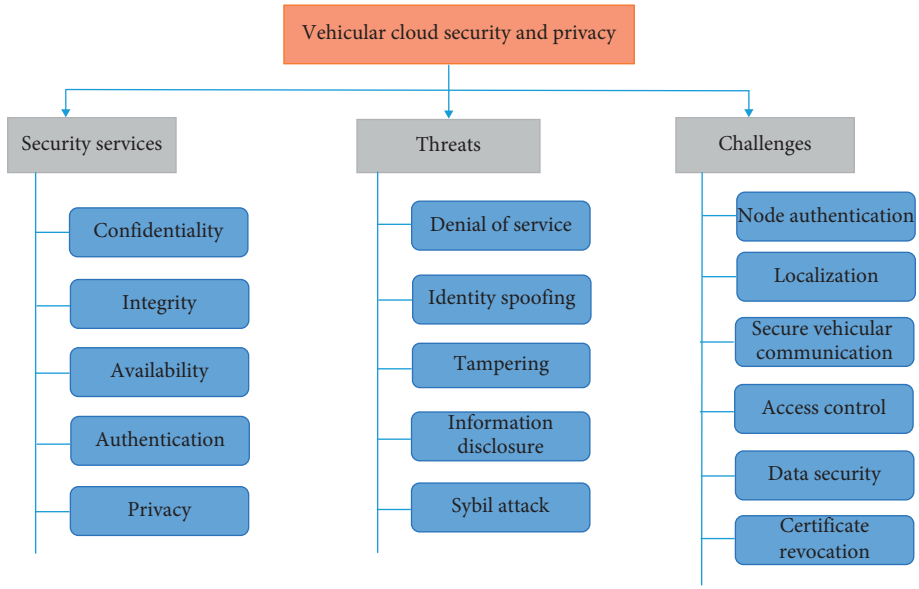

Figure 10: Security and privacy of vehicular cloud.

and privacy. Verifying the sending messages using the location-based authentication method in VC is very difficult task because of high mobility nodes, in which the location of vehicles is always changing [129]. Secure privacy-preserving location-based services (LBSs) are introduced which provides the authentication, integrity, and nonrepudiation for the vehicle and service provider in each LBS event, which subsequently leads to secure the privacy of the vehicle during LBS event [130]. Zhang et al. [131] introduced a secure and privacy-preserving communication scheme for establishing vehicle cloud (VC) and broadcasting data in VC. Once the VC is formed, any cloud user can process their data securely.

8.4.2. Localization. In the VCC, vehicle location information plays an important role, which is able to broadcast data and develop connection because many applications depend on the traffic-related information such as collision warning, lane-changing warning, and emergency warning [17]. There are three models in the VCC to evaluate and integrate the location information. The first one is the active location integrity model, and it can validate vehicle locations by using location devices such as radar and GPS. The second one is passive location integrity, in which the location of vehicles is very difficult to access without using the radar. The third one is a general location integrity model that evaluates the high-level location accuracy from low-level accuracy by filtering the false location in the VC [17, 129].

8.4.3. Access Control. One of the challenging issues in the VC is access control, in which the user identity is checked prior to the gaining access to the network resources. Different access control levels are predefined, in which every user associates with their dedicated cluster based on its characteristics in the network [132].

8.4.4. Data Security. The vehicular cloud offers an effective method which can be used to accommodate computational and storage resources of the vehicles. If the vehicles do not consider the security requirements, the vehicles are able to access and stored data on other vehicles. Thus, the stored data must be encrypted to avoid unauthorized access [17].

8.4.5. Secure Vehicular Communication. As shown in Figure 1, the vehicles and infrastructure such as RSU and traffic light are able to communicate and exchange traffic-related information with each other in terms of V2X communication, i.e., V2V and V2I in the vehicle cloud computing. In vehicular communication, the secure communication plays a very important role which could provide safer and efficient driving experiences. Vehicle communication in an open-access environment which makes VC more vulnerable to attacks, such as jamming signal, inject, modify, or delete the messages disseminated in VC. For instance, if the attacker altered messages, they may spread false information on the road that leads to cause traffic congestions on the road, traffic incidents, accidents, hazards, etc.

8.4.6. Certificate Revocation. The certificate revocation is a robust technique which can protect the data from the attacker or malicious entries. When an attacker certificate is detected, the authority revoked the certificate [133]. In the vehicular network, the certificate revocation list (CRL) plays an important role which managed the list of revoked certificates and broadcast the CRL between vehicles immediately [17]. Raya et al. [134] introduced the revocation protocol of tamper-proof devices (RTPD), in which certificate authority (CA) is responsible to delete the pair keys of each vehicle, then it generates a revocation message, which is encrypted with the vehicle public key, and then it is forwarded to the other vehicle.

9. Open Research Challenges in the VANETs and VCC

We discuss the various open issues and research challenges for the VANETs and VCC, which are used for successful deployment of VANETs and VCC. The VCC is very complex in nature that needs to be configured and designed. The open research challenges in the VANETs and VCC are discussed below.

9.1. Challenges in VANETs. Security and privacy are considered as a challenging issue in VANETs since the messages are broadcasted in an open-access that makes VANETs more vulnerable to attacks that could affect human lives. Security and privacy and trust among vehicles remain a critical issue. The open research challenges in VANETs have been identified and are discussed below.

9.1.1. Security in VANETs. The security plays an important role to ensure the secure communication in vehicular networks. As the communication takes place in an open-access environment, which makes VANETs more vulnerable to attacks that causes multiple threats to the security services. In particular, Sybil attack is one of the most dangerous attacks in VANETs. Maintaining the balance between privacy and nonrepudiation is still required in order to detect Sybil attack. In the past, many works have been performed on the Sybil attack. On the other hand, many other attacks such as jamming attack and malware attack in VANETs need to do further research. Many security challenges still exist, which need a great algorithm in order to solve these challenges. The robust authentication techniques along with the message exchange approach could be used to protect the V2I and V2V communications from inside and outside attackers. For instance, those techniques can perform the robust authentications between OBUs and RSUs without considering any delay. Also, the utilization of certificate authority (CA) or trusted authority (TA), and the techniques which rely on public and private keys for V2V and V2I communications resulted in high computational overheads and also do not provide scalability. We need to determine fast message exchange mechanism, where computational overheads remain same with the RSUs coverage area. In [135], Kang et al. presented an access control authentication scheme for disseminated messages in VANETs. However, the proposed scheme did not consider the delay caused by message verification and communication overhead. Moreover, this technique does not provide traceability in case of any dispute. In [136], Azees et al. proposed an efficient anonymous authentication with conditional privacy (EAAP) to prevent malicious node entering in VANETs. In this technique, the signatures verifications are performed sequentially which could introduce the verification delay up to 300 ms [137].

In short, managing certificates can result in the delay of message verification and overheads of broadcasting of messages signatures. Also, the involvement of the trusted third party to verify vehicle information such as vehicle identity and certificates may limit the scalability in the VANET. Therefore, we need an efficient authentication technique (i.e., message authentication) to ensure secure communication in VANETs.

9.1.2. Group Key Distribution in VANETs. In VANETs, the group signature is one of the robust privacy-preserving authentication techniques, which could be used to ensure the secure communication in VANETs. However, the group keys secure distribution for fast moving vehicles is still a critical issue. In [138], Sampigethaya et al. designed a scheme called AMOEBA. This scheme can provide location privacy by building the group, in which the group members are responsible for sending messages to their respective group leaders. This scheme protects the privacy of all group members by risking the group leader's privacy. However, the group members' privacy could be revealed when the group leader is compromised. In [139], Islam et al. presented a password-based conditional privacy-preserving authentication and group-key generation (PW-CPPA-GKA) protocol for the VANET system. This protocol provides multiple features such as group key generation, user leaving, user entering, and changing password. However, a large number of users leaving and entering areas could significantly increase the computational time. In [140], Lim et al. presented a key distribution technique to perform the verification of group signatures. In this scheme, a group is divided into multiple roadside units for distributing traffic from TA. The proposed technique provides a mechanism to deliver group keys to nodes and also ensure the vehicle security. However, a large number of RSUs could make the VANETs system more complex.

From the abovementioned scheme, we can analyze that the researchers of communication technology background should focus on security and privacy and scalability of key distribution scheme for group-based signature authentication.

9.1.3. Privacy-Preserving LBI. The schemes for silent period [141] and mix zone [65] of location privacy have been proposed to prevent linking pseudonyms in VANETs. However, the existing privacy-preserving schemes do not provide privacy for LBI in traffic management due to future-reported LBI could be used to connect pseudonyms. For example, after a silence period, vehicles A and B change their pseudonyms at the same time. An attacker can use the reported future of LBI to associate pseudonyms, i.e., to identify that (A, A') and (B, B') belong to the same vehicle. Therefore, the route trip could be restructured and the vehicle driver can be traced from the specific location where the vehicle travels. In [142], Zhang et al. employed the VProof system which enables vehicles to prove their locations. In this scheme, vehicles can create their location proof using the VProof system by extracting contents from the received packets from RSUs. This scheme protects the user's privacy by hiding their personal information in the location proof. However, it cannot identify fake location information without actually being there. Rabieh et al. [143] presented a

privacy-preserving route reporting system for managing LBI for present and future traffic routes in VANETs. This technique handles both infrastructure and self-organizing VANETs, which enable vehicles for providing LBI to their future routes securely. However, it can lead to cause collusion attack when the number of vehicles increases to a large extent on the route.

In short, there is a great need for designing efficient privacy-preserving routes reporting framework, which could improve the traffic flow and routes in VANETs.

9.1.4. Trust in VANETs. In VANETs, some of its features create difficulty to meet the security requirements in VANETs such as storage information, time sensitivity, and unreliable link lead to cause packet dropping influenced by malicious nodes. One of the main challenging issues in VANETs is to prevent the attacker from attacking trustworthy information and access to the network. In particular, the trust is based on direct interaction with the vehicle which makes it more vulnerable to attacks such as gray hole attack and newcomer attacks. In [73], Li et al. proposed a reputation-based global trust establishment (RGTE) scheme in VANETs. This technique utilized statistical laws to share trustworthy information in VANETs. And, it also detected the malicious node in VANETs using dynamic threshold mechanism. However, the proposed method does not share trustworthy information among vehicles in case of higher mobility due to the packet dropping.

Due to the security and privacy challenges in VANETs, there is a great need for designing and developing a new security mechanism that could improve the existing VANET system, such as by applying the unique features of the heterogeneous vehicular network.

9.1.5. Reliable Link in VANETs. The next challenging issue in VANETs is the lack of reliability of links between V2V and V2I to collect traffic-related data. In the past, many research works have been carried out to detect malicious users. However, these works suffer from the lack of reliable links between entities due to high mobility on the road, which remains a challenging issue. In [144], Rupareliya et al. presented a watchdog system based on IDS for the detection of malicious nodes performing an illegal activity for their own benefit. In this scheme, every node is linked with the watchdog component to monitoring each node to check whether the network packet forwards to the next node. However, due to high mobility vehicles on the road, there are chances that some nodes may drop the packets and do not forward it to the next node. Such nodes deteriorate trust among nodes and are also considered as a malicious node by the watchdog system. Hortelano et al. [145] proposed a watchdog system to detect malicious nodes in VANETs. In this technique, an independent watchdog protocol was produced. This is the simple and robust technique, which can receive packets from a neighboring node for checking how many packets were forwarded to detect the malicious nodes. However, signal noise, unreliable trust among nodes, and node collision could also lead to drop of a large number of packets.

Therefore, a reliable link between entities improves the detection rate of malicious users. The intrusion detection scheme (IDS) can enhance the detection mechanism by incorporating different wireless technologies. However, an IDS is not studied and implemented yet in this domain.

9.1.6. Other Issues in VANETs. Another main challenge in VANETs is to develop the trust in the drivers, i.e., degree of honesty, selfishness, etc. The honesty of drivers plays an important role to broadcast trustworthy information from the V2V and V2I, and also enhances the security of vehicular networks. The driver information can be obtained from the online social network (OSN) through trusted third party services. In case, when the traffic authorities want to match the ID of drivers with the vehicle ID, and they can collect the driver information from OSN based on the identity.

To the best of our knowledge, until now, no study and trust model consider human factors to obtain the degree of honesty and selfishness. It is an open research area that required attention from the researchers from the communication technology background to develop a robust algorithm, which could improve the trust among vehicles.

9.2. Challenges in VCC. Due to the dynamic nature of computing devices, storage, communication medium, and organization enable responsible authority to handle these issues with the help of extensive influence. The VCC is complex in nature which must be designed to synchronize with the operating system, and the open research challenges are discussed below.

9.2.1. Security and Privacy in VCC. The security and privacy are one of the major aspects of the vehicular network, which establishes, maintains, and enhances the users trust in the VC. In particular, the privacy is used to ensure the communication and information exchange in the VC which is in trustworthy environment, while the security is used to protect the vehicular network from threats and attacks, and also from malicious nodes within the network. In [16], Olariu et al. considered VCC as a set of vehicles, in which a group of vehicles in VCC could share the vehicle resources such as computer resources, the Internet, computing, and communication to form a conventional cloud computing. Therefore, it leads to cause the same security issues as CC [146]. Almost the VCC and VANETs are sharing the same security issues. As shown in Figure 10, the main security challenges of VCC includes the following: (i) ensure the secure location as the most of the applications depend on location information, (ii) nodes' authentication and message integrity, (iii) protect data on cloud from malicious users, and (iv) confidentiality of message with cryptography technique.

The security and privacy issues in the VCC require attention from the researchers to develop a robust algorithm which could be able to prevent VCC from different kinds of security threats.

9.2.2. VCC Cost. The VCC aims to utilize the resources efficiently and perform the tasks at a low cost. However, some additional cost occurs, which remain a challenging issue such as intense utilization of memory, system, and network resources. Memory cost occurs due to a large amount of bandwidth consumption from VC users. Delay between data transfer from one vehicle to another with the cloud occurs and lead to increase in the cost of network resources. The system cost, in which the cloud server collect, process, and manage all the information of the cloud user in terms of vehicle resources, user's location, etc., which consume part of the system resources, and an occurrence of an unexpected event need more computing resources.

The cost of services in VCC must be minimized by significantly reducing a large amount of data exchanged in terms of maintenance and unnecessary utilization of resources among vehicles. Additionally, some personalized services require more information such as user location and identity. Therefore, it needs additional resources to collect, store, and process relevant information. The collection of information which is required by the services to perform specific operation could limit the cost of VCC.

The service cost occurring in VCC is not limited to resources utilization, but it also needs to consider the prices of these resources. Most of the services require a subscription, and to avail these services, users need to pay a monthly or yearly subscription charges. The user also can hire the specific resources from the other vehicles, and after paying them, the user can use those resources. To avail, any resource and service users must need to pay; however, a user may face difficulty to pay for these resources due to the unavailability of any credit management system.

9.2.3. VCC Architectural Structure. The communication between vehicle resources and the architectural structure remains a challenging issue in the VCC. During communication, various unexpected problem, event, and changes occur, which require adoption of the VCC architecture from different perspectives. The architectural challenges are related to road and network topology, technology integration, formation of cloud, and its maintenance, which depend on the location and weather conditions.

As the number of cloud members increases along with the increase in communication entities, this leads to create an ambiguity in the network and resource management performances. Thus, these topologies, road structure, and conditions can be regarded as a challenging issue in the architectural scalability. In irregular traffic environments, the communication link between vehicles is not stable because of the topologies limitation. Therefore, the formation of the vehicular cloud is very difficult and cannot fulfill the users' demands.

Specifically, the VCC has various kinds of requirements such as vehicle resources, communication, and deployment of technology. These requirements become challenging issues for designing VCC architectures, and the designed architecture includes the number of entities, number of cloud users, and technology change. Additionally, the VCC routing among cloud members must be changed to the service provider because it is very useful to have the same routing protocol to perform the desired applications such as warning services, emergency services, delay application, and communication between vehicle-to-everything, i.e., V2X can enhance the network quality. In the VCC, a software-defined networking (SDN) controller could be used to accommodate the routing protocols and resource allocations. After information gathered from each area, the SDN controller can apply the rules and send them to the vehicles.

The trustworthy information is shared and data dissemination policy is considered as a challenging issue that requires attention from the researchers and algorithm developers to design a sophisticated system with an optimum solution.

9.2.4. Data Exchange. In the VCC, all the resources which are used to develop communication should be utilized in a comprehensive manner. The vehicle collects the traffic-related information from the electronic sensors and preserves this information locally, which requires a large number of resources. These resources could be released in case of data validity is expired. In case of traffic incident and congestion, the traffic authorities are looking for traffic-related information data for the specific events occurred such as data of traffic incident and data of traffic congestion. If the authority is looking for incident data, it is not useful to send both data. Consequently, it updates the data and deletes the previous data when improving the performance of the utilization of resources and delivering the information accurately. Data management should be enhanced to meet the user demands for successfully utilization vehicle resources and to obtain the useful traffic information.

9.2.5. Heterogeneity Technologies. In recent years, the latest development in the vehicular industry considers the expansion of new vehicular technology and devices. These new technologies drive from different vehicular technology manufacturers and suppliers. The chances of incompatibility between the communication products of two different manufacturers cause communication failure among vehicles [29]. For instance, if the GPS device generates a distorted signal, the exact location of vehicle information may not be correct. Standardization of technologies could be the best solution to overcome this issue and fill the gap between two different manufacturing technologies.

The VC contains a large number of devices and electronic equipment, which could provide various communication capabilities. Then, these devices construct the machine-to-machine (M2M) network, in which the data can be exchanged between two different devices. Because of a large number of devices, the access to the radio channel increases simultaneously, which leads to the collision, and increases the packet loss ratio.

9.2.6. Technology Selection. In the vehicular network, the VCC is considered as the integration of multiple

technologies and this technology could be used to perform the operation. It is necessary to select the best technology, which can perform a specific task. For instance, smartphones, embedded devices, and other handheld devices intend to leave their available resources that could reduce their traffic. Sending traffic to the conventional cloud can be considered as a challenging issue. Also, the limited bandwidth resources and bad signal result in a large number of packets drop and also introduces the packet delay. Therefore, the RSUs could perform operations as a cloudlet to overcome these issues. However, there are still some challenges that need to be considered such as the cloudlet security and the strategy to deploy and manage its resources [29]. Moreover, radio channel technology is considered as a challenging issue in VCC, in which the significant increase in wireless traffic often leads to the emergence of cognitive radio technology [147].

The interaction between significant amounts of equipment in the vehicle cloud often leads to the consumption of a higher amount of energy. Although, the VCC aims to provide the optimum solution by utilizing available resources efficiently, the transmission rate according to the traffic conditions could reduce the energy consumption [148].

10. Conclusion

The VANETs becomes very popular in the traffic management system, which aims to ensure the safety of human lives on the street and provide comfort to travelers by broadcasting safety messages among vehicles. As these safety messages are broadcasted in an open-access environment that makes VANETs more vulnerable to the attacks, a robust security algorithm must be designed for tackling security threats and attacks which could ensure the secure communication in the VANETs and VCC.

In this survey, we first present the basic overview of the VANETs and its characteristics and VANETs security services. Then, the potential applications which are affected by threats and attacks are explained in detail, followed by the location privacy in VANETs. Second, we have discussed the location privacy mechanism in VANETs, which could protect the vehicle privacy. Third, we have discussed the properties to develop the robust trust management model in VANETs and performed the comprehensive analysis of various trust models, followed by a brief discussion on simulation tools, and VANETs applications. Fourth, we have presented the evolution of VCC in a vehicular network. Then, the VCC architecture is explained followed by the security and privacy issues of the VCC in detail. Finally, we have presented some issues related to VANETs and VCC that are considered as open research challenges in a vehicular network. In short, this survey comprehensively covers the location privacy mechanism and trust models in VANETs, identifies open research challenges in the VANETs and VCC, fills the gap of existing surveys, and incorporates the recent development in the VANETs and VCC.

The future research direction for VANETs focuses on the security and privacy issues such as trust model and cryptography-based technique to authentication safety messages. Based on these techniques, researchers could design a robust security system, which can be able to prevent VANETs from different kinds of security threats and attacks. In addition to VANETs, the VCC is still in the beginning stage and expected to provide an optimum solution to protect the network from different kinds of threats and improve the efficiency of the traffic management system. In our opinion, based on the existing VCC algorithms, architectures, and protocols, an improved algorithm could be designed to reduce the trust and privacy issues in VCC.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported in part by the National Key Research and Development program under Grant 2018YFB1600503 and Natural Science Foundation of China under Grant nos. U1564201, 1664258, and 61773184.

References

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

[2] WHO, *Global Status Report on Road Safety 2015*, WHO, Geneva, Switzerland, 2018, http://www.who.int/violence_injury_prevention/road_safety_status/2015/en.

[3] G. Jyoti and M. S. Gaur, *Security of Self-Organizing Networks MANET, WSN, WMN, VANET,*, CRC Press, London, UK, 2010.

[4] Y. Wang and F. Li, *Vehicular Ad Hoc Networks*, Springer, London, UK, 2009.

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

[6] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[7] E. Hossain, G. Chow, V. C. M. Leung et al., "Vehicular telematics over heterogeneous wireless networks: a survey," *Computer Communications*, vol. 33, no. 7, pp. 775–793, 2010.

[8] Y. Qin, D. Huang, and X. Zhang, "VehiCloud: cloud computing facilitating routing in vehicular networks," in *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (IUCC-2012)*, pp. 1438–1445, Liverpool, UK, June 2012.

[9] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor*, pp. 11–21, Alexandria, VA, USA, November 2005.

[10] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for VANET," in *Proceedings of the Fifth ACM International Workshop on Vehicular Inter-Networking (VANET '08)*, pp. 88-89, San Francisco, CA, USA, September 2008.

[11] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 22–28, 2010.

[12] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) Workshop in Conjunction with IEEE INFOCOM*, Anchorage, Alaska, May 2007.

[13] Y.-C. Hu and K. P. Laberteaux, "Strong VANET security on a budget," in *Proceedings of the Workshop Embedded Security Cars (ESCAR)*, pp. 1–9, Berlin, Germany, November 2006.

[14] C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks : an adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2017.

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

[16] S. Olariu, I. Khalil, and M. Abuelela, "Taking vanet to the clouds," *International Journal of Pervasive Computing and Communications*, vol. 7, no. 1, pp. 7–21, 2011.

[17] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 325–344, 2014.

[18] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1138–1149, 2011.

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

[20] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–9, Gold Coast, Australia, December 2012.

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

[22] 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.

[23] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: a survey," *Procedia Computer Science*, vol. 45, pp. 592–601, 2015.

[24] M. K. Sharma and A. Kaur, "A survey on vehicular cloud computing and its security," in *Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, pp. 67–71, Dehradun, India, September 2016.

[25] S. A. Soleymani, A. H. Abdullah, W. H. Hassan et al., "Trust management in vehicular ad hoc network : a systematic review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, Article ID 146, 2015.

[26] M. Gillani, A. Ullah, and H. A. Niaz, "Trust management schemes for secure routing in VANETs—a survey," in *Proceedings of the 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pp. 1–6, Karachi, Pakistan, November 2019.

[27] C. K. Karn and C. P. Gupta, "A survey on VANETs security attacks and sybil attack detection," *International Journal of Sensors Wireless Communications and Control*, vol. 6, no. 1, pp. 45–62, 2016.

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

[29] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: challenges, architectures, and future directions," *Vehicular Communications*, vol. 9, pp. 268–280, 2017.

[30] A. Boukerche and R. E. De Grande, "Vehicular cloud computing: architectures, applications, and mobility," *Computer Networks*, vol. 135, pp. 171–189, 2018.

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

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

[33] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2018.

[34] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "Geographic routing protocols for vehicular ad hoc networks (VANETs): a survey," *Vehicular Communications*, vol. 11, pp. 20–31, 2018.

[35] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018.

[36] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.

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

[38] C. Kalaiarasy, N. Sreenath, and A. Amuthan, "Location privacy preservation in VANET using mix zones—a survey," in *Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–5, Coimbatore, India, January 2019.

[39] R. R. Kouser and T. Manikandan, "Resource scheduling in vehicular cloud network: a survey," in *Proceedings of the 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 621–627, Coimbatore, India, June 2019.

[40] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect DDoS attacks on VANET system: a survey," in *Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–6, Riyadh, Saudi Arabia, May 2019.

[41] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey," *Vehicular Communications*, vol. 16, pp. 45–61, 2019.

[42] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: a review of design and implementation issues," *Future Generation Computer Systems*, vol. 101, pp. 843–864, 2019.

[43] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: communication, applications and challenges," *Vehicular Communications*, vol. 19, p. 100179, 2019.

[44] 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.

[45] Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/.

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

[47] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," *International Journal of Computer Science*, vol. 2, pp. 88–96, 2013.

[48] S. Yousefi, M. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in *Proceedings of the 6th International Conference on ITS Telecommunications*, pp. 761–766, Chengdu, China, June 2006.

[49] J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for VANETs," in *Proceedings of the 2008 5th IEEE Consumer Communications and Networking Conference*, pp. 912–916, Las Vegas, NV, USA, January 2008.

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

[51] T. Yasser and M. Paul, "Vehicle ad hoc networks: applications and related technicalissues," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 3, pp. 74–88, 2008.

[52] T. Rappaport, *Wireless Communications: Principles and Practice*, Pearson Education Inc., Singapore, 2nd edition, 2002.

[53] M. Nekovee, "Sensor networks on the road: the promises and challenges of vehicular ad hoc networks and grids," in *Proceedings of the Workshop on Ubiquitous Computing and e-Research*, Edinburgh, UK, May 2005.

[54] S. Olariu and M. C. Weigle, *Vehicular Networks: From Theory to Practice*, Chapman & Hall/CRC, London, UK, 1st edition, 2009.

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

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

[57] I. A. Sumra, H. B. Hasbullah, and J. L. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey," in *Vehicular Ad-hoc Networks Smart Cities*, pp. 51–61, Springer, Singapore, 2015.

[58] R. Minhas and M. Tilal, *Effects of Jamming on IEEE 802.11p Systems*, Chalmers University of Technology, Gothenburg, Sweden, 2010.

[59] N. W. Lo and H. C. Tsai, "Illusion attack on VANET applications—a message plausibility problem," in *Proceedings of the IEEE Globecom Workshops*, Washington, DC, USA, November 2007.

[60] G. P. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 9, pp. 2658–2667, 2016.

[61] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks : why simple pseudonym change is not enough," in *Proceedings of the 7th International Conference on Wireless On-demand Network Systems and Services (WONS)*, pp. 176–183, Kranjska Gora, Slovenia, February 2010.

[62] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," Tech. Rep. TUM-I1343, Tech Univ. München Inst. Für Inf., Munich, Germany, 2013.

[63] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of Basic Engineering*, vol. 82, no. 1, pp. 35–45, 1960.

[64] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Computer Communications*, vol. 63, pp. 11–23, 2015.

[65] 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.

[66] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93–105, 2016.

[67] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 13–27, 2011.

[68] N. Takbiri, A. Houmansadr, D. L. Goeckel, and H. Pishro-Nik, "Limits of location privacy under anonymization and obfuscation," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 764–768, Aachen, Germany, June 2017.

[69] J. Zhang, "Trust management for VANETs: challenges, desired properties and future directions," *International Journal of Distributed Systems and Technologies*, vol. 3, no. 1, pp. 48–62, 2012.

[70] Y.-C. Wei and Y.-M. Chen, "Efficient self-organized trust management in location privacy enhanced VANETs," in *Proceedings of the International Workshop Information Security Application*, pp. 328–344, Jeju Island, South Korea, August 2012.

[71] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1287–1309, 2016.

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

[73] X. Li, J. Liu, X. Li, and W. Sun, "RGTE : a reputation-based global trust establishment in VANETs," in *Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 210–214, Xi'an, China, September 2013.

[74] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications (VANET '12)*, pp. 73–82, ACM, Low Wood Bay, UK, June 2012.

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

[76] 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.

[77] S. Yang, J. Li, Z. Liu, and S. Wang, "Managing trust for intelligence vehicles: a cluster consensus approach," *Internet of Vehicles—Safe and Intelligent Mobility*, Springer, Cham, Switzerland, pp. 210–220, 2015.

[78] A. Ltifi, A. Zouinkhi, and M. S. Bouhlel, "Smart trust management for vehicular networks," *World Academy of Science, Engineering and Technology, International Journal of Electronics and Communication Engineering*, vol. 10, no. 8, pp. 1114–1121, 2016.

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

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

[81] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, no. 3, pp. 28643–28660, 2018.

[82] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A hybrid trust management heuristic for VANETs," in *Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 748–752, Kyoto, Japan, March 2019.

[83] 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.

[84] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TROUVE: a trusted routing protocol for urban vehicular environments," in *Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 260–267, Abu Dhabi, UAE, October 2015.

[85] 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.

[86] N. Haddadou, A. Rachedi, and Y. Ghamri-doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3657–3674, 2015.

[87] C. A. Kerrache, C. T. Calafate, N. Lagraa, J.-C. Cano, and P. Manzoni, "RITA: risk-aware trust-based architecture for collaborative multi-hop vehicular communications," *Security and Communication Networks*, vol. 9, no. 17, pp. 4428–4442, 2016.

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

[89] K. Golestan, R. Soua, F. Karray, and M. S. Kamel, "A model for situation and threat/impact assessment in vehicular ad-hoc networks," in *Proceedings of the Fourth ACM International Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '14)*, Montreal, Canada, September 2014.

[90] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.

[91] 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.

[92] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications*, vol. 7, no. 3, pp. 229–242, 2014.

[93] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," *Network and System Security*, Springer, Berlin, Germany, pp. 94–108, 2013.

[94] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, "A hybrid trust management framework for vehicular social networks," *Computational Social Networks*, Springer, Cham, Switzerland, pp. 214–225, 2016.

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

[96] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A categorized trustbased message reporting scheme for VANETs," in *Advances in Security of Information and Communication Networks*, pp. 65–83, Springer, Berlin, Germany, 2013.

[97] 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.

[98] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in VANET," *Wireless Networks*, vol. 6, pp. 1–23, 2018.

[99] 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.

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

[101] 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.

[102] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 121–132, 2015.

[103] Y. He, F. R. Yu, Z. Wei, and V. Leung, "Trust management for secure cognitive radio vehicular ad hoc networks," *Ad Hoc Networks*, vol. 86, pp. 154–165, 2019.

[104] Network simulator (ns-2), http://www.isi.edu/nsnam/ns/.

[105] Network simulator (ns-3), http://www.nsnam.org.

[106] MATLAB-Mathworks, http://www.mathworks.com/products/matlab/.

[107] F. G. Mármol and G. M. Pérez, "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1–5, Dresden, Germany, June 2009.

[108] M. Piórkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux, "TraNS: realistic joint traf_c and network simulator for VANETs," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 12, no. 1, pp. 31–33, 2008.

[109] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular mobility simulation for VANETs," in *Proceedings of the 40th Annual Simulation Symposium (ANSS '07)*, pp. 301–309, Norfolk, VA, USA, March 2007.

[110] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2010.

[111] S.-Y. Wang, C.-C. Lin, K.-C. Liu, and W.-J. Hong, "On multihop forwarding over WBSS-based IEEE 802.11(p)/1609 networks," in *Proceedings of the IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 3040–3044, Tokyo, Japan, September 2009.

[112] L. Miao, K. Djouani, B. J. VanWyk, and Y. Hamam, "Evaluation and enhancement of IEEE 802.11p standard: a survey," *Mobile Computing*, vol. 1, no. 1, 2012.

[113] B. Ducourthial and F. El Ali, "Architecture pour communication véhicules—infrastructure," in *Proceedings of the CFIP*, Strasbourg, France, October 2009.

[114] S. A. Hamid, H. S. Hassanein, and G. Takahara, "Vehicle as a resource (VaaR)," *IEEE Networks*, vol. 29, no. 1, pp. 12–17, 2015.

[115] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in *Ad Hoc Networks*, pp. 1–16, Springer, Berlin, Germany, 2010.

[116] S. Olariu, T. Hristov, and G. Yan, *The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds, Mobile Ad Hoc Networking: Cutting Edge Directions*, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2nd edition, 2013.

[117] F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," *Procedia Computer Science*, vol. 37, pp. 357–362, 2014.

[118] R. Hussain and H. Oh, "Cooperation-aware VANET clouds: providing secure cloud services to vehicular ad hoc networks," *Journal of Information Processing Systems*, vol. 10, no. 1, pp. 103–118, 2014.

[119] R. Hussain, F. Abbas, J. Son, H. Eun, and H. Oh, "Privacy-aware route tracing and revocation games in VANET-based clouds," in *Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 730–735, Lyon, France, October 2013.

[120] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[121] T. Gazdar, A. Benslimane, A. Belghith, and A. Rachedi, "A secure cluster-based architecture for certificates management in vehicular networks," *Security and Communication Networks*, vol. 7, no. 3, pp. 665–683, 2014.

[122] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1299–1314, 2015.

[123] N. Kumar, J. P. Singh, R. S. Bali, S. Misra, and S. Ullah, "An intelligent clustering scheme for distributed intrusion detection in vehicular cloud computing," *Cluster Computing*, vol. 18, no. 3, pp. 1263–1283, 2015.

[124] M. Geral, "Vehicular cloud computing," in *Proceedings of the 11th Annual Mediter-Ranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pp. 152–155, Ayia Napa, Cyprus, June 2012.

[125] J. Blum, A. Neiswender, and A. Eskandarian, "Denial of service attacks on inter-vehicle communication networks," in *Proceedings of the 11th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pp. 797–802, Beijing, China, October 2008.

[126] Y. Chen, W. Trappe, and M. Martin, "Detecting and localizing wireless spoofing attacks," in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Network*, pp. 193–202, San Diego, CA, USA, June 2007.

[127] A. Rawat, S. Sharma, and R. Sushil, "VANET: security attacks and its possible solutions," *Journal of Information Operation and Management*, vol. 3, no. 1, pp. 301–304, 2012.

[128] Y. Xi, K.-W. Sha, W.-S. Shi, L. Schwiebert, and T. Zhang, "Probabilistic adaptive anonymous authentication in vehicular networks," *Journal of Computer Science and Technology*, vol. 23, no. 6, pp. 916–928, 2008.

[129] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular Ad Hoc networks," *IEEE Wireless Communications*, vol. 16, no. 6, pp. 48–55, 2009.

[130] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Computer Communications*, vol. 71, pp. 50–60, 2015.

[131] L. Zhang, X. Men, K. K. R. Choo, Y. Zhang, and F. Dai, "Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2018.

[132] G. Yan, D. Rawat, and B. Bista, "Towards secure vehicular clouds," in *Proceedings of the 6th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, pp. 370–375, Palermo, Italy, July 2012.

[133] P. Papadimitratos, L. Buttyan, T. Holczer et al., "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[134] M. Raya, A. Aziz, and J. Hubaux, "Efficient secure aggregation in VANETs," in *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, pp. 67–75, ACM, Los Angeles, CA, USA, October 2006.

[135] Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li, "Efficient authentication and access control of message dissemination over vehicular ad hoc network," *Neurocomputing*, vol. 181, pp. 132–138, 2016.

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

[137] National Highway Traffic Safety Administration, *Vehicle Safety Communications Project Report*, National Highway Traffic Safety Administration, U.S. Department of Transportation, Washington, DC, USA, 2006.

[138] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[139] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[140] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in *Proceedings of the IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 478–483, New York, NY, USA, October 2017.

[141] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1187–1192, New Orleans, LA, USA, March 2005.

[142] Y. Zhang, C. C. Tan, F. Xu, H. Han, and Q. Li, "VProof: lightweight privacy-preserving vehicle location proofs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 1, pp. 378–385, 2015.

[143] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2703–2713, 2017.

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

[145] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proceedings of the 2010 IEEE International Conference on Communications Workshops (ICC)*, pp. 1–5, Capetown, South Africa, May 2010.

[146] G. Yan, J. Lin, D. B. Rawat, and W. Yang, "A geographic location-based security mechanism for intelligent vehicular networks," *Communications in Computer and Information Science*, Springer, vol. 135, pp. 693–698, Berlin, Germany, 2011.

[147] J. Yang and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[148] J. Toutouh, S. Nesmachnow, and E. Alba, "Fast energy-aware OLSR routing in VANETs by means of a parallel evolutionary algorithm," *Cluster Computing*, vol. 16, no. 3, pp. 435–450, 2013.