Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 2423915, 23 pages
https://doi.org/10.1155/2019/2423915

Review Article

A Comprehensive Survey on VANET Security Services in Traffic Management System

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

[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*

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

Received 28 May 2019; Accepted 18 August 2019; Published 15 September 2019

Guest Editor: Manzoor Ahmed Khan

Recently, vehicular ad hoc networks (VANETs) embark a great deal of attention in the area of wireless and communication technology and are becoming one of the prominent research areas in the intelligent transportation system (ITS) because they provide safety and precautionary measures to the drivers and passengers, respectively. VANETs are quite different from the mobile ad hoc networks (MANETs) in terms of characteristics, challenges, system architecture, and their application. In this paper, we summarize the recent state-of-the-art methods of VANETs by discussing their architecture, security, and challenges. Secondly, we discuss the detailed analysis of security schemes and the possible measures to provide secure communication in VANETs. Then, we comprehensively cover the authentication schemes, which is able to protect the vehicular network from malicious nodes and fake messages. Thus, it provides security in VANETs. Thirdly, we cover the mobility and network simulators, as well as other simulation tools, followed by the performance of authentication schemes. Finally, we discuss the comfort and safety applications of VANETs. In sum, this paper comprehensively covers the entire VANET system and its applications by filling the gaps of existing surveys and incorporating the latest trends in VANETs.

1. Introduction

In today's digital world, intelligent transportation system (ITS) plays a very important role in making the life of the citizens easy in every facet. ITS aims to achieve higher traffic efficiency by minimizing traffic problems and controlling unpleasant events.The ITS offers pervasive and robust services in terms of providing road and traffic safeties, reducing traffic congestion and improving traffic flow, and providing entertainment services on the vehicles, etc. [1]. The automotive industry realizes the need of the vehicle to be connected with the IT system; for example, communication between the vehicles increases the traffic safety and optimizes the traffic flow [2]. This is performed to meet the demands and broaden the recognition event of vehicles, which cannot be possible by sensors [2]. Traffic flow parameters, driver behavior, and driving conditions can be detected and shared with vehicles within their vicinity. To share this information and increase the efficient communication between vehicles, vehicular ad hoc networks (VANETs) have been introduced [3].

The aim of the ITS is to provide traffic safety and enhance traffic flow. VANET is a type of MANET with road routes, which depends on registration mechanism, roadside units (RSUs), and onboard units (OBUs) [4]. The OBUs are the radios that are installed in every vehicle as a transmitter to communicate with each vehicle, while RSUs are installed along the street with network devices. RSUs are used to communicate with the infrastructure and contain the network devices for dedicated short-range communication (DSRC) [5]. VANETs are classified into two categories: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [6]. The main responsibility of VANETs is to produce effective communication; basically, the nodes require specific features to acquire information, to communicate with the neighbors, and then to take decisions

based on all information collected by using sensors, cameras, global positioning system (GPS) receivers, and omnidirectional antennas [7].

Recently, VANETs are gaining a lot of attention in wireless and mobile communication technology. They are one of the robust schemes to implementing the intelligent transportation system (ITS). VANETs and MANETs are quite different from each other in terms of high node mobility, network architecture, and unreliable channel, as well as time deadline, less reliability, driving condition, and network fragmentation [8–10]. The unique features in VANETs such as high mobility and volatility have made them weaker to the internal and external network attacks [11]. These attacks create difficulty in designing secure VANETs in terms of security, privacy, and trust [11]. In recent years, a key management scheme has received a great attention due to its characteristics and reliability in providing a secure channel in fog computing. This scheme can be used in VANETs to form a fog system in terms of RSUs such as edge routers and intelligent traffic light [12].

VANETs face many security challenges and issues related to authentication and privacy [13–17]. In addition to these, untrustworthy vehicles raise many security and communication issues in VANETs [18]. In VANETs, the entire communication is in open access environment, which makes VANETs are more vulnerable to the attacks. Thus, the attacker can modify, intercept, inject, and delete the messages in VANETs. For example, the attacker can get access to the traffic messages, which are used to guide the vehicles on the road. The attacker may alter these messages and may spread false information on the road, which causes traffic congestions, traffic incidents, accidents, hazards, etc.

In order to effectively apply VANETs in wireless communication technology, security and privacy issues must be handled efficiently by introducing sophisticated algorithms to tackle all kinds of threats and attacks. To address these issues, several research studies have been proposed in terms of authentication and privacy schemes for the VANET system. Several methods utilized public key infrastructure (PKI) schemes to authenticate vehicles, which contain the digital signature of the certification authority (CA) and vehicles' public keys. Thus, the vehicles and RSUs require a large amount of computational time and memory to process and verify these certificates [2, 19]. These schemes create more robust solutions by verifying signatures of each vehicle. However, it creates two problems [16]. Firstly, as OBUs contain less power, they may not be able to verify all the signatures in short time. Secondly, each message contains signatures and certificates, which may increase the packet size and then subsequently increase the transmission overhead.

Many researchers have proposed different methods to develop a secure network for the VANETs. Recently, several surveys related to VANETs have been published, which covered the detailed overview and mechanism of VANETs such as characteristics, security, privacy, attacks, and threats, but still they lack some features and there are shortcomings in these surveys. Al-Sultan et al. [20] launched a survey which detailed the overview of VANET architecture, protocols, simulation, and its applications.

In 2014, Sharef et al. [21] presented a survey for the routing characteristics and challenges in the VANETs that may be considered in designing the routing protocol for VANETs. Engoulou et al. [11] conducted a survey in 2014 on security issues and challenges of VANETs and also discussed their security requirement and applications, but did not cover many aspects for security in VANETs. Recently, many simulations and experimental tools have been developed in the 2015 survey article by Qu et al. [14], and in 2016, Azees et al. [22] indicated the privacy and security issues of VANETs. Hasrouny et al. [4] discussed the VANET security, challenges, reasons, and their solution by presenting the most recent security architecture with VANET routing protocols; this intense survey is limited to 2017. Lu et al. [23] conducted a survey in 2018 in which they comprehensively discussed the architecture, security, privacy, and trust management system in VANETs. Furthermore, they also discussed the network simulators and integrated simulators, with less coverage on privacy and security in VANETs. Sharma and Kaul [24] presented a survey on the intrusion detection system (IDS) and security mechanism in a vehicular network such as VANETs and VANET cloud, which are used in handling the security threats. This survey discussed the challenging issues for using the IDS in VANETs. Boualouache et al. [25] launched a survey on pseudonym changing strategies for VANETs. This survey discussed and compared these strategies based on some relevant criteria and also identified open issues. Ali et al. [26] presented a survey on the authentication and privacy schemes for VANETs by classifying and discussing their modeling, requirements, and attacks and by describing performance parameters. They also discussed some open issues for VANET security services.

In recent years, different surveys on VANETs have been proposed relating to security and privacy schemes [23, 26]. These surveys covered most aspects of VANETs, but with limited coverage on VANET security services along with the recent state-of-the-art methods. However, there is a great need of a comprehensive survey that analyzes the VANET security and privacy issues from different perspectives and fills the gap of the above surveys. To accomplish this task, this paper presented a comprehensive review to understand various VANET security threats and attacks. Also, our survey is different from the existing surveys in terms of covering VANET security services and authentication schemes. For better understanding for the readers of different research background, firstly, we have discussed the recent state-of-the-art methods that indicate the existing issues of VANET security and their solutions. Secondly, we presented each security service of VANETs in terms of attacks and threats along with the recent state-of-the-art methods, whereas the above surveys only covered limited security threats and attacks. Furthermore, we have comprehensively covered the authentication schemes in detail, while most of the surveys did not cover the authentication schemes thoroughly. Thirdly, the latest simulation tools and

applications are discussed, followed by the performance of authentication schemes, while most of the surveys did not discuss the simulation tools and their utilization on authentication schemes and applications. Finally, we have identified various security challenges that researchers may face while conducting a research and also indicate the possible solutions to deal with these issues along with the future research direction. It enables researchers to apply VANETs technology efficiently as the popularity of vehicle-to-everything (V2X), cellular vehicle-to-everything (C-V2X), and long-term evolution-vehicle (LTE-V) communications are gaining rapidly due to sharing valuable traffic-related information among vehicles with higher efficiency.

The rest of this survey paper is structured as follows. We have explained the overview of VANETs in Section 2. Section 3 presents the security and challenges. Section 4 presents the attacks and threats on the security services. Section 5 discusses the recent state-of-the-art methods on the security services. Then, the comprehensive explanation of privacy preservation authentication is presented in Section 6. Simulation tools and applications of the VANETs are discussed in Sections 7 and 8, respectively. Finally, Section 9 concludes the review.

2. Basic Overview of VANETs

Since from 1980, VANETs which are ad hoc network infrastructures grow abruptly, in which vehicles are connected through wireless communication [27]. Recently, VANETs are used in enhancing traffic safety, improving traffic flow, and reducing traffic congestion and driver guidance [28]. The basic model diagram of VANETs which shows the vehicles' communication can be distinguished into V2V and V2I communication, road side units (RSUs), and onboard units (OBUs). Firstly, we will discuss these parameters and then explain the unique characteristics and advantages of using VANETs over MANETs in terms of network topology, bandwidth, reliability, etc. As we discussed above, the VANETs consist of three components such as OBUs, RSUs, and trusted authority (TA); these parameters are discussed below.

2.1. VANET Architecture. Generally, the communication between vehicles and RSUs is done via wireless technology called as wireless access in vehicular environment (WAVE). The WAVE architecture describes the exchange of security messages [1], and the WAVE communication ensures the safety of passengers by updating vehicle information and traffic flow. This application ensures the pedestrian and driver safety and also improves the traffic flow and efficiency of the traffic management system. The VANETs comprise several units such as OBUs, RSUs, and TA. Specifically, the RSU typically hosts an application that is used to communicate with other network devices, and the OBU is mounted on each vehicle to collect the vehicle useful information such as speed, acceleration, and fuel. Then, these data are forwarded to the nearby vehicles through wireless network. All RSUs interconnected with each other are also connected to TA via wired network. Additionally, TA is the head among all components, which is responsible for maintaining the VANETs [22].

2.1.1. Roadside Unit (RSU). The roadside unit is a computing device which is fixed alongside of the road or in specified location such as parking area or at the intersection [20]; it is used to provide local connectivity to the passing vehicles. The RSU consists of network devices for dedicated short-range communication (DSRC) based on IEEE 802.11p radio technology. Specifically, RSUs can also be used to communicate with other network devices within the other infrastructure networks [20].

2.1.2. Onboard Unit (OBU). OBU is a GPS-based tracking device which is usually equipped in every vehicle to share vehicle information to RSUs and other OBUs. OBU consists of many electronic components such as resource command processor (RCP), sensor devices, user interface, and read/write storage for retrieving storage information. The main function of OBU is to connect with RSU or other OBUs through wireless link of IEEE 802.11p [29] and is responsible for communication with other OBUs or RSUs in the form of messages. Moreover, OBU takes input power from the car battery, and each vehicle consists of sensor type global positioning system (GPS), event data recorder (EDR), and forward and backward sensors which are used to provide input to OBU [22].

2.1.3. Trusted Authority (TA). Trusted authority is responsible for managing the entire VANET system such as registering the RSUs, OBUs, and the vehicle users. Moreover, it has the responsibility to ensure the security management of VANETs by verifying the vehicle authentication, user ID, and OBU ID in order to avoid harm to any vehicle. The TA utilizes high amount of power with large memory size and also can reveal OBU ID and details in case of any malicious message or suspicious beha2vior [30]. In addition to these, TA has the mechanism to identify the attackers as well.

2.2. Communication Methods in VANETs. ITS is consistently focusing on providing secure communication to improve the traffic flow and road safety and also overcoming the traffic congestion by utilizing different networking techniques such as MANETs and VANETs.

V2X communications play an important role in the ITS to improve the traffic efficiency, traffic safety, and driving experiences by providing real-time and highly reliable information such as collision warning, road bottlenecks information, traffic congestion warning, emergency situations, and other transportation services [31]. V2X communication can exchange the information between V2V, V2I, and vehicle to pedestrians (V2P) as shown in Figure 1.

In V2V communication, transmission medium is characterized by high transmission rate and short latency

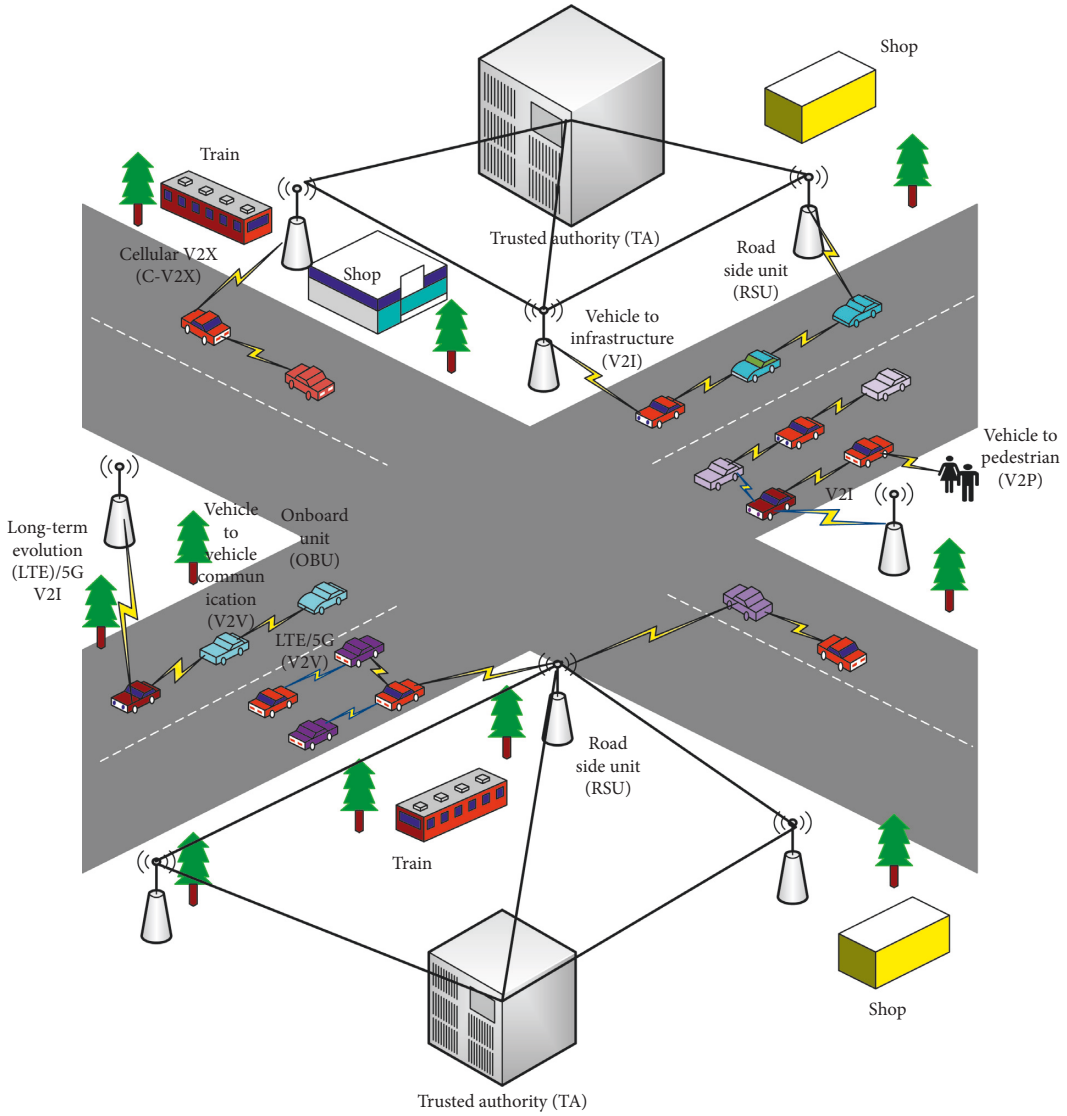

Figure 1: VANET model diagram.

[4]. In V2V, a vehicle can broadcast useful information such as emergency braking, collision detection, and traffic conditions among each other. V2I is used to transmit useful information between vehicles and network infrastructures. In this domain, the vehicle developed a connection with RSUs to exchange information with other networks such as the Internet. Furthermore, due to communication with the infrastructure, V2I requires large bandwidth than V2V but less vulnerable to attacks [32].

Recently, C-V2X technology was introduced; it is a unified connectivity platform which aims to support V2X communications [33]. C-V2X is developed within the third-generation partnership project (3GPP) and regarded as the robust communication technology that can accomplish the V2X communications [34]. It connects each vehicle and enables the cooperative intelligent transport systems (C-ITS) that reduce the traffic congestion and enhance the traffic efficiency [35].

In the year 2016, 3GPP released its first version to support V2X communications, and the standards are referred to as LTE-V, long-term evolution (LTE), and C-V2X [36]. LTE possess robust benefits in V2I communication because of its high data rate, large coverage, and penetration rate [37]. However, in V2V communication, LTE faces many challenging issues due to lack of its centralized structure and limited services to support V2V communication [37]. VANET communications are further classified into four categories [38] which are shown below.

2.2.1. Warning Propagation Message. If there is any crucial situation, the message is required to send to a specific vehicle or to a group of vehicles. For example, if there is any accident or collision, then the warning message should be sent to the vehicles which are on the way to avoid traffic jams, which increases the traffic safety. To deal with this issue, a new

routing algorithm is required, which can be used to send the warning messages to the destination [38].

2.2.2. V2V Group Communication. In V2V communication domain, only vehicles which are sharing some of the same features can take part in this communication [38], such as vehicles with the same brand or vehicles sharing same location in the time interval.

2.2.3. Vehicle Beaconing. This technique periodically sends the beacon messages to all vehicles which are nearby and RSUs. These messages contain the speed, velocity, and acceleration of the sending vehicle.

2.2.4. Infrastructure to Vehicle Warning. To improve the traffic flow and road safety, warning messages are broadcasted from the infrastructure via RSUs to all vehicles within its vicinity when possible accident or collision is detected, especially in the curve route, intersections, or with narrow road.

2.3. VANET Standards. The communication protocol of VANET standards provides the comprehensive requirements to how to implement this policy. The VANET standardization affects all layers of the open system interconnection (OSI) model which is used as a communication tool and includes all necessary features of all the layers [39]. The dedicated short-range (DSRC) communication, wireless access in vehicular environment (WAVE), and IEEE 802.11p are used to designate the full standard of communication protocol to deal with VANETs.

2.3.1. Dedicated Short-Range Communication (DSRC). DSRC is a wireless communication technology tool which permits vehicles to communicate with each other in ITS or other infrastructure networks such as V2V and V2I to enhance and develop the standardization of frequencies which allow VANETs to work [39]. In the year 1999, the Federal Communications Commission (FCC) allocated the band from 5.850 to 5.925 GHz, with a spectrum of 75 MHz for DSRC [40, 41]. As shown in Figure 2, the spectrum of 75 MHz DSRC is sectioned into seven channels, which start from Ch 172 to Ch 184. The Ch 178 is the control channel which can support the safety power applications [41], and the other six channels such as 172, 174, 176, 180, 182, and 184 are the service channel (SCH). The Ch 172 and Ch 184 are used for high power public safety messages [41], while the other channels can be used to send both safety and nonsafety messages.

2.3.2. Wireless Access in Vehicular Environment (WAVE). WAVE is the latest release of ITS standards from IEEE published materials [42]. The WAVE IEEE 1609 describes architecture, mechanism, sets of protocols, and interface which are used to develop the communications with V2V and V2I (see Figure 3) [1].

2.3.3. IEEE 802.11p. After introducing the IEEE 1609 standards, the IEEE extended the family of IEEE 802.11 protocols by adding a new member 802.11p which is used to facilitate the vehicular communication network [1], in compliance with the DSRC band.

2.4. VANET Characteristics. VANETs are ad hoc networks, highly dynamic, and reliable and offer multiple services, but with limited access to the network infrastructure. VANETs have unique characteristics as compared to MANETs, and these characteristics are very critical for security and privacy aspects in VANETs, which are discussed below:

(i) *High Mobility*. VANETs have high mobility as compared to MANETs. Vehicles are moving at high speed that may cause a delay in V2V communication. Also, the high mobility of nodes reduces the less number of mesh nodes in the network [13, 43].

(ii) *Dynamic Network Topology*. The topology of VANETs is not constant and can change rapidly due to the high mobility of vehicles. Therefore, it makes VANETs more vulnerable to the attacks and difficult to recognize the suspected vehicles.

(iii) *Computing and Storage*. In VANETs, computing and storage is also a challenging issue because the processing of a large amount of information exchange between vehicles and infrastructures is very ordinary.

(iv) *Time Critical*. The exchanged information in VANETs must be reached the nodes within a specific time limit, so that decision can be made and further action can be taken immediately.

(v) *Limitation of Transmission Power*. The transmission power is very constrained in the wireless access of vehicular environment (WAVE) which ranges from 0 to 28.8 dBm and is limited to the distance up to 1 km. Thus, the limited power transmission resulted in limited coverage distance of VANETs [39, 44].

(vi) *Volatility*. In VANETs, the connections between vehicles may be lost or remain active within a few wireless hops [23]. Thus, it makes difficult to ensure personal security in VANETs.

3. VANET Security and Challenges

Recently, MANETs introduce a new security concern, which is considered as an important issue for the researcher to deal with the safety purpose such as less number of central points, mobility, insufficient wireless connectivity, and driver issue [45]. VANET security ensures that the transferred messages are not injected or altered by the attackers. Additionally, the driver is responsible for informing the traffic conditions accurately within the limited time frame. VANETs are more sensitive to the attacks because of its distinctive characteristics. Specifically, security challenges should be addressed properly; otherwise, it will create many constraints for secure communication in VANETs [4].

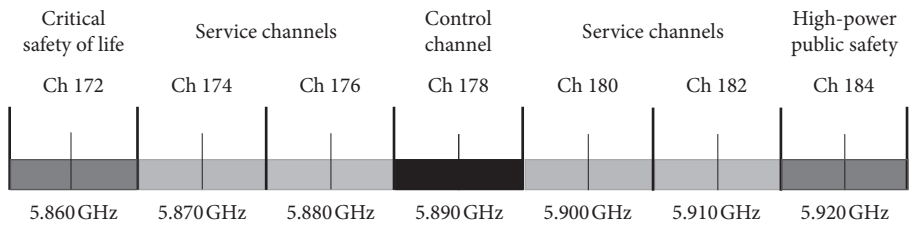

Figure 2: Channel diagram of DSRC.

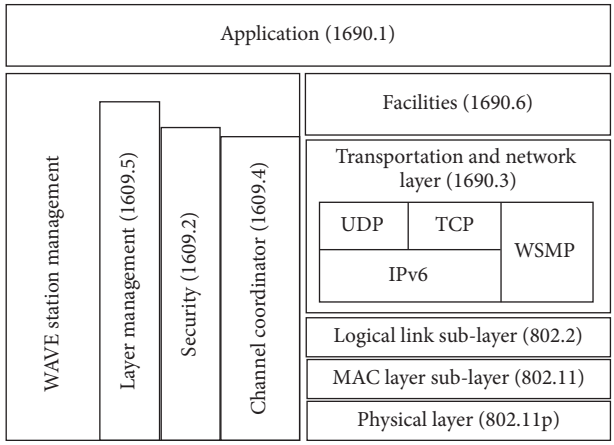

Figure 3: WAVE layout [39].

In VANET security, it is necessary to mention the requirements that the system should be in line with the appropriate network operation. Inability to fulfill these requirements may lead to be a possible threat or attacks in VANETs. The main security requirements are categorized into five main domains such as availability, confidentiality, authenticity, data integrity, and nonrepudiation [2, 46]. Figure 4 shows the security services and their threats and attacks, which will be discussed in the following sections.

3.1. Availability. Availability is the most important part of security services which required attention because it is directly associated with all the safety applications. The main responsibility of availability is to manage functionality, and its security must ensure that the network and other applications must remain functional in case of faulty or malicious conditions [47]. If more dangerous attacks happen in VANETs, then availability is more than any other security aspect [48].

3.2. Confidentiality. Based on certificates and shared public keys, confidentiality ensures that the designated receiver has access to the data while outside nodes may not be able to get access to that data until the confidential data were received by the designated user.

3.3. Authentication. Authentication plays a vital role in VANETs. It prevents the VANETs against suspected entities in the network. It is important to have the related information of transmission mode such as user identification and sender address. Authentication has the right to control the authorization level of vehicles, and it can also prevent from Sybil attacks by assigning individual identity to each vehicle [11].

3.4. Data Integrity. It ensures that the message content is not altered during the communication process. Specifically, in VANETs, it can be ensured by using the public key infrastructure and cryptography revocation process [48].

3.5. Nonrepudiation. It ensures that, in case of dispute, the sender and the receiver of the message do not refuse to engage in transmission and reception [49, 50].

4. Security Attacks and Threats in VANETs

In this section, we will discuss the attacks and threats on each security service.

4.1. Attack on Availability. Availability of information is a very important part of the VANET system, in case of lack of availability feature that may lead to reduction in the efficiency of VANETs [50]. In this section, we will explain the threats and attacks in VANETs.

(i) *Denial-of-Service (DOS) Attacks.* DOS is one of the common attacks in VANETs, which is caused by the internal or external vehicles performed the attacks in VANETs [13]. The attacker jams the communication between vehicles and effectively blocks all possible ways of action. This attack can be performed by many attackers concurrently in a distributed way, called as distributed denial of service (DDoS) [51].

(ii) *Jamming Attack.* In this attack, the attacker disturbs the communication channel in VANETs by using a heavily powered signal with equivalent frequency [52]. This is the most dangerous attack for safety application because it did not follow the valid safety alert. For any successful jamming attack, the jammer can jam the useful signal within the same time of the occurrence of an event by performing an action.

(iii) *Malware Attack.* The attack can be penetrated into the VANET system through the software

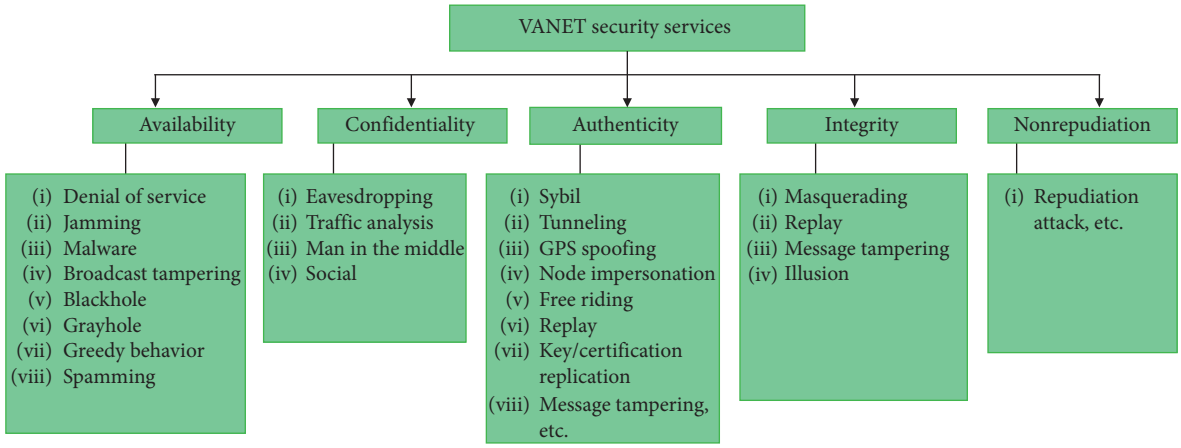

Figure 4: VANET security services.

components which are used to operate the OBUs and RSUs [43, 53]. If the malware attack is occurred in VANETs, malfunction of the other components of the VANET system will occur.

(iv) *Broadcast Tampering Attack*. In this attack, untrustworthy vehicles can replicate the same messages by modifying the message or generate and insert a new message in the VANETs while behaving as a transmit node for intervehicle communication [48]. Therefore, this may lead to hiding of the correct safety messages to dedicated users, which may be the reason for dangerous accidents.

(v) *Blackhole Attack*. This is the main attack which targets availability in the ad hoc network and also exists in VANETs. This attack is usually caused by a registered VANET user. The suspected node receives the packets from the network, but it declines to contribute to the networking operation. This may disrupt the routing table and prevent the important message to the recipients due to the malicious node, which pretends to contribute to the nonpractical event [1, 13, 53].

(vi) *Grayhole Attack*. It is the variant of blackhole attack, and it occurs when untrustworthy vehicles select some of the data packets to forward and drop the others packet without being tracked [48].

(vii) *Greedy Behavior Attack*. This attack is normally on the functionality of message authentication code (MAC), when the malicious vehicle misuses the MAC protocol to increase the large amount of bandwidth which cost to other users. This resulted in overload traffic and caused collision on the transmission channel, which can produce delay in the legitimate services of the registered user [54].

(viii) *Spamming Attack*. In this attack, numerous amount of spam messages were injected by the attacker such as advertisement in the VANET system, which cause collision by utilizing more bandwidth [13, 43].

4.2. Attack on Confidentiality in VANETs. Confidentiality guarantees can be encrypted by using the certificates and by sharing the public keys to all exchange messages, and only designated vehicle can get the access. Therefore, the vehicle which is outside the nodes cannot understand private and confidential information among the vehicles. Confidentiality is guaranteed through the cryptographic solutions. In this section, we will discuss the common threats on confidentiality, which are discussed below:

(i) *Eavesdropping Attack*. Eavesdropping is very common in wireless communication technology, such as MANETs and VANETs. The aim of this attack is to get the confidential information from the protected data. Therefore, by this attack, secret details such as user identity and data location which may be used to track the vehicles can be disclosed with nonregistered users.

(ii) *Traffic Analysis Attack*. This is one of the dangerous attacks which threats confidentiality. In this attack, after listening message transmission, the attacker then analyzes its frequency and tries to extract and gather the maximum useful information purposely.

(iii) *Man-in-the-Middle Attack*. This attack takes place in the middle of V2V communication to check closely and alter the messages. The attacker can get the access and control the entire V2V communication, but the communication entities think that they can communicate with each other directly in private [55].

(iv) *Social Attack*. Social attack is used to divert the attention of the driver. The attacker sends out immoral and unethical messages to the drivers. The aim of attackers is to get the reaction of the drivers after they received such kind of immoral messages, thus affecting the driving experience and performance of the vehicle in the VANET system [56].

4.3. Attack on Authentication in VANETs. Authentication is an important part in the VANET system, which is used to protect against the attacks because of the malicious nodes

entering in the system. The authentication is responsible for protecting VANETs from internal and external attacks [57]. This section highlights the threats and attacks on authentication in VANETs.

(i) *Sybil Attack*. The Sybil attack was first discussed in [58]. This is the most dangerous attack in which `node contains many fake identities to disrupt the normal mode of operations of the VANETs by broadcasting multiple messages. The attacker can manipulate other vehicle behaviors, and receiving vehicle thinks that the messages are transmitting from the different vehicles. Therefore, they may feel there is congestion on the road, so they enforced them to alter their paths and leave the road clear.

(ii) *Tunneling Attack*. This attack is similar to the wormhole attack [13]. The attacker uses the same network to initiate the private conversation, and the attacker joined two far-away parts of the VANETs by utilizing an extra communication channel named tunnel. Therefore, the nodes which are very far can communicate as neighbors.

(iii) *GPS Spoofing*. In the VANET, the position and location of the node are very important which should be very accurate and authentic. The log file is maintained which contains location table in the GPS satellite. In this attack, the attacker uses trick to create false GPS location information and did not reveal the correct position to dodge the vehicles that may think it is available in some another location [59].

(iv) *Node Impersonation Attack*. This attack takes place by successfully acquiring the valid ID of the user and sending it to another authorized user in the VANETs [53].

(v) *Free-Riding Attack*. This attack is very common and initiates by an active malicious user by making false authentication efforts while associated with the cooperative message authentication. In this attack, the malicious user may take advantage of other user's authentication contributions without having its own, and this kind of act is called free-riding attack. This attack may raise a serious threat to the cooperative message authentication [60].

(vi) *Replay Attack*. This attack is very common attack which is also known as a playback attack; this attack occurs when a valid data is fraudulently transmitted or causes delay to produce unauthorized and malicious effect. In order to tackle this attack, the VANET must require enough time sources with larger cache memory which are used to compare the received messages.

(vii) *Key and/or Certificate Replication Attack*. This attack is caused by the utilization of duplicate keys and/or certificates of other users as a proof of authentication to create an uncertainty which makes the situation worst for traffic authorities to identify the vehicle. Specifically, the aim of this attack is to create confusion for TAs especially in case of any dispute.

(viii) *Message Tampering*. It is a very common attack, in which the attacker can alter the exchanged messages in V2V or V2I communication which is intentionally used to avail counterfeit responses.

(ix) *Masquerading Attack*. The attacker uses false IDs to act as another vehicle. This attack is occurred when one user did not show his own identity and pretends to be a different user to obtain an unauthorized access legally.

4.4. Attack on Data Integrity in VANETs. In this section, we will discuss the common threats on integrity, which are discussed below:

(i) *Masquerading Attack*. The attacker enters in the VANET system by registered user ID and passwords and tries to broadcast false messages which appeared to come from the registered node [61].

(ii) *Replay Attack*. The attacker aims to repeat or delay the transmission fraudulently by having a valid data and inject beacon messages which received before on the VANETs continuously, which may cause difficulty for traffic authority to identify the vehicles in case of emergency [62, 63].

(iii) *Message Tampering Attack*. As the name of the attack indicated, this attack normally occurs when the attacker modifies or alters recent message data to be transmitted [64]. For instance, if the route is congested, then the attacker alters the data to clear the road which can influence the users to alter their driving paths.

(iv) *Illusion Attack*. This attack received data from antennas and collected malicious data from sensors which generate traffic warning messages by using the existing road condition which may create illusion to the vehicles nearby [65]. Illusion attack may be caused by vehicle accidents and traffic congestion and also minimizes the performance of the VANET system by utilizing undesirable bandwidth.

4.5. Attack on Nonrepudiation. It ensures that the sender and receiver of messages cannot deny the transmitted and received messages in case of dispute.

(i) *Repudiation Attack*. This attack occurs when an attacker denies engaging in the activity of sending and receiving messages in case of any dispute [22].

Table 1 summarizes all the security attacks in VANETs. It identified each attack with their related compromised security services and their possible countermeasures.

Table 1: Security attacks and their countermeasures in VANETs [1, 4, 22, 66].

Attack	Compromised services	Countermeasures
DOS	Availability, authentication	Use the bit commitment and signature-based authentication technique
Jamming	Availability	Use frequency hopping technique, direct-sequence spread spectrum (DSSS)
Malware	Availability	Reliable hardware and digital signature of software
Broadcast tampering	Availability, integrity	Cryptographic primitives are enabled for prevention, but a nonrepudiation mechanism may exist
Blackhole, grayhole	Availability	Reliable hardware and digital signature of software
Greedy behavior	Availability	Use intrusion detection systems (IDSs)
Spamming	Availability, confidentiality	Reliable hardware and digital signature of software
Eavesdropping	Confidentiality, integrity	Exploit physical layer security protocols
Traffic analysis	Confidentiality	Use encryption techniques
Man-in-the-middle	Authentication, confidentiality, integrity	Robust authentication technique such as digital certificates
Social	Confidentiality	Use digital signatures
Sybil	Availability, authentication	Deployment of central validation authority (VA), location and position verification, and efficient allocation of transmission resources.
Tunneling	Integrity	Reliable hardware and digital signature of software and sensors
GPS spoofing	Authentication	Signature-based authentication technique with positioning system and the usage of bit commitment
Free-riding	Authentication	Use strong authentication technique
Key and/or certificate replication	Confidentiality, authentication	Use certified keys, and check the validity of certificates in real time through CRL
Message tampering	Availability, authentication	Zero-knowledge schemes for authenticate message
Masquerading	Authentication, nonrepudiation, integrity	Digital signature of software, and trusted and reliable hardware which makes impossible to change protocols
Replay	Authentication, integrity, nonrepudiation	Message authentication, using digital signature scheme
Illusion	Authentication, integrity	Software must be handled by authorized entity, sensors operation must be authenticated, and use the plausibility validation network (PVN)
Repudiation	Nonrepudiation	Identity-based signature and ID-based online/offline (IBOOS) techniques with complex managing certificates may exist

5. Research Work on Security Services and Requirement of Authentication

Security services play an important role to ensure the secure communication in VANETs. In this section, we have described the recent research work related to the VANET security services.

5.1. Research Work on Availability. In recent years, an intense amount of research work have been done, which enhanced the performance of availability services by introducing new protocols. In this section, we will explain the robust existing methods which have been used to enhance the performance of availability in VANETs.

Kitani et al. [67] presented a new method named a message ferrying which is used to improve the message circulation in less populated areas. This method utilized buses to obtain maximum traffic information from vehicles such as location, fuel, and acceleration in their vicinity and then gathered information and forwarded the collected information to the neighboring vehicles. The proposed method implemented on NETSTREAM traffic simulator and then compared the information propagation efficiency with other competent methods. In the proposed method, the author did not mention the detail performance parameters which were involved in and only limited to low-density area.

Okamoto and Ishihara [68] introduced a method of information sharing technique for location-dependent data which are generated by vehicles using the pull and push method to balance the message delivery and the traffic for data dissemination called assigning populated area as message storage area (APAM) scheme. This method is limited to deliver the reliable information based on the pull and push method, but may incur large amount of computational charges.

Akila and Iswarya [69] introduced an effective data replication technique to manage data access application in VANETs such as location, fuel, and acceleration. Due to high mobility vehicles, the VANETs topology changes dynamically, which often causes frequent disconnection. If

disconnection happens frequently, then the vehicles will not be able to communicate and share data with each other. Specifically, the data replication is used to improve the performance of data access in distributed system.-However, most of the nodes in VANETs contain less storage. Therefore, they cannot replicate heavy mp4 files or some short duration video clips. This problem is significantly improved by generating the request to the vehicles in a platoon to give some part of their buffers to reproduce data while sharing the same platoon and data among other vehicles. In case, when a vehicle wants to leave a platoon, it transferred the buffered data to other vehicles prior to leaving a platoon. Therefore, the other vehicles have an access to the data after it leaves. This method has limitations; vehicles frequently leaving and entering a platoon may require large amount of computational time and incur computation charges.

Park and Lee [70] introduced an effective method to enhance the data accessibility in VANET by utilizing the data replica of the RSU. In this approach, selection of data item is made by using the data access pattern and driving pattern which must be reproduced in the RSUs. Then, the reproduced data are sent directly to the surrounding vehicle without involving communication with RSUs. The main drawback of this approach is if the data size is larger, then the data replication process may require a large amount of time to handle the replication process.

5.2. Research Work on Confidentiality. In recent years, several methods have been proposed in confidentiality to ensure the safety of data which contain some useful information from nonregistered users in the VANET system. Additionally, it ensured secure communication through cryptographic solution. In this section, we will explain the existing methods for confidentiality in the VANETs.

Sun et al. [71] introduced a new security system by protecting the confidentiality of sensitive information using shared key encryptions. The aim of the proposed technique is to ensure the confidential information of the registered users and tracking of vehicles legitimately, which can be done by integrating the new security requirements and designing the sophisticated VANET security system against nonauthorized users. However, the confidentiality messages are very crucial where vehicles get the useful data from the Internet and RSUs.

Lu et al. [72] introduced a dynamic privacy-preserving key management method referred as DIKE, which is used to achieve and improve the confidentiality of data in location-based services (LBSs) in the VANET system. In order to control the eavesdropping attack, the confidentiality must be well maintained and the service contents from these kinds of attacks are protected. In this method, if a user does not engage in the VANET system, then the user may not join the current VANET system and thus cannot have an access on the current LBS content. To gain the confidentiality in an LBS session, all vehicle users who are joined are requested to share a secure session key, and that session key can be used to encrypt service contents.

5.3. Research Work on Data Integrity. To ensure the integrity of the sending message, digital signatures are used to generate and integrate with the messages [73]. In recent years, some work that presents the reliable information for securing data integrity in the VANET system is discussed below.

The main problem occurred when an inaccessible receiving location generates many current packets and forwards protocols inefficiently in VANETs. To solve this problem, Lin et al. [74] introduce a STAP approach to acquire the receivers' location privacy preservation in VANETs. By using the concept, vehicles always traveled to the busy places and downtown area such as shopping mall and busy street. In order to achieve data integrity, they deploy RSUs at the main social spot to form a social tier with them. Firstly, the sender computes MAC and attaches the generated code to the message before sending to the receiver. Once the message is received, in order to obtain integrity, the receiver uses the key session to check MAC. This method is limited to only busiest place, and due to traffic congestion, this algorithm may consume large memory.

Lin and Li [60] introduce an efficient cooperative authentication technique for the VANET system. This technique is used to shorten the authentication overhead on individual vehicles and to reduce the delay. To block the various attacks, this method uses token method to control and manage the authentication workload. When the vehicle passes the RSUs, the vehicle can get the evidence token from TA. Therefore, this token indicates that the vehicle contributed to cooperative authentication before. This method comprises the large computational algorithm to control the authentication issue.

Lin et al. [75] introduced a GSIS-based method which is used to develop secure privacy-preserving protocol based on the group signature and identity-based signature schemes. In case of dispute, the proposed method can also be used to trace each vehicle, but ID of the sending message needs to be disclosed by TA.

5.4. Research Work on Nonrepudiation. Li et al. [76] introduced a novel framework with conditional privacy preservation and repudiation (ACPN) for VANETs. This method utilized public key cryptography (PKC) to obtain nonrepudiation of vehicles by ensuring third parties to get real identities of vehicles. The identity-based signature (IBS) and ID-based online/offline signature (IBOOS) schemes are utilized for the authentication between V2V and vehicle to road side unit (V2R). This method significantly reduced the computational cost. However, the handling of managing certificates is complex due to IBS and IBOOS authentication schemes.

5.5. Requirement of Authentication. In VANETs, authentication can be done by two ways: firstly, at the level of node, called node authentication, and secondly, at the level of message level, called message authentication. Verifying the message integrity plays an important role to improve the

VANET security system. Therefore, message authentication is regarded as a key parameter in the VANETs [77].

In order to provide secure communication in VANETs, some requirements of authentication which must be satisfied are listed below.

5.5.1. Computational and Communication Overhead. Computational cost incurred due to large amount of cryptographic operation to be done by a vehicle or trusted authority for verifying an authentication request must be shortened. Furthermore, the time required to process a digital signature in authentication must be controlled.

5.5.2. Utilization of Bandwidth. The bandwidth utilization is very important in authentication and must be utilized properly in bytes per second (bps) to handle a request for an authentication such as exchanging cryptographic secret key and credentials.

5.5.3. Scalability. The process of authentication should be scalable which can handle multiple network operations and communications.

5.5.4. Time Response. The time which is needed to respond for an authentication mechanism must be reduced.

5.5.5. Powerful Authentication. The authentication schemes must have good capability to prevent VANETs from attacks.

6. Privacy-Preserving Authentication

Authentication plays a very important part to tackle all attacks which can verify whether a vehicle user is registered or not and a legitimate user before allowing them to access the VANETs. The vehicle user can differentiate between false and reliable information by using message authentication. Considering the verification pattern of messages, authentication schemes are further classified as one-by-one message verification [75] and batch verification [78]. Privacy is a system which is used to protect the sensitive and confidential information of the vehicles or passengers from the attackers. In addition to security issues, the privacy of vehicles should be considered an important issue in the VANET system. In recent years, several research works have been done in terms of security and privacy of the VANET system, which ensures vehicle safety and improves the traffic flow. Anonymous authentication is one of the well-known schemes. In the past, most of the recent existing works were relying on a pseudonym-based approach which can be used to protect the privacy and security of the vehicle users. By utilizing the pseudonym-based approaches, users can get better and robust privacy preservation. To control privacy attacks, the trusted authority needs to change pseudonyms frequently. The privacy is further categorized into two types: (i) privacy of user and (ii) user location privacy.

(i) *Privacy of User Protection*. This privacy is used to prevent the personal information of users from the malicious users or attackers.

(ii) *User Location Protection.* This privacy is used to protect user's information such as vehicle location at certain time or the area which the vehicles followed, and user personal information such as user ID and vehicle ID.

In vehicular networks, an authentication, security, and privacy leverage to develop trust among V2V and V2I communications. The main aim of the authentication schemes is to identify malicious nodes and bogus messages. Therefore, by utilizing suitable authentication schemes enable trusted authority to easily identify malicious users and fake messages that lead to provide secure communication in VANETs. In this context, several research works have been proposed related to authentication schemes which aim to protect VANETs from malicious users, fake messages, and unregistered entities and tackle all kinds of threats and attacks. Several of these schemes utilize cryptography techniques such as symmetric cryptography and asymmetric cryptography to authenticate messages in terms of signing and verifying messages. In this section, we present the authentication schemes in terms of cryptography and signature in detail as shown in Figure 5. The cryptograph-based authentication schemes are categorized into symmetric cryptography and asymmetric cryptography. Signature-based authentication schemes are classified into identity-based signature, certificateless signature, and group signature. These authentication schemes covered the recent state-of-the-art methods in VANETs.

6.1. Symmetric Cryptography. This authentication-based cryptography is also called as private key cryptography. This scheme utilizes message authentication code (MAC) to authenticate the messages. By using the shared secret key, sender can generate MAC for each message, and also all nodes in anonymity set verify the MAC attached with the messages by using that key. Symmetric cryptography is fastest and obtains robust computational efficiency because of a single key. To achieve a high level of reliability and privacy, Choi et al. [79] introduced a new method which can produce high efficiency of privacy by combining symmetric authentication with the short pseudonyms in VANETs. In this method, to generate short-lived pseudonyms, authority needs to send the different ID and seed value to each vehicle. And RSU is capable of performing verification for MACs because it can share keys with vehicles.

Xi et al. [80] proposed a random key-set-based authentication to maintain the user privacy by using zero-trust policy without having trust of central authority with user policy. In this method, the anonymity is improved by using independent keys for authentication at neighboring RSUs, and also identifying an attackers and key revocation has been considered in terms of practical application. This method is better but requires large amount of computational cost to handle zero-trust policy. As we know that, symmetric

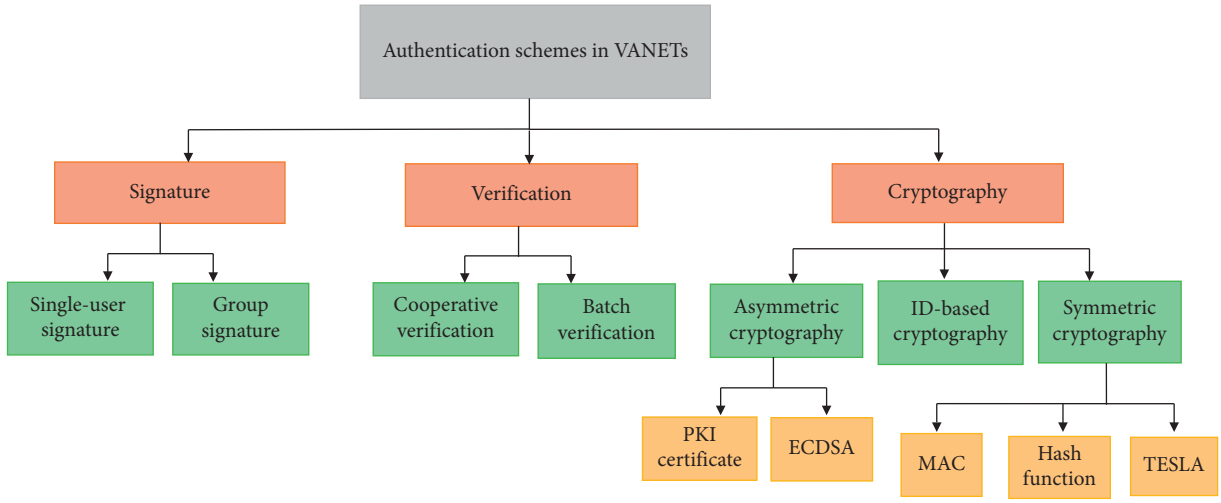

Figure 5: Categories of authentication in VANETs.

cryptography-based authentication consists of two major issues. Firstly, the key management system in VANETs is very weak which can increase the communication overhead and storage. Secondly, this technique has lack of non-repudiation; therefore, it is difficult to provide authentication to each vehicle.

Vijaykumar et al. [81] designed a trusted authority (TA) to facilitate online services to the customers via VANETs. Therefore, it is vital that the exchanged communication between the TA and VANETs preserves the confidentiality and authentication of messages. Besides that, a dual authentication and key management technique are used to provide a secure transmission of data in the vehicular network. Dual authentication technique offers a sufficient security to the vehicle which can efficiently intercept the malicious vehicles to enter in the VANETs.

Lin et al. [82] introduced a time-efficient and secure vehicular (TSVC) method with privacy preservation; this method is used to significantly reduce the packet consumption without limiting the security requirements. The authentication of the packet is done by MAC tag which is attached to each packet, but it required a fast hash operation to verify each packet. By using this method, the packet overhead is minimized by reducing the signature overhead and its verification latency, and the bandwidth utilization decreases with the decrease in the number of packet size. Rhim et al. [83] introduced an efficient method for MAC-based message authentication scheme, but this method cannot tackle and secure against the replay attack and requires a sophisticated algorithm which was proposed by Taeho et al. [84] by utilizing the improved MAC authentication scheme for the VANET system. Zhang et al. [85] presented a new method to authenticate a message by using the roadside unit-aided message authentication (RAISE) technique. In this approach, RSU verifies the authentication of messages which are transmitted from vehicles and notifies the results back to vehicles. Instead of verifying the message through traditional PKI-based scheme, they used the concept of each safety message attached with a MAC which was generated by the sender by using the secret key and RSU, and then RSU is responsible for verifying MACs and circulating the outcomes of message authenticity to other vehicles within their range.

The next category of symmetric cryptography is hash function which is responsible for examining the message integrity without any encryption of the message. The message is an input in hash function which can generate a fixed string referred as the hash value. In order to ensure the message integrity, the hash value must be attached with the sending message. Chuang et al. [86] introduced a decentralization-based lightweight authentication scheme named TEAM (trust-extended authentication mechanism). This technique uses the concept of transitive trust relation, but the amount of cryptographic data in TEAM is less compared with other existing methods because it only utilizes XOR and hash function during the authentication process.

Chim et al. [87] introduced a method which discussed the security and privacy issues of V2V in VANETs, and this scheme utilizes one-way hash function and secret key between vehicle and RSU. Therefore, this methodology can resolve privacy issue which may occur during communication. Vighnesh et al. [88] introduced a novel sender authentication technique for enhancing VANET security by using hash chaining and authentication code to authenticate the vehicle. This method ensures secure communication between vehicle and RSU, and a confidential data is encrypted through master key. Before sending packets to the authentication center, the RSU attaches its identity which can eliminate the possibility of rogue RSU abusing the VANET. He and Zhu [89] presented a method which addresses the problem of DOS attack against signature-based authentication. To tackle DOS attack, the preauthentication can be done before signature verification. In this scheme, the preauthentication mechanism is utilized, which takes the advantage of using one-way hash chain and a group rekeying technique.

The symmetric cryptography is further extended to timed efficient stream loss-tolerant authentication (TESLA).

In this approach, firstly the sender computes MAC using a known key and attaches a MAC to each sending message, and the receiving messages are buffered without authentication at the receiving part. The main disadvantage of TESLA is that the advance synchronization of the clock at receiving side is required with the clock at sending side. Additionally, TESLA is vulnerable to DOS attack in terms of memory which is caused by unregistered vehicles that utilizing receiver memory with fake messages [90, 91].

Jahanian et al. [92] introduced a TESLA-based technique; in this technique, timed method checking approach based on timed color Petri model is used to design and verify TESLA. Later, the researchers have found that the two factors need to be analyzed: the first is the security efficiency and the second is the percentage of successful attack. Studer et al. [93] introduced a modified form of TESLA which is known as TESLA++, and it provides the same broadcast authentication which is computationally efficient as TESLA with less memory consumption and also presented a method to effectively verify the new RSUs and OBUs which encountered during communication. The goal of TESLA++ is to control memory DOS attacks, which can be obtained by receivers self-generated MAC which may lower down the memory requirements for authentication. However, TESLA does not offer multiple hops authentication and nonrepudiation [91].

6.2. Asymmetric Cryptography. The next authentication scheme in VANETs is referred as asymmetric cryptography which is also called as public key cryptography. This technique can be used to encrypt and decrypt a message to ensure the security of data in major communication networks. Specifically, the asymmetric can be used to encrypt a message which can be done either by using a public key or by generating a digital signature. Normally, a private key is only used for decrypting an encrypted message and verifying digitally signed message.

In general, mostly vehicles contain public or private key for pseudonymous communication. In order to achieve in a secure and reliable way, the public key certificates are the best method which is used in public key infrastructure (PKI) to authenticate vehicles; it contains the digital signature of the certification authority (CA) and vehicle key for authentication [23]. The CA is the centralized management unit which is responsible for certifying nodes, keys, etc. Furthermore, it can also authenticate the vehicles in V2V communication. Every vehicle needs to be registered with CA database before it officially joins the VANET system; the vehicle can communicate with CA in two ways either directly as an offline registration or via RSU as an online registration by indirect way. Raya and Hubaux [94] introduced a new method which utilizes the anonymous public keys to provide privacy. The anonymous keys must be changed in the way that the receiver will not be able to track the vehicle owner key. The main demerits are it required a large amount of storage and memory and also requires huge amount of certificate revocation list (CRL) checks, since using large amount of anonymous keys. Therefore, it may be the reason for DOS attack due to large amount of computational overhead.

Calandriello et al. [95] introduced a robust pseudonym-based authentication method to reduce the security overhead, but the robustness of traffic safety is maintained. This scheme alleviates the limitations of a pseudonym by using the combination of baseline pseudonym and group signature which can generate own pseudonym on-the-fly and self-certification [91]. And it minimizes the requirements of handling pseudonym in authentication. Wasef and Shen [96] introduced an expedite message authentication protocol (EMAP) which adopts PKI and CRLs for their security. In this scheme, EMAP of VANETs replaced the lengthy process of CRL by an effective revocation process. This process uses keyed hash message authentication code (HMAC) in EMAP. The purpose of key is used to calculate HMAC and to share only among nonrevoked OBUs to safely share and update the secret key. The proposed scheme significantly reduces the message loss ratio in EMAP caused by the conventional authentication schemes.

Eichler [97] proposed a new scheme in which vehicles generate a request to CAs for short-term pseudonyms during specific intervals. To reduce the communication overhead with CAs, Zeng [98] introduced the self-issuance scheme to enable vehicle to generate pseudonyms independently. Lu et al. [99] introduced a new method for effective pseudonyms changing at social spot (PCS) for privacy of location, by determining the several vehicles gathered on specific spots such as intersection or parking area. It utilizes anonymity size as a privacy metric (ASS), and if ASS reaches threshold, then the pseudonyms are changed simultaneously. However, it cannot perform well in low density.

In the year 2010, Schuab et al. [100] proposed a new approach that does not depend on pseudonyms-identity mapping to achieve accountability, but instead, resolution information is embed with V-token pseudonym certificates. In this scheme, by using V-token approach, each vehicle carries its own resolution information which can provide scalability. The main challenge is the revocation of pseudonym certificate which may limit the scalability in the VANET. In case, if the vehicle long-term certificate is revoked, then the vehicle cannot obtain a new pseudonym from CAs. In recent years, few works have been proposed on the CRL distribution methods [101, 102]; these methods cannot stop the revoked vehicle from continuous communication in VANETs until and unless all the pseudonyms become inactive. The drawbacks of checking CRL process make it not reliable to authenticate a large number of messages under the specific period in VANETs [103].

Azees et al. [104] introduced an effective anonymous authentication with conditional privacy (EAAP) scheme to avoid a malicious vehicle entering in the VANETs. This scheme is used to track mechanism and track vehicles or RSUs that create disturbance for VANETs. Recently, bilinear pairing has been introduced in which trusted authority (TA) in EAAP does not require to keep the anonymous certificate of the vehicles and RSUs [105]. Additionally, the TA has the right to cancel the anonymity of a disobedient vehicle and reveal their identity in a group. Then, the revoked identity

added to the identity revocation list (IRL) managed under the supervision of TA.

The next part of asymmetric cryptography is ECDSA authentication scheme which is an analogue type of digital signature depending on elliptic curve cryptography [106]. Manvi et al. [107] introduced an ECDSA-based message authentication scheme in VANET. This technique utilizes a secure hash algorithm (SHA) by the sending vehicle to generate private and public key and also creates hash of the message by using SHA. At the receiving part, the received message is decrypted by using the public key. Kalkundri et al. [108] presented a new technique which utilizes ECDSA algorithm to obtain the message authentication. Furthermore, it can also provide security in terms of point-to-point (p2p) mechanism to obtain authentication in VANETs. The combination of p2p and ECDSA along with VANET can improve the efficiency of the algorithm and also minimizes the message delay. Smitha et al. [109] proposed a new method, classification of critical safety message and provided an adaptive way to authenticate the message based on Merkle tree and ECDSA. This scheme discussed the DOS, man-in-the-middle, and phishing attacks. Furthermore, this approach can increase the message authentication delay.

6.3. Identity-Based Signature. The signature based on identity called as IBS which uses node identifiers in terms of public key and sign messages with the private key which is generated from the identifiers [110]. In IBS, the private key generator (PKG) used as a third trusted authority for generating and assigning the private key. Recently, a new identity-based signcryption (IBSC) has been introduced by utilizing bilinear pairing which required strict analysis of security based on robust security modeling without considering random oracle background, indicating that the IBSC is considered as a reliable method [111].

IBS is a four-step process such as setup, key extraction, signature signing, and verification. The details are discussed below:

(i) *Setup*. In this category, firstly PKG evaluates the master key and public parameters. Then, PKG can disclose these parameters to all vehicles publicly in the VANET.

(ii) *Key Extraction*. In this part, PKG uses the vehicle ID and master ID to compute a private key, and then the PKG sends these private keys to communicate with vehicle through a secure channel.

(iii) *Signing Signature*. Signature SIG can be generated by using a private key by assuming a message M and timestamp T.

(iv) *Verification*. This algorithm is used to find out whether SIG is valid or not by having these parameters such as ID, SIG, and M.

To overcome the computational overhead in the IBS method for VANETs, in the year 2012, Lu et al. [112] proposed a new method with adaptive privacy to authenticate vehicles by using ID-based online/offline authentication (IBOOS). In [113], Zhang et al. introduced an identity-based technique for signature hierarchical aggregation and batch verification. In this approach, identity-based signatures are generated from different vehicles, which can be aggregated and verified in a batch, and the message collector is used to reaggregate the aggregated signatures. This scheme significantly reduced the large computational process of certification verification by utilizing the identity-based vehicles and RSUs. In 2001, a new method has been proposed based on trapdoor hash function to develop a new hash-sign-switch paradigm, which can convert signature into highly online/offline signature. Due to good pairing process, the efficiency of this method is better than the IBS scheme. However, the requirement of memory storage space makes IBOOS unsuitable for VANETs [114]. In the verification process, the IBS eliminates the requirement of certificates which can be used in the verifications of public keys. Thus, it did not need to distribute public keys which are related to certificates [23]. Specifically, only PKG knows the private keys in VANETs because it is generated by PKG in IBS which may generate escrow problem. To overcome this problem, in the year 2017, Zhang et al. [115] introduced an efficient technique to authenticate vehicle protocol named distributed aggregate privacy-preserving authentication (DAPPA) which is based on multiple trusted authority with IBS technique.

In [116], Zhang introduced a novel approach based on new security tool named one-time identify-based authenticated asymmetric group key to develop cryptography mix-zone (CMIX) against eavesdropping.

In 2018, Zhang et al. [117] introduced a secure privacy-preserving communication scheme for establishing vehicle cloud (VC) and data broadcasting in VC. In this approach, a group of vehicles which are located nearby in VANETs are used to develop a secure and dynamic VC. Therefore, it enables all the vehicle resources to be integrated and exchanged data securely, and any cloud user can process their data securely once the VC is formed.

Figure 6 illustrates the diagram of DAPPA, in which RSU consists of large communication range as compared to the vehicles. Each RSU consists of an initial key pair and a corresponding certificate which is issued by the trusted authority [23]. Every vehicle contains secret to develop secure channels with RSUs, and every vehicle generates a request to RSUs when entering in the communication range to share its private key. After the authentication is done, RSUs share the private key and authorized period to the vehicle, but this sharing only utilized within the authorization period and will be deleted later. Additionally, the vehicle can utilize the sharing to generate a one-time private key and then the MTA-OTBIAS. Finally, on the corresponding message, the MTA-OTBIAS can be aggregated and verified by other vehicles. By using private key, DAPPA resolves the escrow problems which are not familiar by root TA, and this can lead to increase the complexity because vehicle needs to request the shares from adjacent RSU. Furthermore, the utilization of the private key and ID-based signature can cause the delay and significantly reduces the communication efficiency in the VANET system [23].

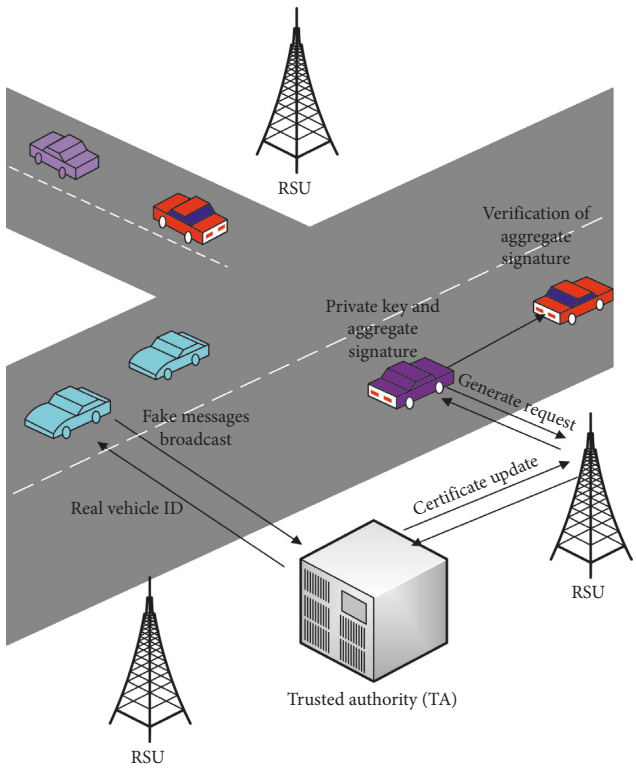

Figure 6: Graphical representation of DAPPA.

6.4. Certificateless Signature. The certificateless signature is used to overcome the high cost of certificates based on the PKI technique to resolve the escrow issue in IBS. In the year 2003, certificateless public key mechanism is presented for the first time [118]. In the certificateless cryptography, the key generation center (KCG) plays an important part which works as a third party and is responsible for providing the user with private partial key ***DIDi*** which is evaluated from the identity of user ***IDi***.

Basically, the secret value user can generate the actual private key and the partial private key delivered by key generation center (KGC). In contrary with ID-based cryptography scheme, the KGC may not have access with this type of private key. Consequently, a user can use secret values and different parameters to produce his public key identity known as ***PKIDi***. The certificateless signature (CLS) method is categorized into seven different algorithms: setup, partial private key extract, set secret value, set private key, set public key, sign, and verify [118]. All these techniques are discussed below:

(i) *Setup.*Setup utilizes a security parameter k to produce the master key *msk* and master public key *mpk*. Furthermore, it can also produce parameter *param* which can be distributed among all nodes [23].

(ii) *Partial key*. It can produce a partial private key D_{ID} by having different parameters such as master key, master public key, system parameters, and an identity ID [23].

(iii) *Secret value*. The secret value x_{ID} is generated by using master public key and system parameter *param* [23].

(iv) *Set Private Key*. This algorithm utilizes *param*, partial private key D_{ID}, and secret value x_{ID} as input parameters. The secret value x_{ID} is used to transform D_{ID} into full private key P_A. The algorithm returns P_A [118].

(v) *Public Key*. It generates the public key PK_{ID} by using different parameters such as master key, system function, an identity, and its secret value [23].

(vi) *Sign*. It generates certificateless signature μ by using system parameter *param*, master public key *mpk*, an identity ID, secret value x_{ID}, partial key D_{ID}, and a message M [23].

(vii) *Verification*. It can verify the signature by using several parameters such as system parameter *param*, master public key *mpk*, identity ID, public key PK_{ID}, and a message/signature pair (M, μ) [23].

The security models are further classified into two types: super type I adversary $\boldsymbol{A_I}$ and super type II adversary $\boldsymbol{A_{I\ I}}$ [119]. $\boldsymbol{A_I}$ solves the real-world adversary who can obtain IDs some valid signatures, while $\boldsymbol{A_{I\ I}}$ solves the malicious KCG which contains master secret key and can be able to initiate the attack such as eavesdropping attack on signatures and create signing queries. In recent years, few research works have been proposed regarding certificateless signature referred as certificateless short signature (CLSS), which improved the performance of this scheme [120, 121]. This scheme proposed a secure method against $\boldsymbol{A_I}$ and $\boldsymbol{A_{I\ I}}$ in the random oracle model [23]. At the end of 2014, several researchers have proposed CLS scheme without utilizing any pairing to increase the efficiency, but the signature length is very large which cannot constraint the unlimited bandwidth and storage devices in VANET [122, 123]. In the year 2015, a new scheme of V2I communication based on certificateless signature is introduced. In this technique, conditional privacy preservation is obtained by mapping the traffic message transmitted by the vehicle into false identity. In case of dispute, the responsible authority can recover the real identity from the pseudoidentities [124]. Furthermore, this method produces efficient computational overhead in comparison with other competent techniques. At the beginning of 2018, Cui et al. [125] introduced a new method for certificateless aggregate signature based on elliptic curve cryptosystem (ECC) which can support conditional privacy preservation. It provides secure communication between V2I in VANET. Furthermore, it can satisfy privacy requirements and also achieve lower message overhead which are advantageous over other methods.

6.5. Group Signature Scheme. The vehicles' privacy is preserved in group signature, which can allow registered members of the group to sign up for the messages anonymously as a representative of the group [14]. The head of the group has the right to find out which sign is coming from the original sender. This algorithm usually requires large amount of time to verify signature which makes it limited to time-related applications in VANETs.

In 2010, Zhang et al. [126] proposed an efficient method which utilized each RSU to maintain and manage on-the-fly group within its range of communication, and the vehicles which are entered in the group can secretly send V2V messages that can be further verified by users of the same group, if any bogus message produced by the vehicle can be traced by the trusted authority. In the year 2011, Park et al. [127] presented a RSU-based decentralized key management (RDKM) which is used only for multicast services in VC systems. This scheme reduced the large amount of rekeying overhead by contributing some portion of the key management functions to the RSUs and also through updating the key encryption keys (KEKs) within the RSUs.

To alleviate the overhead of revocation, the distributed management system is used, which is a promising approach; based on this technique in the year 2012, Sun et al. [128] introduced a distributed key management system (DKM) in the VANET system; in this scheme, domain is formed into small subregions, and the vehicle needs to update its secret key from the regional head of the group who is responsible for managing the region. In this approach, during the updating process, the DKM restricts the vehicle to disclose the updated value of a secret key to the regional head of the group. However, the anonymity feature of group signature makes it vulnerable to attack by a malicious user through broadcasting fake messages. Malina et al. [129] introduced a group signature with short-term linkability and categorized the batch verification, and this method produces efficient signing and verification as compared to other competent methods. In [130], Zhang et al. introduced a location-based service (LBS) protocol, which is used to address the inherent challenges in terms of authentication and conditional privacy to offer LBSs in VANETs. In this scheme, the providers of RSUs and LBS are identity based, and a vehicle only requires a member key. By using this, the key vehicle can generate verifier-location group signatures. The LBS validates these signatures without interfering the privacy of a vehicle. If an LBS request is found to be false, then the key generation certificate can evaluate the vehicle ID.

Islam et al. [131] introduced a password-based conditional privacy-preserving authentication and group-key generation (PW-CPPA-GKA) protocol for the VANET system. This method provides several features such as user exiting, user entering, and changing password. This protocol is computationally stable as it is designed without using bilinear pairing and elliptic curve techniques.

7. Simulation Techniques in VANETs

Simulation tools are considered as the most important tool to evaluate and analyze the performanceof any network or system in order to highlight any existing issues. Simulation tools are used to obtain the theoretical results based on the observations.

In VANETs when designing and developing applications for VANETs, privacy and security should be considered seriously. The main problem occurs when evaluating the performance of security and privacy due to the limited features of the VANET system in terms of mobility, network structure, and decentralization. To get the optimal solution, it is important to design and develop sophisticated simulation tools which can be used to produce the VANET results efficiently. VANET simulation tools are categorized as mobility simulator and network simulators. Specifically, mobility simulator is used to generate vehicle mobility [23]. Network simulator is mainly used for evaluating the performance of the VANETs and also indicates the issues related to the network.

7.1. Mobility Simulator. In the VANET system, mobility model can determine the movements of the node which are linked with the simulator; by using this terminology, simulator generates random topology based on each vehicle condition [20]. The mobility model consists of two patterns named the traffic and the motion patterns, respectively. The motion pattern is determined by the behavior and attitude of drivers which can create vehicle movements with the pedestrians and vehicles [20]. The traffic generator produces random topologies and map, which are used to evaluate the vehicle behavior according to the traffic environment. Generally speaking, it is a big challenge to manage system modeling to integrate with the real traffic environment. Therefore, the designing of the mobility model can be done by using several other types of models depending on the traffic conditions and situations. The mobility model can be categorized into two types: macroscopic and microscopic models [23].

METACOR [132] utilizes traffic at high scale and also used to determine the vehicle attitude. METACOR is very useful to provide the macro of traffic environment.

VanetMobiSim [133] is an extended version of CanuMobiSim. It aim to extend support to CanuMobiSim in terms of vehicle mobility to a higher level. It reviews the microscopic and macroscopic mobility and outline the details to both scopes.

SUMO [134] is an open source microtraffic simulator that can generate the vehicle traffic and update the vehicle parameters such as speed and positions. It is a microscopic traffic simulation which can import city maps with different file format and version. Each vehicle contains user ID, time of departure vehicle, vehicle routes and location, etc. [134]. Additionally, SUMO is capable of handling highly integrated simulations which can be used for large networks, and it can be able to get the timely feedback from the network simulator. Specifically, SUMO is more reliable and suitable for V2X communication by considering an individual vehicle behavior and feedback of each vehicle by updating the network simulator for future processing.

7.2. Network Simulator. The University of California located in Berkley and the VINT project have developed the NS-2, a discrete simulator which is applied in networking research. Recently, many network simulators such as NS-2 [135], NS-3 [136], GlomoSim [137], and OMNeT++ [138] are used to evaluate the performance of the model and measure the privacy and security of routing protocols in VANETs.

Additionally, many programming languages such as C++ and JAVA are used to construct simulators.

The NS-2 simulator is designed and written in C++ with an object tool command language (OTCL). NS-2 is mainly used for research in network communication to support simulation for routing, and multicast protocol through wired networks [135]. The main disadvantage of NS-2 is that the node must be programmed manually by the users in order to find the vehicle in their vicinity and establish communication. To overcome this problem, NS-3 provides an optimal solution, which is used to improve the network modeling and reliability; NS-3 can also provide interface for Python and mechanism to integrate with other open source platforms [136].

The global mobile information system (GlomoSim) was developed in California, USA, which is used to simulate the wireless network. It is one of the most famous techniques of network simulator after NS-2. GlomoSim is capable to run on shared-memory symmetric processor (SMP) and assist in dividing the network into separate modules and each functions with the different process [20]. The main purpose of GlomoSim is to support millions of nodes performed as a single simulation. Aggregation of nodes and layer is the limitation of the most network simulators.

The OMNeT++ is the discrete simulation library which was developed to simulate the network communication, multiprocessing, system configurations, and other distributed systems [138]. Specifically, OMNET++ provides a simulation platform which can be used to design simulation modeling and also provide more reliability for the larger mobility of VANET application [23].

7.3. Simulation Overview. To change traffic settings, the information which is received from the network simulator must be processed by mobility simulator. SUMO is used to generate high mobility traffic to simulate the vehicular network because of its unique characteristics of network traffic. SUMO has function which can simulate single part and whole cities in one simulation [139].

The traffic and network simulator environment (TraNS) is a JAVA-based visualizing tool, which consists of SUMO and NS-2 which is specially designed for the VANET system. A new TraNs Lite version is developed for mobility generator which excluded NS-2 network simulator [20]. The major disadvantage of TraNS simulator is that it cannot support highly large-scale network and is also not cost-efficient in terms of acquiring protocol of VANETs [140].

An integrated wireless and traffic platform for real-time road traffic management solution (iTETRIS) [141] aims to enhance the large-scale simulation network of VANETs for evaluating the services for transport and traffic management. In order to obtain the real-time closed-loop coupling simulation platform, the iTETRIS combined with SUMO and NS-3 can be considered as an extension of TraNS [140].

The vehicles in network simulation (Veins) is an open source framework [142] which is used to run vehicular network simulations. Veins implements IEEE 802.11p protocol at the physical and the MAC layers and is responsible for managing the data transfer between OMNET++ and SUMO through TraCI [143]. The main advantages of bidirectional coupling are twofold: Firstly, the network simulation mainly controls the mobility of simulation for handling the traffic communication in VANETs. Secondly, information which includes position or routes may be provided by mobility simulation to the network simulation. Additionally, the Veins offers comprehensive function to achieve bidirectional coupling which can provide better accuracy to the development of protocols [142].

7.4. Simulation Tools and Performance of Authentication Schemes. In order to evaluate which algorithm of authentication schemes obtained the better results in each of its category, several papers have been reviewed related to the authentication schemes. In symmetric cryptography, Vijayakumar et al. [81] obtained a better result by using JAVA-based simulator, which considers multiple nodes and each node acts as a VANET user. Also, the proposed dual key management scheme significantly obtained computationally efficient and secure data transmission. Thus, in symmetric cryptography, this scheme obtains better results as compared to the other competent methods.

In asymmetric cryptography, Azees et al. [104] introduced EAAP scheme to avoid malicious users to enter in VANETs. In this approach, Cygwin 1.7.35-15 with the gcc version 4.9.2 has used to evaluate the computational performance of EAAP. The proposed scheme achieved low computational cost by verifying the multiple signatures and certificates in 300 ms as compared to the other competent methods in asymmetric cryptography scheme.

In identity-based signatures, Zhang et al. [113] introduced privacy preservation scheme based on identity-based signature. The proposed method used NS-2 [135], VanetMobiSim [133], and the cryptography library MIRACL [144] to evaluate the performance by assuming different degree parameters and generating the vehicle mobility with the speed ranging from 50 to 60 km/h. This scheme is significantly used to reduce the transmission overhead and also minimize the vehicle waiting time to initiate the batch verification process, and thus, this scheme is the best scheme among other competent methods.

In certificateless signature, Cui et al. [125] introduced certificateless signature based on ECC, which can be able to support conditional privacy preservation. Several different parameters have been used to evaluate the performance of this scheme. Bilinear pairing is created with security level of 80 bits. In the system model, two different layers of the vehicular network are considered: the first layer consists of a vehicle and RSU, and the communication medium between OBUs and RSUs is 5.9 GHz DSRC, and the second layer consists of TA and KGC. In this approach, each vehicle transmits traffic-related message in 300 ms, and the total time that needed to verify more than 650 signatures is less than 300 ms. Thus, it can verify the large number of messages simultaneously. In the proposed method, the message overhead is significantly reduced along with the less computational and transmission cost as compared to the other certificateless signature schemes.

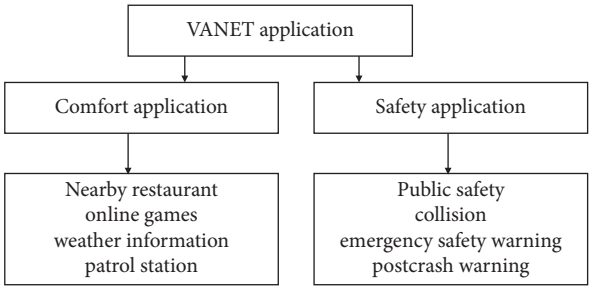

Figure 7: VANET applications.

For group signature scheme, Zhang et al. [130] introduced location-based service (LBS) protocol. In order to evaluate the efficiency of the proposed method, this scheme considered LBS and revocation stages. In the simulation, the cryptography tool MIRACL [144] and MNT curve implemented on embedded degree, which is built in C language, are used. In each LBS event, RSU processes only one pair to decrypt the message which required 2.17 ms. This approach can protect the identity and privacy of the vehicle by providing the service to the vehicle anonymously. Thus, it can outperform other competent methods.

8. VANET Applications

VANETs are used to provide communications to nearby vehicles in terms of V2V and vehicles to other communication devices such as V2I and V2R. The RSU is maintained and managed by the government authorities but run by a private organization to handle the operation in some countries. The types of VANET application are discussed below (Figure 7).

8.1. Comfort Applications. This VANET application is referred as a nonsafety application, which aims at enhancing drivers and passenger's comforts. It can provide the driver and passenger with the updated climate information, hotels, nearby restaurant, and patrol stations. Furthermore, passengers can play games online, get Internet access, and send and receive messages when vehicle is within the range of the network [145].

8.2. Safety Applications. The safety applications of VANETs are used to enhance the protection. In this application, vehicle-to-vehicle and/or vehicle-to-infrastructure communications can be used to improve the traffic safety, lane changing warning, emergency video streaming, avoiding collisions, and accidents. The main purpose of this application is to ensure the safety of drivers, passengers, and pedestrians [145].

The requirements of all the VANET applications have a common set of requirements which is defined as 10–1000 m coverage, with a speed of maximum 500 km/h, and latency range varies from 50 to 500 ms. Additionally, the compactness of the network must be split into small groups of 2–20 vehicles and considers the traffic bottlenecks with 1000 s of vehicles per radio cell in the vicinity.

9. Conclusion

In an intelligent transportation system, VANETs are considered as a more vital and promising research area due to its unique characteristics; thus, security and privacy are considered as critical issues. The aim of VANET is to ensure the safety of human living on the street by broadcasting safety messages among the vehicles and also provide comfort services to the passengers. The safety messages are broadcasted in an open environment that can make the VANETs more vulnerable to attacks. Therefore, a sophisticated and robust security algorithm must be designed to tackle dangerous security and privacy attacks.

After reviewing the several articles regarding different state-of-the-art schemes for security and privacy threats in VANETs and to address these problems, this paper provides a comprehensive survey which covers most of the VANET issues, particularly the VANET system model, architecture, standards, and security and challenges issues of VANETs. Firstly, we have discussed the basic model and function of the VANETs. Then, the security services and threats and attacks on these services followed by the recent state-of-the-art schemes on each security service are explained. Secondly, we have comprehensively covered the authentication schemes, which are able to protect the vehicular network from malicious nodes and fake messages. Finally, we have discussed the various simulation tools, followed by the performance of authentication schemes in terms of simulation tools and the applications of the VANET system. Specifically, this survey is well studied and covered most aspect in security issues, focusing on novel privacy-preserving methods, filling the gaps of existing surveys, and incorporating the latest trends in VANETs.

In our opinion, the future research direction for the VANET system must be focused on security and privacy issues such as privacy preservation, which required more amount of research in order to tackle the security and privacy threats. In addition to these, the security system must be enhanced by robust authentication schemes for providing secure communication in VANETs. Also, an efficient algorithm is required to handle all kinds of security attacks.

The rapid demand of V2X, C-V2X, and LTE-V communications in the ITS, the traffic information such as vehicle ID and location, and the weather conditions can be shared between vehicles. The drivers and passengers are looking for the reliability and trustworthiness of the large amount of information and data exchanged which required protection and privacy. Thus, they require sophisticated VANET algorithm which can provide trustworthy communication between V2V and V2I and also protect their vehicles ID and location privacy.

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 no. 2018YFB1600503, the Natural Science Foundation of China under Grant nos. U1564201, 1664258, and 61773184, Six Talent Peaks in Jiangsu Province under Grant no. DZXX-048, the College Graduate Research Innovation Program of Jiangsu University under Grant no. 18KJA580002, and the Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD).

References

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

[3] S. Biswas, J. Mišić, and V. Mišić, "DDoS attack on WAVE-enabled VANET through synchronization," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 1079–1084, Anaheim, CA, USA, 2012.

[4] 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.

[5] M. Smita and N. Pathak, "Secured communication in real time VANET," in *Proceedings of the International Conference on Emerging Trends in Engineering and Technology (ICETET)*, pp. 1151–1155, Nagpur, India, 2009.

[6] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Vehicular Communications*, vol. 1, no. 1, pp. 33–52, 2014.

[7] A. Stampoulis and Z. Chai, "A survey of security in vehicular networks," *Project CPSC*, vol. 534, 2007.

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

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

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

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

[12] L. Zhang, "Key management scheme for secure channel Establishment in fog computing," *IEEE Transactions on Cloud Computing*, 2019.

[13] 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.

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

[15] R. Mishra, A. Singh, and R. Kumar, "VANET security: issues, challenges and solutions," in *Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1050–1055, Chennai, India, March 2016.

[16] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621–1632, 2019.

[17] R. Akalu, "Privacy, consent and vehicular ad hoc networks (VANETs)," *Computer Law & Security Review*, vol. 34, no. 1, pp. 37–46, 2018.

[18] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *Cognitive Systems Research*, vol. 55, pp. 153–163, 2019.

[19] J. P. Hubaux, S. Capkun, and J. Jun Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49–55, 2004.

[20] 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.

[21] B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: a survey," *Journal of Network and Computer Applications*, vol. 40, pp. 363–396, 2014.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] X. Liang, T. Yan, J. Lee, and G. Wang, "A distributed intersection management protocol for safety, efficiency, and driver's comfort," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1924–1935, 2018.

[28] T. Neudecker, N. An, T. Gaugel, and J. Mittag, "Feasibility of virtual traffic lights in non-line-of-sight environments," in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications—VANET'12*, pp. 103–105, Lake District, UK, June 2012.

[29] Draft guide for wireless access in vehicular environment (WAVE) architecture 2012, http://ieeexplore.ieee.org/servlet/opac?punumber-6320593.

[30] M. Ghosh, A. Varghese, A. A. Kherani, and A. Gupta, "Distributed misbehavior detection in VANETs," in *Proceedings of the IIEEE Wireless Communications and Networking Conference (WCNC)*, Budapest, Hungary, April 2009.

[31] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-Enabled cooperative intelligent vehicular (5GenCIV) framework: when benz meets marconi," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 53–59, 2017.

[32] S. S. Kaushik, "Review of different aproaches for privacy," *International Journal of Advanced Engineering and Technology*, vol. 5, no. 2, pp. 356–363, 2013.

[33] M. Gonzalez-Martin, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, "Analytical models of the performance of C-V2X mode 4 vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1155–1166, 2019.

[34] H. Chen, R. Zhang, W. Zhai, X. Liang, and G. Song, "Interference-free pilot design and channel estimation using ZCZ sequences for MIMO-OFDM-based C-V2X communications," *China Communications*, vol. 15, no. 7, pp. 47–54, 2018.

[35] Cellular-Vehicle-to-Everything-C-V2X, https://internetofthingsagenda.techtarget.com/definition/Cellular-Vehicle-to-Everything-C-V2X.

[36] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: a new 5G technology for short-range vehicle-to-everything communications," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 30–39, 2017.

[37] S. Chen, J. Hu, Y. Shi, and L. Zhao, "LTE-V: a TD-LTE-based V2X solution for future vehicular network," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 997–1005, 2016.

[38] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, *Overview of Security Issues in Vehicular Ad Hoc Networks*, Hershey, Derry Township, PA, USA, 2010.

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

[40] Federal Communications Commission, "Amendment of the commission's rules regarding dedicated short-range communication service in the 5.850–5.925 GHz band, FCC 02-302," Technical Report, Federal Communications Commission, Washington, DC, USA, 2002.

[41] Dedicated short range communications (DSRC) home," 2017, http://www.leearmstrong.com/dsrc/dsrchomeset.htm.

[42] ITS standard fact sheets of IEEE 2014, http://www.standards.its.dot.gov/factsheets/factsheet/80.

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

[44] 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.

[45] M. Misra, I. Woungagng, and M. Chandra, *Guide to Wireless Ad Hoc Networks*, Vol. 427–454, Springer, Berlin, Germany, 2009.

[46] V. S. Yadav, S. Misra, and M. Afaque, *Security of Wireless and Self-Organizing Networks: Security in Vehicular Ad Hoc Networks*, CRC Press, Boca Raton, FL, USA, 2010.

[47] Y. Qian and N. Moayeri, "Design of Secure and Application-Oriented VANETs," in *Proceeding IEEE Vehicle Technology Conference (VTC Spring)*, pp. 2794–2799, Calgary, Canada, September 2008.

[48] 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, 2016.

[49] F. A. Hawi, C. Y. Yeun, and M. A. Qutayti, "Security challenges for emerging VANETs," in *Proceedings of the Fourth International Conference on Information Tecnology, ICIT 2009*, pp. 3–5, Amman, Jordan, December 2009.

[50] M. Kassim, R. Rahman, and R. Mustapha, "Mobile ad hoc network (MANET) routing protocols comparison for wireless sensor network," in *Proceedings of the IEEE International Conference on System Engineering and Technology, ICSET*, pp. 148–152, Shah Alam, Malaysia, January 2011.

[51] 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, Singapore Springer, 2015.

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

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

[54] M. Raya and J. P. Hubaux, "DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots," in *Proceedings of the International Conference Mobile Systems, Applications and Services (MobiSys2004)*, Boston, MA, USA, June 2004.

[55] M. Lal, A. Saxena, V. P. Gulati, and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," *Computers & Security*, vol. 25, pp. 184–189, 2006.

[56] M. Raya and J. P. Hubaux, "Security aspects of inter-vehicle communications," in *Proceedings of the Fifth Swiss Transport Research Conference (STRC)*, Ascona, Switzerland, March 2005.

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

[58] J. R. Douceur, "The sybil attack," in *Peer-To-Peer Systems*, pp. 251–260, Springer, Berlin, Germany, 2002.

[59] H. Wen and J. Dyer, *Countermeasures for GPS Signal Spoofing*, University of Oklahoma, Norman, Oklahoma, USA, 2011.

[60] X. Lin and X. Li, "Authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.

[61] http://searchsecurity.techtarget.com/definition/masquerade.

[62] http://careerride.com/Networking-replay-attacks.aspx.

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

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

[65] 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, Novenber 2007.

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

[67] T. Kitani, T. Shinkawa, N. Shibata, K. Yasumoto, M. Ito, and T. Higashino, "Efficient VANET-based traffic information sharing using buses on regular routes," in *Proceedings of the Vehicle Technology Conference, VTC Spring*, pp. 3031–3036, IEEE, Singapore, May 2008.

[68] J. Okamoto and S. Ishihara, "Distributing location-dependent data in VANETs by guiding data traffic to high vehicle density areas," in *Proceedings of the IEEE Vehicular Networking Conference*, pp. 189–196, Jersey City, NJ, USA, December 2010.

[69] M. Akila and T. Iswarya, "An efficient data replication method for data access applications in VANETs," in *Proceedings of the Internatioanl Conference on Electronics, Communication and Computing Technologies (ICECCT)*, Pauls Nagar, India, September 2011.

[70] S. Park and S. K. Lee, "Improving data accessibility in vehicle ad hoc network," *International Journal of Smart Home*, vol. 6, no. 4, pp. 169–176, 2012.

[71] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[72] R. Lu, X. Lin, X. Liang, X. Shen, and X. S. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2012.

[73] 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, Ak, USA, May 2007.

[74] X. Lin, R. Lu, X. Liang, and X. S. Shen, "STAP: a social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in *Proceedings of the 30th IEEE INFOCOM*, pp. 2147–2155, Shanghai, China, April 2011.

[75] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[76] J. Li, H. Lu, and M. Guizani, "ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[77] M. Bellare and P. Rogaway, *Introduction to Modern Cryptography*, CRC Press, Boca Raton, FL, USA, 2005.

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

[79] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proceedings of the 1st ACM International Workshop Quality Service Security Wireless Mobile Network*, pp. 79–87, Quebec, QC, Canada, October 2005.

[80] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proceedings of the 8th International Symposium IEEE Autonomous Decentralized System (ISADS)*, pp. 344–351, Sedona, AZ, USA, March 2007.

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

[82] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987–4998, 2008.

[83] W. Rhim, "*A study on MAC-based efficient message authentication scheme for VANET*," M.S. thesis, Hanyang University, Seoul, South Korea, 2012.

[84] S. Taeho, J. Jaeyoon, K. Hyunsung, and L. Sung-Woon, "Enhanced MAC-based efficient message authentication scheme over VANET," in *Proceedings of the 7th International Multi-Conference on Engineering and Technological Innovation, IMETI*, pp. 110–113, Orlando, FL, USA, January 2014.

[85] C. Zhang, X. Lin, R. Lu, P. Ho, and X. S. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008.

[86] M. Chuang and J. Lee, "TEAM : trust-extended authentication mechanism for vehicular ad hoc networks," in *Proceedings of the International Conference on Consumer Electronics, Communications and Networks CECNet*, pp. 1758–1761, Xianning, China, April 2011.

[87] T. W. Chim, S. M. Yiu, L. K. Hui, and V. K. Li, "Security and privacy issues for inter-vehicle communcations in VANETs," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Net-works Workshops*, pp. 1–3, Rome, Italy, June 2009.

[88] N. V. Vighnesh, N. Kavita, R. U. Shalini, and S. Sampalli, "A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks," in *Proceedings of the IEEE Symposium on Wireless Technology and Applications ISWTA-2011*, pp. 25–28, Langkawi, Malaysia, September 2011.

[89] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," in *Proceeding IEEE International Conference on Computer Science and Automation Engineering CSAE-2012*, pp. 261–265, Zhangjiajie, China, May 2012.

[90] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 1–18, Oakland, CA, USA, 2000.

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

[92] M. H. Jahanian, F. Amin, and A. H. Jahangir, "Analysis of TESLA protocol in vehicular ad hoc networks using timed colored Petri nets," in *Proceedings of the 6th International Conference on Information and Communication Systems (ICICS-2015)*, pp. 222–227, Amman, Jordan, April 2015.

[93] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2009.

[94] 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 Sensor1*, pp. 11–21, Alexandria, VA, USA, November 2005.

[95] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *Proceedings of the 4th ACM International Work-Shop on Vehicular Ad Hoc Networks*, pp. 19–28, Montreal, Quebec, Canada, September 2007.

[96] A. Wasef and X. Shen, "EMAP: expedite message authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, 2013.

[97] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility," in *Proceedings of the IEEE Intelligent Vehicle Symposium*, pp. 541–546, Istanbul, Turkey, June 2007.

[98] K. Zeng, "Pseudonymous PKI for ubiquitous computing," in *Proceedings of the Europe Public Key Infrastructure Workshop*, pp. 207–222, Turin, Italy, June 2006.

[99] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. S. Shen, "Pseudonym changing at social Spots : an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[100] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V -tokens for conditional Pseudonymity in VANETs," in *Proceeding in IEEE Wireless Communication Networking Conference (WCNC)*, pp. 1–6, Sydney, Australia, April 2010.

[101] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal, "Analysis of certificate revocation list distribution protocols for vehicular networks," in *Proceedings of the IEEE Global Telecommunication Conference (GLOBECOM)*, pp. 1–5, Miami, FL, USA, December 2010.

[102] M. E. Nowatkowski and H. L. Owen, "Scalable certificate revocation list distribution in vehicular ad hoc networks," in *Proceedings of the IEEE GLOBECOM Workshops (GC Wkshps)*, pp. 54–58, Miami, FL, USA, December 2010.

[103] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943–955, 2016.

[104] 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.

[105] I. F. Blake, V. Kumar Murty, and G. Xu, "Refinements of Miller's algorithm for computing the Weil/Tate pairing," *Journal of Algorithms*, vol. 58, no. 2, pp. 134–149, 2006.

[106] A. D. Woodbury, D. V. Bailey, and C. Paar, "Elliptic curve cryptography on smart cards without coprocessors," in *Proceedings of the 4th Smart Card Research and Advanced Applications Conference (CARDIS)*, pp. 20–22, Bristol, UK, September 2000.

[107] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, "Message authentication in vehicular ad hoc networks: ECDSA based approach," in *Proceedings of the International Conference on Future Computer and Communication (ICFCC)*, pp. 16–20, Kuala Lumpur, Malaysia, April 2009.

[108] R. Kalkundri and S. A. Kulkarni, "A secure message authentication scheme for VANET using ECDSA," in *Proceedings of the 4th Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1–6, Tiruchengode, India, July 2013.

[109] A. Smitha, M. P. Manohara Pai, N. Ajam, and J. Mouzna, "An optimized adaptive algorithm for authentication of safety critical messages in VANET," in *Proceedings of the 8th International Conference on Communications and Networking in China (CHINACOM)*, pp. 149–154, Guilin, China, August 2013.

[110] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, vol. 84, pp. 47–53, Springer, Berlin, Germany, 1984.

[111] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of Things environments," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2904–2914, 2018.

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

[113] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.

[114] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Advances in Cryptology-CRYPTO 2001*, pp. 355–367, Springer, Berlin, Germany, 2001.

[115] L. Zhang, Q. Wu, J. Domingo-ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[116] L. Zhang, "OTIBAAGKA: a new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2998–3010, 2017.

[117] 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.

[118] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Asiacrypt*, vol. 2984, pp. 452–473, Springer, Berlin, Germany, 2003.

[119] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signature revisited," in *Information Security, Confidentiality*, pp. 308–322, Springer, Berlin, Germany, 2007.

[120] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 390–394, 2009.

[121] R. H. H. Chun-Ifan and P. H. Ho, "Truly non-repudiation certificateless short signature scheme from bilinear pairings," *Journal of Information Science and Engineering*, vol. 27, pp. 969–982, 2011.

[122] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings," *International Journal of Communication Systems*, vol. 27, no. 7, pp. 1083–1090, 2014.

[123] K.-H. Yeh, K.-Y. Tsai, and C.-Y. Fan, "An efficient certificateless signature scheme without bilinear pairings," *Multimedia Tools and Applications*, vol. 74, no. 16, pp. 6519–6530, 2014.

[124] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.

[125] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Information Sciences*, vol. 451-452, pp. 1–15, 2018.

[126] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

[127] M.-H. Park, G.-P. Gwon, S.-W. Seo, and H.-Y. Jeong, "RSU-based distributed key management (RDKM) for secure vehicular multicast communications," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 644–658, 2011.

[128] Y. Sun, Z. Feng, Q. Hu, and J. Su, "An efficient distributed key management scheme for group-signature based

anonymous authentication in VANET," *Security and Communication Networks*, vol. 5, no. 1, pp. 79–86, 2012.

[129] L. Malina, J. Castellà-Roca, A. Vives-Guasch, and J. Hajny, "Short-term linkable group signatures with categorized batch verification," in *Proceedings of the International Symposium Found Practice Security*, pp. 244–260, QC, Canada, October 2012.

[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] S. K. 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.

[132] N. Elloumi, H. Haj-Salem, and M. Papageorgiou, "Metacor: a macroscopic modeling tool for urban corridors," in *Proceedings of the Triennial Symposium on Transportation Analysis*, pp. 135–150, Capri, Italy, June 1994.

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

[134] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo—simulation of urban mobility: an overview," in *Proceedings of the 3rd International Conference on Advances in System Simulation SIMUL, ThinkMind*, pp. 23–28, Barcelona, Spain, October 2011.

[135] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in NS-2," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems—MSWiM'07*, pp. 159–168, New York, NY, USA, 2007.

[136] G. F. Riley and T. R. Henderson, *The NS-3 Network Simulator, Modeling and Tools for Network Simulation*, Springer, Berlin, Germany, 2010.

[137] T. R. Andel and A. Yasinac, "On the credibility of manet simulations," *Computer*, vol. 39, no. 7, pp. 48–54, 2006.

[138] A. Varga and R. Hornig, "An overview of the OMNET++ simulation environment," in *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*, p. 60, Marseille, France, March 2008.

[139] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO-simulation of urban mobility," *International Journal on Advances in Systems and Measurements*, vol. 5, no. 3-4, pp. 128–138, 2012.

[140] M. Piórkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux, "TraNS," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 12, no. 1, pp. 31–33, 2008.

[141] V. Kumar, L. Lin, D. Krajzewicz et al., "iTETRIS: adaptation of ITS technologies for large scale integrated simulation," in *Proceedings of the 71st IEEE Vehicular Technology Conference, VTC Spring 2010*, pp. 1–5, Taipei, Taiwan, May 2010.

[142] 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.

[143] A. Wegener, M. Piorkowski, M. Raya, H. Hellbrück, S. Fischer, and J. Hubaux, "TraCI: an interface for coupling road traffic and network simulators," in *Proceedings of the 11th communications and networking simulation symposium*, pp. 155–163, Ottawa, ON, Canada, April 2008.

[144] M. Scott, *Multiprecision Integer and Rational Arithmetic Cryptographic Library*, Shamus Software Ltd, Dublin, Ireland, 2015.

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