IEEE Open Journal of Vehicular Technology

Received 30 April 2020; accepted 1 June 2020. Date of publication 4 June 2020;
date of current version 19 June 2020. The review of this article was coordinated by Editor S. Sun.

Digital Object Identifier 10.1109/OJVT.2020.2999885

Recent Advances and Challenges in Security and Privacy for V2X Communications

JIAQI HUANG [1] (Student Member, IEEE), DONGFENG FANG [2] (Member, IEEE), YI QIAN [1] (Fellow, IEEE), AND ROSE QINGYANG HU [3] (Fellow, IEEE)

(Invited Paper)

[1] Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Omaha, NE 68182 USA
[2] Department of Computer Science and Software Engineering, California Polytechnic State University, San Luis Obispo, CA 93407 USA
[3] Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84322 USA

CORRESPONDING AUTHOR: YI QIAN (e-mail: yi.qian@unl.edu)

This work was supported by the National Science Foundation under grants EARS-1547312 and EARS-1547330.

ABSTRACT In recent studies, vehicular networks have been considered as a promising solution to achieve better traffic management and to improve the driving experience of drivers. In vehicular networks, vehicle-to-everything (V2X) services, e.g. on-road traffic information exchange and location-based services, are provided to facilitate road safety for vehicles and traffic management for the relevant authorities. Dedicated Short Range Communications is specifically designed for V2X communications, and recently the cellular network has shown great potential to support V2X with better performance and more applications. Due to the wireless nature of V2X communications, how to secure V2X communications and guarantee the privacy of users are great challenges that have hampered the implementation of vehicular services. Many solutions have been proposed by researchers in last two decades. In this paper, we present a comprehensive survey on the state-of-the-art solutions concerning security and privacy for V2X communications. For security, detailed discussions on cryptography based schemes and trust based schemes are provided. For privacy, we summarize and compare general solutions in preserving identity privacy and location privacy. Cellular based V2X communications have shown many advantages over DSRC, and the oncoming fifth-generation cellular technology is going to provide more possibilities to V2X. Thus, security architectures and solutions for cellular based communications are also illustrated and discussed. Finally, we summarize the remaining challenges and point out future research directions.

INDEX TERMS Security, privacy, trust management, V2X, vehicular networks, LTE, and 5G.

I. INTRODUCTION

Vehicular networks have received great attentions in recent years as a key component of the Intelligent Transportation System (ITS) [1]. In vehicular networks, an on-board unit (OBU) is installed in each vehicle to communicate with other vehicles, road infrastructures, pedestrians, and networks. These vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) and vehicle-to-network communications are collectively known as vehicle-to-everything (V2X) communications. Information about traffic conditions, such as proxy accidents and traffic jams, is included in V2X communication messages so that drivers can know the information on road conditions in advance and take an early action [2]. Moreover, emergency rescue operations can benefit from V2X communications by sending notifications to the vehicles on the road ahead to speed up rescues. Applications of discovering services nearby, such as finding gas stations and restaurants, are also envisioned through V2X communications.

However, the implementation of vehicular networks confronts many challenges especially security and privacy issues [3]. Without a proper authentication protocol, attackers may inject unauthenticated messages to gain personal benefits [4]. For example, an attacker broadcasts fake traffic jam messages to have a less congested road by misleading other vehicles in proxy area to reduce the target road traffic. Due

to the wireless feature of V2X communications, the on-the-air messages are very vulnerable. Thus, security mechanisms should be adopted to secure V2X communications [5].

To handle security issues for V2X communications, a great volume of solutions have been proposed. The majority of them can be classified into cryptography based schemes and trust based schemes. Cryptography based schemes are robust and efficient against outside attackers [6]. Lin *et al.* [7] proposed a group signature based scheme, where in each group, a group head is selected to do the key management and then group members use their identical group secret key and the group public key to communicate with each other. Lu *et al.* [8] proposed to use short time certificates for vehicles to have authenticated communications. Vehicles can get short time certificates from road side units (RSUs) after a mutual authentication process. Although [7] and [8] can secure communications in vehicular networks, both of them are not efficient to verify hundreds of messages within a short time period. Due to the nature of heavy communication overhead and computational cost in cryptography based schemes, some tailored batch verification schemes have been proposed to improve the efficiency of signature verification. Zhang *et al.* [9] first introduced batch verification into vehicular networks by flexibly utilizing properties of bi-linear mapping in message signing and verifying processes. Since messages can be verified in a batched way, the verification time is reduced significantly. Attracted by benefits brought by the batch verification, many protocols have been proposed to improve the efficiency and security level following the idea of [9]. Trust based schemes are more suitable to preclude inside attackers. Raya *et al.* [10] proposed a trust based mechanism to improve the efficiency of detecting junk messages to prevent black hole attack and denial-of-service (DoS) attack.

As for privacy, most of the solutions for V2X communications are using pseudonyms to achieve conditional privacy preservation, where authorities can trace real identities of identified malicious vehicles. However, pseudonyms alone cannot preserve privacy perfectly, where side information, such as users occurring probability related to time and locations, can be utilized to reveal sensitive information of users [11]. Moreover, if a vehicle changes its pseudonyms when sending messages continuously, the similarity among the messages of its speed and direction may reveal useful clues for location or identity tracking. Therefore, privacy preservation remains a big challenge especially the location privacy [11]–[15], which needs to be settled by extra protocols integrated with pseudonyms.

Several survey works have been done concerning about security and privacy issues in V2X communications. In [16], Hartenstein and Laberteaux not only provided a summary of various application requirements and implementation challenges of vehicular networks, but also pointed out future research directions for security and privacy issues in vehicular networks. In [17], the authors summarized the security and privacy problems in vehicular networks. However, they mainly discussed the identity privacy of users, where the location privacy is barely studied. Azees *et al.* [18] provided a security survey, which introduced some security protocols by discussing their contributions on different security services. Anita *et al.* [19] presented several authentication schemes and provided comparisons of these schemes based on their advantages and disadvantages. However, only a few papers were studied in [19]. Petit *et al.* [20] thoroughly explored pseudonyms based schemes from aspects of the life-cycle of pseudonyms. The authors divided all the surveyed protocols into four categories which are public key infrastructure (PKI), identity-based cryptography, group signature, and symmetric authentication. Pros and cons of surveyed protocols are elaborated in that paper. Alnasser *et al.* [21] presented a survey discussing the design challenges of security model for V2X communications as well as security threats of V2X enabling technologies. Discussions and comparisons are made on a moderate number of security solutions. Recently, Lu *et al.* [22] summarized trust, security and privacy vulnerabilities in 5G based V2X services. In [22], security strategies that address those vulnerabilities are elaborated and categorized based on the layers these strategies are applied to. Different from the existing surveys that either study authentication schemes, or privacy-preserving mechanisms, or security issues in 5G based vehicular networks, this paper covers most of the security topics in vehicular networks to provide a comprehensive overview of footprint and state-of-the-art solutions in securing V2X communications.

The major contributions of this survey can be generalized as follows. A comprehensive survey of stage-of-the-art solutions for both security and privacy in vehicular networks are presented. For security concerns, both the cryptography based schemes and trust based schemes are analyzed. Moreover, we further categorize cryptography based schemes into non-batch verification schemes and batch verification schemes, where advantages and limitations of batch verification schemes are summarized. Besides the security concern, privacy preserving methods are analyzed, where identity privacy preserving schemes and location privacy preserving schemes are elaborated in details. Considering the cellular based V2X communications are winning more attention from both industry and academy, we illustrate and analyze the security architectures and recent advances of Long Term Evolution (LTE) based V2X communications and the fifth-generation (5G) based V2X communications. At the end of discussion, we present remaining challenges and future research directions in securing V2X communications. The outline of security and privacy solutions discussed in this survey is shown in Fig. 1.

The rest of this paper is organized as follows. Section II introduces system architecture, attacks, security services, and basic solutions for vehicular networks. Section III introduces cryptography based schemes. Section IV discusses trust based schemes. Section V shows privacy solutions for both identity privacy preservation and location privacy preserving. The current status of LTE-V2X and 5G-V2X and some most recent solutions are given in Section VI. Section VII discusses

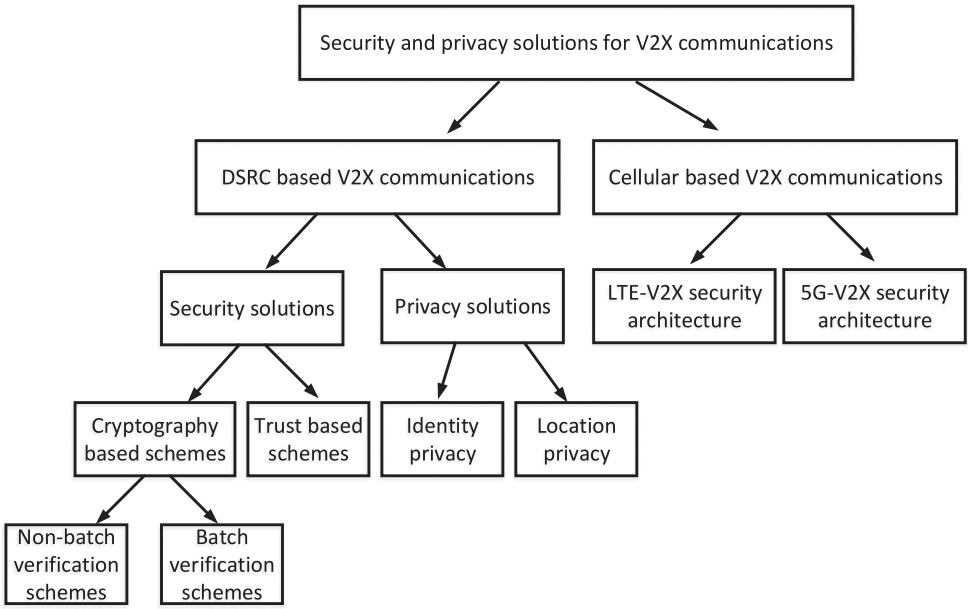


FIGURE 1. **Outline of security and privacy solutions for V2X communications.**

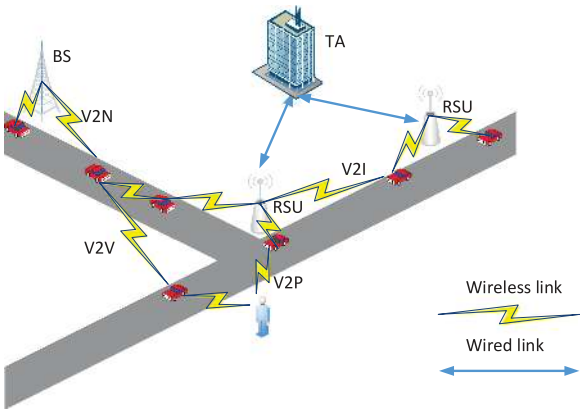


FIGURE 2. **A generic architecture of vehicular networks.**

challenges and future research directions for V2X communications. Section VIII concludes this paper.

II. SYSTEM ARCHITECTURE, ATTACKS, SECURITY SERVICES, AND BASIC SOLUTIONS IN VEHICULAR NETWORKS

In this section, first, we introduce a generic system architecture of vehicular networks. Then, we illustrate various attacks and security services in vehicular networks. In the end, we summarize general solutions to counter the various attacks.

A. GENERIC SYSTEM ARCHITECTURE OF VEHICULAR NETWORKS

As depicted in Fig. 2, a trust authority (TA), RSUs, Base Stations (BSs), and OBUs are major entities in vehicular networks [23]. OBUs can communicate with other OBUs and roadside infrastructures within communication range through wireless accesses. Both BS and RSU are access points (APs) of the network, receiving orders from the TA and collecting messages from OBUs [24]. All roadside infrastructures are connected to the TA through wired access. Detailed definitions of the these entities are shown as follows.

TA: The TA is a trust administration that manages the registration process of all vehicles and APs [25]. Certificates of OBUs and APs are usually issued by the TA after registration. The TA is responsible to preserve all the information of legitimate users, e.g. real ID and location of APs, real ID and reputation scores of OBUs, which will be used to reveal the real identities and locations of the malicious users. In most cases, the TA is fully trusted with unlimited storage and strong computation capability.

APs: APs include BS and RSU deployed on roadside. They are responsible to manage communications between vehicles within their coverage area and to deliver messages sent from vehicles to the TA through wired networks. Road side infrastructures are considered to have less computation capability and more vulnerable to attackers compared to the TA.

OBUs: An OBU is a communication device installed in vehicle with certain computation and storage capacity. Usually, a tamper-proofed device (TPD) is equipped with OBU to support secure communications between OBUs and roadside infrastructure through wireless access. Credential information is stored in each TPD. In general, OBUs are considered to have limited computation and storage capability.

The TA is the most powerful administrator in the vehicular network system. Each vehicle should register at the TA with its identity information to join the network. If a vehicle is found behaving suspiciously, a report should be generated and delivered to a nearby AP. The report will be further forwarded

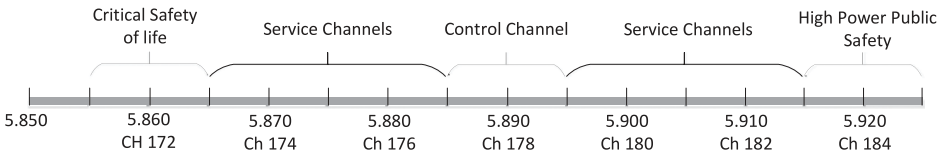


FIGURE 3. DSRC spectrum defined in U.S.

to the TA. Then the TA can verify this report and take proper actions if the report is valid, e.g. revoke the suspicious vehicle. The revocation scheme in IEEE 1609.2 standard relies on a certificate revocation list (CRL). Once the TA decides to revoke a vehicle, it will add the identity of the vehicle into the CRL and send an update request to APs. APs accept this update and broadcast the updated CRL. OBUs within communication range receive the message and update their CRLs. APs and OBUs will discard the message in which the attached certificate is in the latest CRLs. Although in different schemes, capabilities and functions of APs are defined differently, the primary goal of them is to relay messages in vehicular networks. Due to the fact that APs are usually exposed in public environment, they are more likely to be corrupted.

In general, V2X communications are considered to use either DSRC [26] [27] or mobile cellular communication networks. DSRC based V2X communications utilize the assigned 75 MHz DSRC spectrum allocated at 5.9 GHz frequency band. The detailed spectrum allocation is shown in Fig. 3. Service channels (channel 174, 176, 180, and 182) can be used for both non-safety and safety messages. The control channel (channel 178) can be used to broadcast safety-related applications for vehicle safety traffic at all power levels. Channel 184 is allocated for public safety communications and channel 172 is designed for highly reliable and very low latency communications [18]. The DSRC based V2X communications have a low end-to-end delay but low capacity. Cellular technologies like LTE and 5G can provide a larger communication range, lower deployment cost and better QoS guarantee compared to DSRC [28]. The 3GPP is working on the standardization to support the LTE-based V2X communications. Except for DSRC and cellular communication technologies, some other wireless communication technologies like Bluetooth and satellite radio are also considered for some V2X applications. In vehicular networks, OBUs are required to send basic security related messages every 300 ms, which plays a vital role in safety related applications [29]. The sender's real-time position, speed and steering information can be obtained from security related messages, which can be utilized to optimize routes for nearby vehicles based on aggregated traffic information. Most of the safety related messages transmitted in vehicular networks should be authenticated.

B. ATTACKS AND SECURITY SERVICES IN VEHICULAR NETWORKS

1) ATTACKS

Existing various attacks significantly impede the application of vehicular networks. Since messages are transmitted through a wireless link, vehicular networks are vulnerable to many attacks. In this subsection, several common attacks in vehicular networks are briefly discussed as follows.

1) **Bogus messages:** Bogus messages stand for fake or junk messages generated and distributed by attackers. An attacker can be an outsider or an authenticated insider. The attacker can broadcast bogus messages to misguide other drivers' decisions to get benefits. For example, the attacker sends a fake traffic jam alarm to make other drivers choose alternative routes so that few vehicles would be left on his way [17].
2) **Message modification:** Message modification is defined as modifying the original message through deleting, adding to, changing, or reorganizing. Attackers can modify the messages exchanged in the air to mislead drivers or achieve other malicious goals.
3) **Sybil attack:** Sybil attack is defined that attackers join a system using multiple real/fake identities. This attack is hard to detect. Attackers can send multiple messages with different identities to misguide other vehicles without being identified. Even a spoofed identity has been identified, the attacker may get away without being punished [30].
4) **DoS:** DoS happens when attackers inject a great volume of messages into the network aggressively to make network resource unavailable to legitimated users. This attack can be launched in a distributed way to form the distributed DoS attack, which can severely jeopardize the availability of vehicular networks. Note that this attack can be triggered by both inside and outside attackers [31].
5) **Eavesdropping:** This attack occurs when attacker collecting all possible information from the network. Different from the previous mentioned attacks, eavesdropping is a passive attack, and it has no effects to the network directly. However, it violates the confidentiality and location privacy of users [32].
6) **Impersonate attack:** This attack occurs when an attacker sending messages on behalf of other vehicles from whom it successfully filches those identities. Usually, the attacker has to hack legitimate vehicles first. Once succeed, attackers not only do harm to the network but also shift punishments to hacked vehicles.
7) **Replay attack:** Replay attack occurs when attackers maliciously or fraudulently transmitting repeated data. This attack in vehicular networks can make other legitimate vehicles have a wrong estimation of the current traffic condition. Moreover, it can induce the DoS attack.

8) **Black hole attack:** Black hole attack is named by its attributes. Attackers drop all the packets like a black hole instead of forwarding them. This attack can cause great data loss and it is hard to be detected.
9) **Grey hole attack:** This attack is similar to black hole attack, instead it drops packets selectively. The selective dropping behavior making this attack more difficult to detect and prevent than the black hole attack.
10) **Location tracking:** This attack occurs when attackers tracking legitimate vehicles location through keeping monitoring and analyzing messages sent by targets. This attack can be done even when targets keep changing their pseudonyms [33].

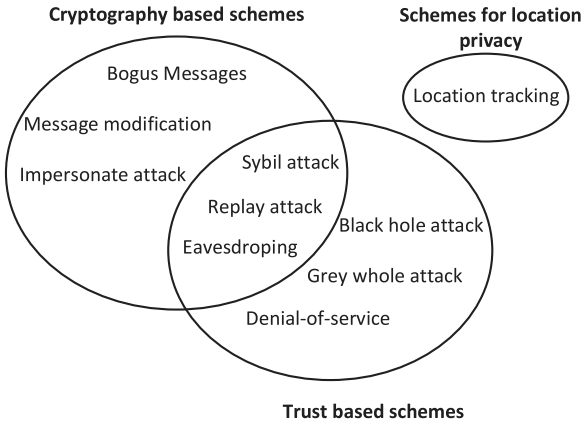


FIGURE 4. Attacks and solutions.

2) SECURITY SERVICES

Due to the increasing number of attacks in vehicular networks, security and privacy services are required to provide a reliable environment for vehicular networks [34], [35]. Qu *et al.* summarized primary security services in vehicular networks from aspects of the authenticated information source, the confidentiality of users and scalability of the service [17]. Karagiannis *et al.* categorized security requirements of vehicular networks in detail at the application level [36]. Referring to the previous research work in vehicular networks and the problems encountered in vehicular communication cases, we summarize the security services and requirements of vehicular networks as follows.

1) **Authentication:** Authentication requires that messages should be authenticated before further actions. It forms the first defense line against various attacks. Modified messages, fake and illegitimate signatures, and time-out requests are excluded directly [37].
2) **Integrity:** Integrity requires that the messages received by vehicles or APs should be authenticated and cannot be modified in any situation. Any forged or modified message from malicious nodes should be detected and removed from vehicular networks.
3) **Non-repudiation:** Non-repudiation requires that for any message, the TA can trace the real identity of the message sender with clear location and time records. Any identity cannot successfully impersonate others to send messages. If this is not guaranteed, then malicious users can cause dangerous consequence without being punished.
4) **Availability:** Availability is the fatal service and requirement in vehicular networks. It requires that in any situation, vehicular networks should guarantee access to vehicular services for all entities in the network. It also requires that the authentication methods implemented in vehicular networks to be highly efficient.
5) **Anonymity:** Anonymity requires that legitimate users' real identities are protected and cannot be revealed by others except the TA. Generally, pseudonyms are employed to achieve this requirement.
6) **Unlinkability:** This service has two levels. The first level is that no clear relation can be found between a real identity and its corresponding pseudonyms. The second level requires that there is no clear clue among all pseudonyms used by one vehicle so that attackers cannot link pseudonyms from multiple messages to trace a particular vehicle.
7) **Conditional Traceability:** Conditional traceability requires that legitimate users' real identities be protected and not be revealed while the malicious users' real identity can be easily traced and revealed by the TA.
8) **Efficient Revocation:** Since every vehicle may need to handle hundreds of messages within a short time, efficient revocation requires that the revocation scheme should be scalable and efficient to meet the stringent requirement of vehicular networks.
9) **Location Privacy Preservation:** Location privacy is also an important factor needs to be preserved as identity privacy. It must be preserved to protect the interests of legitimate users from attackers tracking their locations [38]. However, this requirement cannot be achieved only by authentication schemes with pseudonyms. Some other mechanisms should be applied to protect the location privacy. For example, the mixed-zones and the caching methods are proposed to provide location privacy. Detailed discussions will be provided in Section VI.

C. BASIC SOLUTIONS

A secure vehicular network should be resistant to various attacks. Many common attacks in mobile ad hoc networks like DoS, eavesdropping and impersonate can also be triggered in vehicular networks. A proper protocol that meets all security services and requirements is desirable. However, all of the current solutions have somewhat limitations and drawbacks.

As showed in Fig. 4, bogus messages, message modification and impersonate attack can be solved mainly by cryptography based schemes since cryptography is the only way to provide authentication [6]. Cryptography based schemes prevent Sybil attacks by checking the validity of the pseudo ID attached in the message, which could be a certificate, a pseudonym or the sender's public key. The legitimate user

only has one valid pseudo ID at a time and faked pseudo ID cannot pass the authentication process so that the Sybil attack could be largely resolved. To deal with the replay attack, cryptography based schemes attach a timestamp to mark every message, thus the replayed one will be neglected by receivers. Up to now, how to efficiently protect security and privacy remains a big challenge, although numerous protocols have been proposed in the past two decades. In general, these schemes can be categorized into group signature based schemes, identity based schemes and hybrid schemes. In group signature based schemes, each group member can sign the message on behalf of the group and the signature can be verified using the shared group public key. This kind of scheme can provide privacy for the message signer within the group. However, the group management is an issue since the vehicular network has highly unstable topology. Another potential problem is that the group head or manager may have too much power to reveal the identity of any group member. In identity based scheme, the vehicle's public key is related to the vehicle's identifier and the private key is generated using the identifier. In this way, no certificate is needed to verify the public key, thus the certificate management issue is eliminated compared to the PKI based scheme. However, the identity based algorithms are usually computation-intensive, leading to large verification delay. Hybrid schemes try to combine advantages of group based schemes and identity based schemes and avoid their shortcomings. A more detailed discussion about cryptography based schemes are introduced in Section III.

Most trust based schemes are incorporated with cryptography methods, e.g. public key infrastructure and certificates, to authenticate each vehicle's reputation score. Since cryptography methods are used to authenticate the reputation score instead of messages, most trust based schemes cannot prevent message modification and repudiation. But for Sybil attack, attackers do not have valid reputation scores for their virtual Sybil, so those messages sent by virtual identities will not be accepted. Trust based schemes are capable of preventing black hole attacks, grey hole attacks and DoS by constructing a supervision system. In trust based schemes, the reputation score is slowly incremented but easy to lose [39]. Once a vehicle is found dropping messages or injecting a massive number of massages, its reputation score drops quickly. If vehicle's reputation score is under a threshold, it will be excluded from the network. Since trust based schemes are using historical interactions among peers to judge the trustworthiness of a vehicle or a message at current time, they are vulnerable to some attacks like on-off attack and platooning attack. In the on-off attack, the attacker act "smartly" to do malicious activities while maintaining its reputation score above the detection threshold. In the platooning attack, a platoon of attackers collaborate together to keep generating positive feedback for each other. In such a way, their reputation scores are always high, and they can use their high reputation score to launch attacks without being detected. Thus, for trust based schemes, how to efficiently identify and eliminate these "intelligent malicious behavior" are in great concern. A more detailed discussion about trust based mechanisms are provided in Section IV.

As for the privacy concern, an attacker may track a specific vehicle by tracking the safety related messages, which are shown in plaintext and contain the vehicle's speed, direction and location. Even if the vehicle frequently changes its pseudonyms, attackers can relate the new pseudonym to the old one by analyzing the similarities among the safety related messages. Thus, some schemes are proposed to prevent location leakage by obscuring the pseudonym changing process to attackers, e.g. vehicles change their pseudonyms simultaneously when the safety related messages are indistinguishable among a set of vehicles. However, this kind of mechanism require the number of vehicles gathered together exceeds a threshold to be effective, which is not suitable for suburban areas. There are also some other methods to preserve location privacy, e.g. k-anonymity, cloak region, and dummy locations. These kinds of methods protect user's location privacy by sacrificing the accuracy of location information. So, there is always a tradeoff between the privacy level and QoS. A more detailed discussion of privacy preserving are shown in Section V.

III. CRYPTOGRAPHY BASED SCHEMES

In this section, we demonstrate the cryptography based security solutions for vehicular communications. Most of these schemes can provide promising security services, however, large communication overhead and computation time are unavoidable [40]. Zhang *et al.* [9] proposed an identity based scheme, which utilized a batch verification algorithm to improve the efficiency of doing multiple authentication processes. Attracted by high efficiency of batch verification, a bunch of batch verification schemes are proposed in recent years. Batch verification schemes and non-batch verification schemes are very different in the processes of pseudo identity generation, message signing and verification. To our best knowledge, there is no survey that has discussed batch verification schemes in details. Thus, in this paper we categorize cryptography based schemes into non-batch verification schemes and batch verification schemes. Detailed comparisons and analyses are given in the following context.

A. NON-BATCH VERIFICATION SCHEMES

Without losing the generality, we categorize the non-batch verification schemes into group signature based schemes, identity based schemes, and hybrid schemes.

1) GROUP SIGNATURE BASED SCHEMES

Chuam *et al.* proposed the "Group Signature" in 1991, which enables every group member to sign messages on behalf of the group anonymously [41]. In group signature based schemes, as shown in Fig. 5, a group of vehicles sign messages anonymously with their group private keys, and then the signed messages can be verified by any group member with the group

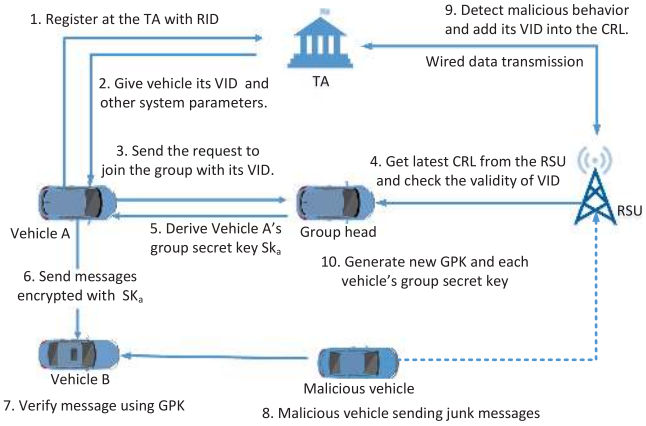


FIGURE 5. A general architecture of group signature based schemes.

public key. The elliptic curve digital signature algorithm [42] is usually utilized to sign messages with lower communication overhead, and it is adopted by Wireless Access in Vehicular Environment standard [43]. At the initial stage of the whole process, a vehicle is required to register at the TA with its real ID (RID) to get system parameters and a valid vehicle ID (VID). With the valid VID, a vehicle can send a request to the group head to join the group. The group head checks whether the latest CRL contains the requester's VID, which is updated through RSUs. With the negative checking result, the group head derive a private key for the requester and secretly sent it back. If a vehicle in the group is identified as malicious vehicle, then the group head will report its VID to the TA meanwhile generating a new group public key and new group secret keys pairs for unrevoked vehicles.

Guo *et al.* proposed a communication framework for vehicular networks based on group signature, which can achieve authentication, data integrity, anonymity, accountability and traceability [44]. However, the key distribution issue is not discussed. Lin *et al.* proposed a scheme that each vehicle only has to cache one group key and one private key [7]. The anonymous message authentication and conditional traceability are achieved by implementing the group signature. However, a checking process of CRL for every message is required. Furthermore, the CRL grows exponentially as the number of revoked vehicles increases which may introduce great delay for message verification. As a result, the heavy burden of communication overheads make the proposed scheme not suitable in practice.

Lu *et al.* first developed an efficient conditional privacy preserving protocol (ECPP) to support vehicles to receive their short time pseudonymous certificates from RSUs [8]. ECPP minimizes the storage used for anonymous keys without losing the security level. In ECPP, each RSU uses its private key and the system public key to make a short time certificate for the authenticated vehicles nearby. Each vehicles uses this short time certificate to communicate with others within a certain period of time. In this way, there is no need to check the revocation list. However, this scheme relies too much on RSUs, which are vulnerable to attackers. The scalability issue, which affects the performance in practice, is not studied.

To reduce the communication overhead and solve the key distribution problem, Hao *et al.* enhanced the distributed key management framework with a novel collaborative message authentication protocol [45]. It eliminates the number of parameters need to be verified of a single message. But the authentication process is still not efficient enough. Thus, Lin *et al.* proposed a secure cooperative message authentication to reduce the authentication overhead and computation cost [46]. The cooperative vehicles are chosen based on geographical information with the help of an evidence token. The evidence token indicates cooperative authentication effort. Furthermore, the evidence token approach can be utilized to resist the free-riding attacks. Although the proposed scheme has been verified through intensive simulations, a large number of RSUs are needed to achieve the performance, which dramatically increased the cost of basic construction. Considering that the CRL checking process in OBU brings a large delay, Shao *et al.* proposed a new group signature protocol aiming at reducing the delay [47]. In the proposed group signature protocol, a new entity named Tracing Manager is introduced to trace malicious vehicles and provide updated CRL to RSUs. The RSU's certificate is provided by the TA and the OBU's certificate is managed by a Tracing Manager. If an OBU is in the revocation list, the RSUs will not provide the group certificate to the OBU so that the OBU will be excluded from group. By transferring the revocation work to the Tracing Manager, the burden of both TA and OBUs are released. To achieve efficient traceability and message unlinkability, the signature is made as a large communication overhead with 826 bytes, which increases the authentication processing time. Even though batch authentication is available in the proposed scheme, it still needs 52 seconds to check 100 signatures. The harsh requirements in vehicular networks are not satisfied.

Different mathematical principles were applied to optimize the authentication schemes making them more suitable for vehicular networks. In [48], the authors proposed a dual authentication scheme based on Chinese Remainder Theory (CRT) [49]–[52]. In [52], the computation complexity of generating new keys at user side is minimized. However the computation processes in the server becomes a great burden. To solve this problem, the scheme proposed in [48] divides users into two categories, named Primary Users (PU) and Secondary Users (SU). The PU can communicate with the TA directly while the SU has no direct interactions with the TA. Since the average group size is reduced, the computation complexity and time consumption at server side are reduced. The dual authentication procedure can also help to protect the system from masquerade and Sybil attacks. The main idea of the dual authentication is that before a vehicle gets the authentication code for receiving information from the TA, and exchanging information among peers, the TA needs to validate the vehicle's Hash code and the vehicle needs to

TABLE 1. Comparison of Group Signature Based Schemes

Paper	Integrity	Non-repudiation	Unlinkability	Anonymity	Traceability	Efficient Revocatoin	Low delay	Formal security proof
[7]	✓	✓	✓	✓	✓			✓
[44]	✓	✓	✓	✓			✓	
[45]	✓	✓		✓	✓			
[46]	✓	✓	✓	✓	✓			
[47]	✓	✓	✓	✓	✓	✓		✓
[48]	✓	✓	✓	✓		✓	✓	
[53]	✓	✓	✓	✓		✓		

verify the fingerprint of the driver. Considering that the group key update and setup process in [48] only needs one broadcast message and one single calculation, the CRT based scheme is very suitable for vehicular networks and worth further study. Besides CRT, probabilistic is also utilized to optimize the authentication schemes. Wasef [53] significantly reduces the computation time for authentication and revocation process with a novel expedite message authentication protocol. Besides the probabilistic key distribution employed in [53], a keyed hash authentication method is introduced to replace the time consuming revocation process based on CRL so as to improve revocation efficiency. In the proposed protocol, the group key is chosen by the TA which is not included in any revoked vehicles key pool but processed by most of the legitimate vehicles. For other legitimate vehicles who do not have the group key in their key pools, they can send a request to nearby vehicles and get the key from them. The simulation results show that the key update process can be done within 1 second and the overhead for communications between vehicles is 201 bytes. However, the performance of this scheme was only studied when the TA has a small key pool, while the key pool could be very large in reality.

A general comparison of group signature based schemes are shown in Table 1. From this table, we can see that all these group signature based schemes can achieve message integrity, non-repudiation, and anonymity for V2X communications. However, only a few of them can achieve efficient revocation. Moreover, most of these schemes are using bilinear pairing, which is a complicated crypto operation and has large verification delay. Thus, a group signature scheme with low computation overhead and efficient revocation mechanism remains an open topic.

2) IDENTITY BASED SCHEMES

Different from the group signature based schemes, identity based schemes require every vehicle posses an identifier (pseudonym) and the corresponding secret key. The "identity-based encryption" [54] and "short signature" [55] provide theoretical bases for the identity based authentication schemes in vehicular networks. As showed in Fig. 6, the TA pre-install system's key parameters to vehicle's TPD after vehicle registered with its real identity. Vehicle's secret keys are related with its identifier, both of which are derived from system's key parameters. Vehicle uses its secret key to sign messages and attaches the corresponding pseudonym to the message. Legitimate users can verify the received

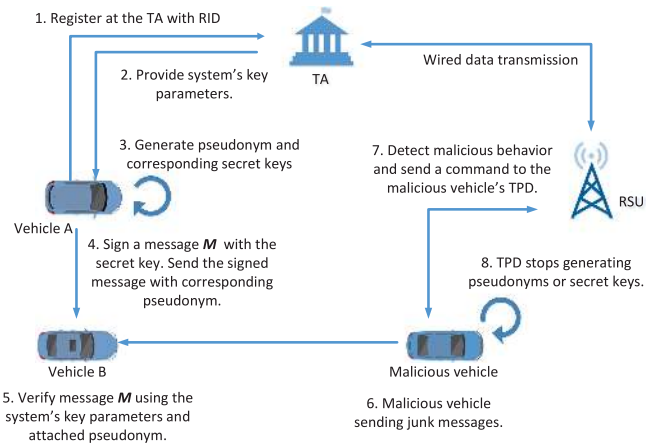


FIGURE 6. A general architecture of identity based schemes.

message using pre-installed system's key parameter and the pseudonym attached to the message. In this way, RSUs are not necessarily needed in V2X communications, which reduces the communication overhead.

In [56], the authors provided secure and privacy-preserving communications in vehicular networks using a PKI based authentication scheme. Every vehicle is pre-installed with massive certified public and private key pairs. When sending a message, the sender signs the message with its private key and attaches the corresponding certificate. Then the receiver will decide to accept this message or not by checking the CRL to verify whether the certificate is valid or not. Since the CRL can be extremely long due to the unpredictable scale of vehicular networks, the CRL checking process brings great delay and makes the authentication inefficient.

Wasef *et al.* proposed a distributed-certificate-service (DCS) scheme with flexible interoperability between different administrative authorities, in which OBUs can update their certificates efficiently [57]. The proposed DCS scheme employs a hierarchical architecture where a Master Authority (MA), a Certificate Authority, RSUs, OBUs are ranked in descending order. The MA is the root of the system, and other units will get their public/private key pairs and certificates from the higher layer. The OBUs can get certificates from RSUs settled in all the regions directly. The proposed protocol supports batch verification to reduce the verification time if many certificates need to be verified within a constrained time slot.

Sun *et al.* pointed out that the capability of DCS largely relies on the distribution condition of RSUs [58]. If RSUs

are poorly distributed, the certificate updating overhead will be inefficient and the revocation cost will be high. The CRL list grows exponentially as the number of revoked vehicles increases, which degrades the authentication performance. Therefore, the authors proposed a new authentication scheme with strong privacy preservation. The proposed scheme guarantees the privacy of the vehicles even all the RSUs are compromised. It also enables the CRL to grow linearly as the number of revoked vehicles increases, which significantly relieves the revocation burden. Although the authentication overhead of [58] is larger than some other schemes (BP, ECPP, DCS, Hybrid), the overall performance is much better when comparing the authentication cost and revocation cost. However, the location privacy is not well considered.

Huang *et al.* claimed that most of the previous schemes using authority units to generate pseudonyms for vehicles are not truly anonymous [59]. Therefore, the authors proposed a protocol which makes the pseudonym generating process to be operated by vehicle itself. In [59], the function of RSU is to provide the credential and define constrains for vehicles. The self-generated short-time lived pseudonymous also can be traced back to reveal the real identity by authorities if needed.

To further improve the computation efficiency for both V2V and V2I communications, Guo *et al.* proposed a light weight privacy-preserving protocol [60]. The proposed protocol is based on a chameleon signature [61], where the signature is generated without the interaction with receivers. By using the ECC-based chameleon hash signature, many desired properties for vehicular networks, for example, anonymous, mutual authentication, conditional privacy preservation, unlinkability and high efficiency are achieved. This paper provides us a novel research direction for securing communications in vehicular networks. However, the time-consuming CRL checking process still limits the overall authentication performance.

To reduce the delay in authentication and to avoid the exponential growth of the CRL, Rajput *et al.* proposed to divide pseudonyms into two hierarchies for V2V and V2I communications with the help of a Revocation Authority and a Law Enforcement Agency [62]. The primary pseudonyms are provided by TA and used for vehicles to be authenticated by RSUs. Each RSU generates secondary pseudonyms with its signature for authenticated vehicles. Vehicles broadcast messages with its secondary pseudonym and receivers verify messages by checking RSU's signature in the sender's second pseudonym. By using a long time primary pseudonym and a short time secondary pseudonym, the proposed scheme gets rid of the heavy burden of CRLs. Moreover, by introducing the Revocation Authority and the Law Enforcement Agency into vehicular networks, less trust is needed on the TA and RSUs in case of the information disclosure due to compromised entities.

Having the same incentive with [62], Wang *et al.* proposed another protocol for vehicular networks named two-factor lightweight privacy-preserving authentication scheme [63]. In order to reduce the workload of TA, this protocol decentralizes TA's function to a local security center. The two-factor authentication requires the driver's biological password and an USB device to pass the verification process in a TPD. After the authentication, vehicles can use the TPD to communicate with others. The TPD is responsible for the revocation process in this protocol. If the TPD receives a revocation command from the TA, it will stop working so that the vehicle cannot send messages anymore. Instead of checking the CRL, the message verification is processed directly by checking a light weight hash code. The communication efficiency is around hundred times better than some previous protocols. However, the outstanding performance of this protocol is built based on a powerful TPD which is not always valid in real cases.

Comparisons of discussed identity based schemes are summarized in Table 2. From Table 2 we can see that all of the introduced identity based schemes can achieve message integrity, anonymity, and traceability. And most of these schemes have new vehicle revocation mechanisms instead of using CRL, which reduces the verification overhead. However, most of these schemes require the involvement of RSU or TA to generate a valid pseudonym. Thus, these schemes require the pervasive distribution of RSUs. Among these schemes, [63] satisfies most security requirements for vehicular networks and is highly efficient. However, it heavily relies on the ideal TPD, so the feasibility of this scheme needs to be further verified. Though there is a large number of solutions to provide secure communications in vehicular networks, the main contradiction between high security level and high authentication efficiency is still not well solved. Compared to group signature based schemes, identity based schemes tend to be more efficient in large scale vehicular networks.

3) HYBRID SCHEMES

Group signature based schemes and identity based schemes possess different advantages and disadvantages. Some hybrid schemes trying to inherit the good properties of both two kinds of schemes while eliminating the shortcomings of them [64].

Rajput *et al.* [64] proposed a hybrid scheme reducing the large computational overhead by avoiding the group management and CRL checking process at the vehicle side. In the proposed scheme, each vehicle receives one long term certificate and a large number of one-time pseudonyms from the TA to support long term vehicular communications. All identifiers of a vehicle, i.e. its real identity and all pseudonyms, are stored in the TA to track vehicles. Every pseudonym is signed by the TA and can only be used once at a specific time due to the unique timestamp contained in the pseudonym. When a vehicle enters a region, which is divided by geographical map, a public/private key pairs of this region are sent to the vehicle if its long term certificate is not in CRL list. Messages sent by vehicles are concatenated with pseudonyms and can be encrypted/decrypted by region's key pair. The message verification is done by validation the TA's signature in the concatenated pseudonym using TA's public key. Thus, the computation overhead at the vehicle side is only a signature verification. All the workloads are left at TA.

TABLE 2. Comparison of Identity Based Schemes

Paper	Integrity	Non-repudiation	Unlinkability	Anonymity	Traceability	Efficient revocation	Low delay	Self-generated Pseudonym
[57]	✓	✓	✓	✓	✓			
[58]	✓	✓	✓	✓	✓			
[59]	✓			✓	✓	✓		
[60]	✓	✓	✓	✓	✓	✓	✓	✓
[62]	✓	✓		✓	✓	✓	✓	
[63]	✓	✓	✓	✓	✓	✓	✓	✓

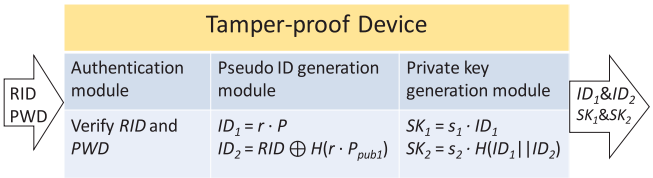


FIGURE 7. Operations in the TPD [9].

B. BATCH VERIFICATION SCHEMES

Batch verification is a method that can verify multiple signatures from various users in a batched way. Thus, batch verification schemes can reduce verification time significantly when the number of signatures need to be verified is large. Since each vehicle in vehicular networks may need to handle hundreds of messages within 300 ms in real cases, batch verification schemes are promising solutions for vehicular networks.

The identity-based batch verification (IBV) was first introduced into vehicular networks by Zhang *et al.* for V2I communications [9]. The bi-linear map is utilized in the proposed IBV protocol. In the proposed scheme, every vehicle is equipped with a TPD. Vehicle's pseudo IDs, which are used as pseudonyms, are generated by the TPD. As shown in Fig. 7, there are three modules in the TPD. First is the authentication module, where the TPD authenticates the vehicle by checking the RID and the password (PWD). The RID and PWD are predefined in the TPD and used to prevent malicious vehicles get advantages over the TPD. If the authentication result is positive, then the TPD self-generates its pseudo IDs and private keys step by step. Both the pseudo ID and private key are consisting of two parts denoted as ID_1, ID_2 and SK_1, SK_2, respectively. The r is a random number and the P is the generator of the cyclic additive group. The $H()$ is the MapToPoint hash function [65]. s_1 and s_2 are the TA's two secret keys, and the P_{pub1} is one of the TA's public key, which is generated by $P_{pub1} = s_1 P$. At last, TPD generates the pseudo $ID = (ID_1, ID_2)$ and $SK = (SK_1, SK_2)$. From the generating process, we can see that secret keys of a vehicle are generated by its pseudo IDs with the TA's secret keys. When a vehicle sending a message, it signs the message with the SKs and attaches the pseudo IDs. Once an RSU receives the message, it can use the attached pseudo IDs and the public key of the system to verify the signature. Due to the properties of additive cyclic group and bi-linear map, all signatures can be simply added and verified by the added IDs and SKs. In this way, all messages can be verified through one bi-linear paring operation, but with some additive operations. If all of the signatures, pseudo IDs and messages are correct, the batch verification will success. However, if any false signature (invalid) occurs, the verification will fail causing the inefficiency of the batch verification.

To solve the inefficiency of the batch verification caused by false signatures, Zhang *et al.* proposed to use a group testing technique to filter false signatures, thus improving the efficiency of the verification process [66]. Four group testing algorithms are compared and evaluated. For the best verification performance, a generalized binary splitting algorithm is chosen to find false signatures. And the total computation cost with signature checking process is negligible when the percentage of false signatures is low.

To address the replay attacks and the scalability of IBV, Huang *et al.* proposed an anonymous batch authentication scheme with key management [67]. In [67], not only batch authentication is achieved, but also the generalization of session keys between the RSU and vehicles can be done in a batched way. All the verification computations only evolve with multiplication based on ECC without bilinear pairing making the computation process very efficient. However, the authors haven't considered the revocation process in detail and relied heavily on the TPD. Thus, the proposed scheme may not be practical.

Lee and Lai proved that the IBV scheme is vulnerable to replay attack and the non-repudiation service can be compromised [68]. To solve these two issues, the authors modified the IBV scheme to improve both the security and efficiency. By adding a timestamp into vehicles' private key generation process, a replay attack can be detected. By distributing a random small number to every message in the batch verification process, the non-repudiation problem can be solved. The MapToPoint function is replaced by a common hash function to reduce the computation cost. The total verification time can be approximated as a constant value no matter the number of messages.

Later, Zhang *et al.* proved that protocol proposed in [68] cannot resist replay attack, or satisfy the non-repudiation requirement [69]. Moreover, the security problem is even worse that anyone can send malicious messages and pass the batch verification without being traced by the TA. In IBV scheme, the signature of a message is created by using two secret keys. These two keys are derived by the TPD using the TA's private key and vehicle's real ID. The TA's private key stored in TPD is confidential to anyone including the vehicle itself so that the

vehicle cannot generate its secrete keys by itself. The problem of [68] is that both of these two keys can be generated with the TA's public key, where the attacker can generate two secret keys and a valid signature using any real ID without being traced. To fix this problem, Zhang *et al.* added an additive value into the second secret key in the proposed scheme. Then the attacker cannot generate the second secret key to create a valid signature. The scheme in [69] has similar performance comparing to Lee's scheme in terms of verification efficiency.

Following the main idea of [67] and [68], Tzeng *et al.* [70] proposed an improved IBV scheme recently. The authors in [70] proved that [68] exists some security risks. In [68], any vehicle who has public parameters can reveal sender's real identity with the signature attached to the message. Different from the previous IBV schemes where two parts of the vehicle's secret keys are derived from two parts of the pseudo identities respectively, the proposed scheme integrates those two parts of secret keys as a whole. If two parts of secret signing keys are generated and used separately, an attacker can derive the second part of the secret key first, and then use the signature and the second part of the secret key to derive the first part of the secret key. After knowing these keys, the attacker can get the real identity of the message sender. Therefore, by combining the two parts of secret keys together, the attacker cannot get the secret information step by step. High verification efficiency is also achieved by the proposed scheme. Only a constant short time period is required to verify batch of the messages.

In order to improve the efficiency of IBV scheme, Shim proposed a batch verification scheme only using common hash function instead of the MapToPoint function [73]. The proposed protocol has less reliance on TPD which is more practical. According to the simulation results, this protocol is 18 percent better than IBV schemes in terms of verification time, when verifying 800 signatures. To further reduce the communication overhead and improve the efficiency of message verification procedure, He *et al.* [74] and Lo and Lai [75] made their preliminary attempts. The bilinear mapping is replaced to reduce the computation time by avoiding the time-consuming paring operation. [75] also adopts ECC to be the cryptographic tool and avoids the use of MapToPoint operation.

Although those batch verification schemes achieve promising results in terms of efficiency and security, they rely too much on the TPD. To prevent the single point of failure caused by compromised TPD, Chim *et al.* proposed a software based scheme where the secret value is delivered through software [71]. All the vehicles can get the encrypted secret value after they authenticated by a TA. Attackers cannot get any information from the hardware. In order to reduce the communication overhead, authors adopted the bloom filter to store the hashed value of verified messages and signatures. Later, Horng *et al.* [72] found that [71] is vulnerable to impersonate attack. An attacker can impersonate another entity in the network to deliver malicious information after the attacker receives a message with public parameters of the message sender. The problem in [71] is that the TA's secret key may be exposed to attackers. [72] fixed this problem by concealing the TA's secret key in the first handshake procedure between TA and vehicles. However, in [71] and [72], the TA is in charge of generating secret values for vehicles and batch verification can only be used for V2I communications. Zhang *et al.* proposed a scheme that enables batch verification in V2V communications without using ideal TPD [77]. Different from other schemes which store the TA's master key in ideal TPD, [77] only stores the RID, pseudonyms and secrets of the vehicle. Thus, even if all information in a TPD is extracted by an attacker, the attacker can only compromise the vehicle with the compromised TPD but not the whole system. Two secret values of each vehicle are derived from a RSU's secret key. Vehicles within the same RSU coverage area can sign messages with secret values and perform batch verification to verify multiple messages simultaneously using RSU's public key.

The revocation problem has not been well discussed in the previously introduced schemes. However, the revocation checking process is a heavy burden of communication overhead. Jiang *et al.* proposed a scheme based on a hashed message authentication code to overcome the revocation issue [76]. In the proposed scheme, a large area is divided into several domains. All the communications are divided into two situations. One is for vehicles joining a new domain. Another is after vehicles joining the new domain. The mutual authentication of a vehicle and an RSU is processed through pre-stored parameters and system public parameters when a vehicle wants to join a new domain. A new group key is distributed to the vehicle after the mutual authentication. Then, vehicles broadcast the security-related messages with a hashed message authentication code which is derived from the group key. All the messages can be verified in a batched way. Since the RSU ensures only legitimate vehicles can join the group and the group key is updated periodically, in this scheme there is no need to use the CRL to check the revoked vehicles.

Table 3. shows a comparison of the batch verification schemes in terms of security, communication overhead, and computation cost. From Table 3, we can conclude that there is no single protocol can satisfy all the requirements with small communication overhead and computation cost. Some of the protocols like [68], [69], and [70] can achieve excellent performance in terms of verification delay. However, how to securely and efficiently revoke vehicles is not solved in batch based schemes. As long as the revocation problem is not well solved, the overall authentication delay will be high due to the checking process of the CRL. Hence, proposing an appropriate revocation method remains a challenge for batch verification based schemes. How to ensure the success rate of batch verification is another unsolved problem for batch based schemes. If a false signature exists, the whole verification will fail. How to find the false signature and do the re-batch verification work efficiently should be concerned in future work.

TABLE 3. Comparison of Batch Verification Schemes

	Integrity	Non-repudiation	Unlinkability	Anonymity	Traceability	Resist to DoS	Efficient Revocation	Batch check	Overhead (Bytes)	Verification Time	Rebatch time
[66]	✓		✓	✓	✓			✓	21+42n	3TP+nTM+nTm	3TP
[67]	✓	✓	✓	✓	✓			✓	84n	(2n+1)Tm	Tm
[68]	✓		✓	✓	✓				32+46n	3TP+2Tm	
[69]	✓	✓	✓	✓	✓				21+46n	3TP+2Tm	
[70]	✓	✓	✓	✓	✓				67n	2TP+Tm	
[71]	✓		✓	✓	✓	✓			42+21n	2TP+2nTm+nTM	
[72]	✓		✓	✓	✓	✓			42+21n	2TP+2nTm+nTM	
[73]	✓	✓	✓	✓	✓		✓	✓	109n	3TP+(n+1)Tm	3TP
[74]	✓	✓	✓	✓	✓				144n	(3n+2)Tm-ecc + (3n-1)TP-ecc+2nTh)	
[75]	✓		✓	✓	✓				107n	(n+2)Tm-ecc	
[76]	✓	✓	✓	✓	✓		✓		96n	3TP+(n+1)Tm	
[77]	✓	✓	✓	✓	✓				40n	2TP+nTM+2nTm	

[1]"TP" is the time for a paring operation. "TM" is the time used for multiplication based on pairing operation. "Tm" is the time used for basic multiplication. "-ecc" stands for the computation time based on ECC. Th stands for the time used to run a hash function. Both the Overhead and the Verification Time are considered to verify n messages.

IV. TRUST BASED SCHEMES

Trust management is used to complement cryptography based schemes against some specific attacks, e.g. DoS and black hole attacks. Unlike the cryptography based schemes that require 100 percent correctness to pass the authentication process, trust based schemes check whether the reputation score is higher than a threshold. The trust of an entity, either vehicle or message, is determined by the corresponding reputation score, which is accumulated and calculated by a reputation server based on the feedback given by other users. Since there is no cryptography involved in the computation process, the verification efficiency can be achieved much higher than cryptography based schemes. In order to use the reputation score as a supervising tool to protect the vehicular environment from various attacks, a solid and practical method for generating and updating the reputation score must be developed. To improve both the efficiency and security of the trust based schemes, researchers have made tremendous efforts.

A reputation system, proposed by Dotzer *et al.*, is one of the first reputation systems for vehicular networks [78]. In the proposed system, a message generator broadcasts messages to its neighbors. Each forwarder attaches its own opinion and reputation to the message. This approach is named opinion piggyback, which makes each forwarder aggregates all the previous opinions and generates its own opinion providing a reference for the following receivers. However, this scheme only provides a frame of how the trust based scheme works without any detailed design. Many problems haven't been solved. For example, the authors didn't mention how to accumulate vehicle's reputation and to revoke malicious vehicles. The vehicle's ID, reputation and opinion are appended directly into the message without any encryption which makes this protocol vulnerable to various attacks.

Different from [78] where the trustworthiness of the message is mainly based on the reputation of the message generator, Raya *et al.* proposed a scheme that determines the trust level of messages based on data itself [10]. In the proposed scheme, vehicles are divided into different types with different trust levels. The same event reported by vehicles with different trust level is considered to have different trustworthiness. The location relevance and time freshness also make attributes to the logical decision. A comparison of different logic decision methods is provided in this paper. From the simulation results, the authors concluded that the Bayesian inference and Dempster-Shafer theory (DST) are excellent methods for evidence evaluation. The Bayesian interference is the best for the scenario with low uncertainty and DST is more suitable when the uncertainty is high. However, the proposed scheme is only evaluated for the sparse area.

Considering that a central server may be temporary unavailable, Li *et al.* proposed a robust and fault tolerant scheme to overcome this situation [79]. The message sender's reputation is still the major factor that affects the reliability of the message. The reputation server is responsible to collect, update and certificate reputations of all vehicles. Two digital signatures are used to achieve integrity and authentication requirements. And two time stamps are used to check the freshness of messages and reputation score. The trustworthiness of a message is based on the product of the reputation score and the freshness of the reputation. If the multiplication exceeds a pre-defined threshold, the message is considered as trustable. The reputation server decides whether to revoke a vehicle or not by counting the number of negative feedback. When the number of negative feedback is larger than a threshold, then that vehicle should be revoked and its reputation score will be set to 0. However, infrastructures need to be densely installed on the road to achieve a good performance of this scheme. Large communication overhead and verification delay make this scheme inefficient.

Jaimes *et al.* proposed a reputation system to reduce the acceptance rate of fake messages and to improve the efficiency of the reputation based schemes with anonymous [80]. The trustworthiness of a message is generated by the weighted sum of the reputation score of message generator and all forwarders. The friendly state and the unfriendly state of the system are implemented to further improve the system efficiency. In the friendly state, all the vehicles only need to check the signature of messages using the system's public

parameter. While in the unfriendly state, both of the reputation certificate and reputation level need to be checked. The initial state of the system is a friendly state. If the number of negative feedback received exceeds a threshold, the reputation server will inform all the vehicles to switch to the unfriendly state. Though the idea is creative and promising, it only reduces 27 percent of the fake messages showed in simulation results compared to the scenario without using the reputation scheme. The performance and feasibility of this scheme need to be further improved.

Hu *et al.* proposed to choose a platoon header in vehicular networks based on trust mechanism [81]. A platoon header is used to lead a group of vehicles from their origin to destination with a better driving experience. In this scheme, the quality of feedback received from the vehicles is guaranteed by using an iterative filtering. The Dirichlet Model is introduced to cope with the untrustworthiness of vehicles. A reputation server calculates the reputation score of the platoon header according to the filtered feedback and the corresponding trust score of the vehicles who generate the feedback. This scheme is robust against some intricate attacks like badmouth, ballot-stuffing attacks and on-off attacks. But the application area is limited.

In order to handle various attacks, Li *et al.* designed a new trsut management scheme to be attack-resistant [82]. In this scheme, the trustworthiness is evaluated by both node trust and data trust. The proposed scheme has two phases named as data analysis and trust management. All the traffic data is aggregated as evidence by using the DST. Based on the evidence, data and vehicles' trustworthiness can be evaluated. For the node trust, it is further divided into functional trust and recommendation trust. Functional trust is used to indicate the trustworthiness of a vehicle directly. The recommendation trust is used to show the trustworthiness recommendations for other vehicles. It is calculated by computing the similarities between the two vehicles. From the simulation results, the authors concluded that this scheme is resistant to various attacks and has a better performance than the traditional weighted voting approach.

Li *et al.* pointed out that it is not practical to verify the reality of messages with the ephemeral attributes of vehicular networks for checking the data trust [83]. For the entity trust, the average reputation level of the whole network is not a constant. Therefore, the threshold of trustworthiness is modified corresponding to the system's reputation level in the proposed scheme. Each vehicle maintains a trust matrix which contains direct trust value between two vehicles. A reputation center is responsible to update the matrix. Each vehicle's experience trust is calculated by accumulating historical direct trust values of other vehicles toward itself. A central limit theorem is used to filter the experience trust. At last, the vehicle's reputation score is calculated as the average value of the filtered experience trust. Each vehicle needs to attach its ID, reputation, reputation lifetime, and status to the message. The status reflects whether the vehicle is revoked or not. However, there is no simulation results in this paper. Since the scale of vehicular networks could be extremely large, the reputation matrix can be tremendous which is a heavy burden for the reputation center.

Similar to [83], a reputation table is employed in [84]. But in [84], the reputation table is stored in each vehicle. In the table, only a neighbor vehicle's reputation score is recorded. Each vehicle needs to add the new comer's reputation score into its table and check that the reputation score is not equal to zero before they start communication. This scheme is data-trust oriented. If the vehicle is within range of the origin of a message, it will validate this message itself and broadcast the result. If not, it will collect responses from other vehicles until the number exceeds the threshold value to accept the message. Receivers can also make decisions based on the message sender's reputation score directly. Once the message is accepted, the reputation score of the message sender will increase. The major advantage of this scheme is that it does not require too much involvement between vehicles and infrastructures.

V. SOLUTIONS FOR PRIVACY ISSUES

The same as security in vehicular networks, privacy is also a critical factor that affects the feasibility of vehicular networks. The privacy issue in vehicular networks can be further divided into identity privacy and location privacy [17], where the identity privacy requires that the message receivers cannot know any information about "who" send this message and the location privacy should be guaranteed to prevent others know "where" the sender is.

A. IDENTITY PRIVACY PRESERVATION

For identity privacy, the main requirements are conditional anonymity and unlinkability. The conditional anonymity requires that a user's real identity cannot be revealed by any other entities except the TA under restricted conditions. The unlinkability requirement has already introduced in Section II. To achieve identity privacy, group signature based schemes and identity based schemes utilize different approaches.

In group based schemes, each legitimate group member acquires its group private key from the group head to sign messages anonymously. No one can identify a signature to the real sender and no information of sender's real identity is leaked. In identity based schemes, pseudonyms are used to conceal the real identity and frequently changed to prevent tracking. Those pseudonyms are generated with some random value so as to eliminate relations between them. Since pseudonyms are frequently changed in vehicular network applications, some mechanisms are proposed to supplement fast-consumed pseudonyms. One solution is to generate pseudonyms by the vehicle itself, like [9] and [59], so there is no limitation for vehicles to get pseudonyms. Some schemes are using the TA or RSUs to generate pseudonyms, in which vehicles need to keep in touch with RSUs [53]. An alternative way of avoiding generating pseudonyms while using vehicular networks applications is to pre-store pseudonyms in the vehicle. This

method requires a large storage capacity of vehicles and regular pseudonyms update activities, which was considered not applicable in vehicular networks. But the authors in [64] also adopted this method and made a calculation to show that only 1 GB is needed for a vehicle to have a one-month nonstop tour. Thus the pre-store method is feasible.

B. LOCATION PRIVACY PRESERVATION

Identity privacy can be preserved by utilizing pseudonyms. However, using pseudonyms alone cannot preserve location privacy perfectly, where side information, such as users occurring probability related to time and location, can be utilized by attackers.

Recent literature focuses on two aspects which compromise the location privacy in vehicular networks: the pseudonym changing strategies and applications of Location Based Service (LBS). The authors in [11] pointed out that if the pseudonym is shifted at an improper time or at an improper situation, e.g. a vehicle changes pseudonyms at a constant rate, attackers can still track the vehicle's according to the correlation between safety messages which contains vehicle's speed, location, and direction. One of the effective solutions for this problem is to find a moment that the broadcast information (location, speed, direction. etc) of all vehicles is the same or similar so that attackers cannot identify a vehicle from the set of vehicles [11] [85]. Another threat comes from the application of LBSs. With the fast development of wireless technologies, LBS has flourished. Driving experience can be improved by using those LBSs, e.g. vehicles can use LBSs to find the best 10 restaurants in vicinity. To get LBSs, vehicle needs to send requests with its location information to a server. For some services, e.g. navigation, a vehicle needs to send its location information periodically. If the LBS server is compromised or eavesdropped by attackers, users' location privacy is endangered. Different schemes have been developed to solve this problem. Most of them can be classified into two sorts. The first sort utilizes ambiguity to obfuscate vehicle's location, where vehicles can purposely add dummy locations into requests to confuse attackers. Another sort is based on the idea that the less information obtained by the attacker, the harder attacker can attain the vehicle's real location. Thus, location privacy is preserved by reducing the number of requests sent from vehicles to the server. The most common scheme in this category is caching, which stores answers to some specific queries in vehicles so that interaction between vehicles and the server is reduced. Detailed descriptions of those schemes are presented in the following content.

1) PSEUDONYM CHANGING STRATEGIES

Lu *et al.* proposed a scheme that manages vehicles to change their pseudonyms at public social spots, e.g. crossroad and parking lot, to protect location privacy [11]. In the proposed scheme, each vehicle holds a bunch of the authenticated pseudonyms when it is active in vehicular networks. Pseudonyms are not changed after a certain period of time or used in a certain number of messages, but rather changed at social spots. In the proposed scheme, vehicles stop and gather at a crossroad if the traffic light is red. Once the light turns to green, all those vehicles change their pseudonyms at same time so that attackers cannot track a specific vehicle anymore since the side information (speed, direction, location) of vehicles is same. For vehicles entering a parking lot, they should change their pseudonyms when they leave the lot. In [11], the achieved quality of privacy is measured by the privacy metric, i.e. anonymity set size. It uses the anonymity set size as the privacy metric to measure the quality of privacy that has been achieved. It is clarified that the larger the anonymity set size is, the better quality of privacy can be achieved. The anonymity set size is affected by the duration of red lights in a specific road intersection and vehicle's parking time in the parking lot. Game theory is applied to prove that all the vehicles have incentives to change their pseudonyms at social spots to achieve their highest security payoffs.

The idea proposed by Lu [11] is to change pseudonyms when vehicles are static. However, vehicles sometimes keep moving for long distance, where [11] may not be applicable. Ullah *et al.* [85] proposed a pseudonyms changing strategy which is used for vehicles on the way. The authors propose to group vehicles with the same speed. Each group has a counter, which is an arithmetic product of the vehicle's speed and a timer that records the travel time. If the counter reaches a threshold, all vehicles within the same group change their pseudonyms immediately, where those vehicles are relatively static to each other. Simulation results show that this scheme achieves large anonymity size only after the long travel time, e.g. ten hours. This is not suitable for common cases in vehicular networks where the travel time of a vehicle is within one hour.

2) SOLUTIONS FOR LBS

In [12], Niu *et al.* proposed to achieve k-anonymity of vehicles by using dummy locations. When a vehicle sends a query to a LBS with its real location, it also sends other $k-1$ dummy locations. Therefore, the LBS server only has a probability of $1/k$ to reveal the real location of the requester. How to choose those $k-1$ dummy locations greatly affects the practical performance of this kind of schemes. In the proposed scheme, the study area is divided into a grid of 10×10 cells. For each cell, there is a probability of being queried in the past. The entropy of the candidate set is calculated by using these probabilities (the less variance among those probabilities, the larger the entropy will be). The entropy can be seen as the privacy level where the higher entropy stands for higher privacy level. The candidate set that has the highest entropy value is the final decision set send to the LBS. An enhancement is added to this scheme by considering the distance between real location and the dummy locations. The product of the distances between every pair in the candidate set should be larger to make a wider cloaking region. The cloaking region is such an area

that an attacker at most knows its target is inside but cannot figure out the specific location.

In [13], Niu *et al.* employ caching to improve the privacy level and reduce the computation overhead at the vehicle side. If the answer to a request is already cached in the vehicle, then do not have to send the same request again. The fewer requests delivered to LBS server, the harder attacker learns the real location of the vehicle. In this scheme, answers to history requests will be cached in each vehicle. The vehicle first checks whether it already has the answer. If the answer is not contained in the cache, it will send a request to the server, which includes its real location and other random locations. For the selection of dummy locations, an algorithm that can contribute most to the caching is designed. Furthermore, the distance between candidate dummy location and the user's real location, and freshness of the cashed information are considered to improve the performance.

Liu *et al.* proposed another caching based scheme and compared three different ways to manage the cached information [14]. In [14], RSU not only can store data but also broadcast the information at a constant rate. Vehicles within the communication range of RSU receive LBS related messages and store them. When a vehicle has a query, it will first check the cached content. If it has the required information, then the vehicle replies directly to itself. Else, it sends the query with its real location information with k-1 dummy locations to the LBS server. Since the content included in one message and the storage in each vehicle is limited, this paper compares three different methods to minimize the total number of requests sent to LBS server. These three different ways are the first in first out rule, the least recent used methods, and the knowledge-based preaching to sort the LBS answers according to the probabilities queried in the past. The answer with high requested probability has the higher priority to be sent. The knowledge-based preaching method can achieve the highest privacy degree among those three methods in any tested situations according to simulation results. However, the tradeoff between privacy level and the RSU power consumption has not been well considered. Moreover, the power consumption and the storage capacity at vehicle side have not been considered.

Recently, Cui *et al.* [86] pointed out that using dummy locations and caching may degrade the performance of LBS, since the location information obtained by LBS is inaccurate. In [86], a vehicle selects a virtual route that has the least deviation from the real route. The maximum deviance of the virtual route to the real route is defined in the range to 10 to 15 meters so as to reduce the success guessing probability of attackers. The vehicle sends two requests, i.e. one with real route and another with virtual route, to the LBS at same time. When receiving two responds from LBS server, the vehicle drops the useless one. With the increasing number of virtual routes a vehicle sent to the LBS server, the anonymity set of all possible routes of the vehicle grows larger. The larger the anonymity set is, the lower tracking success ratio can be achieved by attackers.

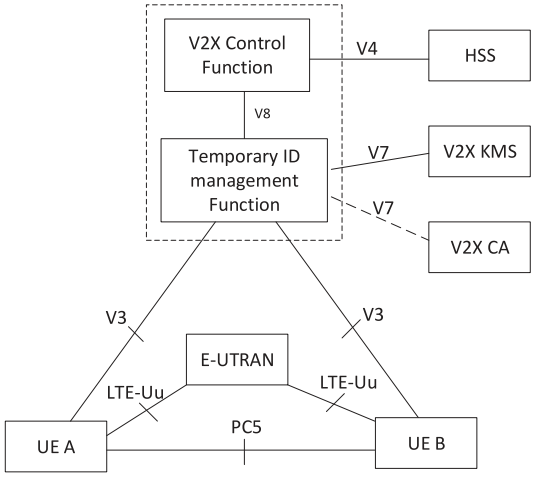


FIGURE 8. Security architecture for V2X communications (PC5 and LTE-Uu based) [91].

Realizing the limitation of using methods of k-anonymity, cloak region, mixed-zone, and cache to provide location privacy, Lim *et al.* proposed a new method named Mutually Obfuscating Paths [87]. One of the major problems of previous location privacy scheme is that these schemes sacrifice the location accuracy to preserve the privacy. So, the proposed scheme in [87] is designed to provide privacy with continuous and high-accuracy location updates. The insight of this scheme is to take advantage of both DSRC and LTE communication accesses. In [87], vehicles in appropriate time and locations that communicate through DSRC will generate fake but plausible positions for each other, and then report both fake and real paths to location based service server through the LTE network. However, this paper only studied the scenario that two vehicles exchange their fake paths. How the proposed scheme works with multiple vehicles has not been discussed.

VI. SECURITY IN CELLULAR BASED V2X COMMUNICATIONS

As one of the major supportive technology of V2X communications, DSRC has attracted great attentions in the last decade. However, many research works have shown that the DSRC bears many disadvantages, e.g. short coverage range (less than one thousand meters), large transmission latency in high density scenario, and low scalability [88]–[90]. On the contrary, the cellular based V2X communications, which have a much larger coverage area and higher transmission data rate, are getting more attention from both industry and academia. 3GPP has made specific standards for V2X services using LTE in Releases 14 [91] and 15. The security architecture for LTE-V2X communications is shown in Fig. 8 [91]. Entities in this architecture are UE, V2X Control Function (VCF), the Home Subscribe Server (HSS), Temporary ID management Function (TIMF), the V2X Key management Server (V2X

KMS), the V2X Certificate Authority (V2X CA) and the E-UTRAN. From the figure we can see that the LTE-Uu is used for the V2I communications and the PC5 is used for V2V and V2P communications. For the LTE-V2X communications based on PC5, UE also needs to connect with the V2X Control Function, which is used to provide necessary parameters for UE. The authentication and authorization of UE are controlled by the VCF through HSS. The distribution of UE's temporary ID and credential is done by TIMF, which can be seen as one network entity with VCF. More details about the cellular based V2X architecture can be found in [92].

Since DSRC and cellular based V2X communications are defined by different standards, their vulnerability to potential attacks is also varied. In LTE-V2X communications, the mutual authentication between the LTE server and UE should be done before UE starts any V2X services. Without the authentication of UE, the LTE server may allocate radio resources to malicious users, thus reducing the availability of legitimate users. Moreover, the DoS attack could be launched if the attacker sends a large number of radio requests simultaneously. So, it is necessary for the LTE server to authenticate each UE before allocating spectrum. On the other hand, the UE has to authenticate the LTE server, because the attacker may act as a fake server to provide service so as to mislead the UE or gain personal information of the UE. The LTE V2X communications can benefit from the existing LTE Authentication and Key Agreement Protocol (LTE-AKA) [93], which is designed to fulfill various functions like user identification and authentication, key derivation, and etc. However, improvements on LTE-AKA are needed due to some inherent vulnerabilities [94]–[99]. Some improvements have already been raised and surveyed in [93]. As for the 3GPP, they have defined some specific solutions in the Release 14 to protect the security between network entities and the privacy of data transmission over PC5. However, for the V2X communication security, there is no normative solution. Security services in V2X communications, like authorization verification, integrity, replay protection, and confidentiality, will rely on the application layer security protocols proposed in other Standard Developing Organizations.

As the LTE-V2X won more focus from DSRC, its successor, 5G-V2X has already been motivated to be the major wireless technique to support V2X services. Some telecommunication and automotive companies like Audi AG, BMW, and Huawei have formed the Fifth-Generation Automotive Association (5GAA), which aims at speeding up the development of connected cars, automated drivings and the ITS [99]. The first 5G automotive tests have been done in South Korea by the 5GAA [100]. The results of those tests are exciting that 5G-V2X communications can have uninterrupted connections with consistent data transmission rate at Gb/s level. Moreover, the transmission latency is controlled in a few milliseconds. This is a good start for stepping into the 5G-V2X era. Shah *et al.* summarize proximity service, mobile edge computing and network slicing as the building blocks for 5G-V2X communications [101]. For the proximity service, it

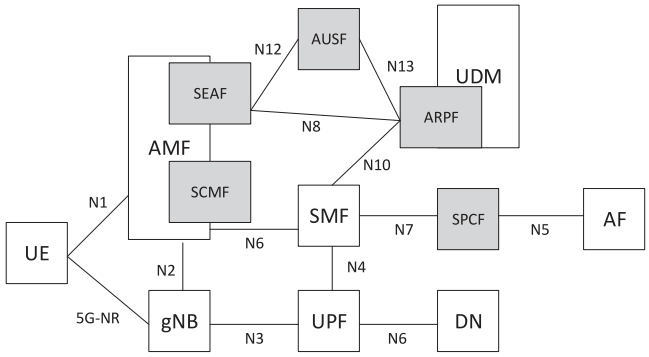


FIGURE 9. Security architecture for 5G-V2X [107].

enables V2X service between UE without the intervention of eNodeB, but the interference at the user side will be higher. An efficient spectrum allocation method, which can be dynamically changed according to service priority, QoS requirement and security, is expected for proximity service. Mobile edge computing is proposed to reduce the response time. Since 5G networks are heterogeneous, availability of all radio access technologies should be considered [102]. One of the solutions is to use SDN and network slicing [103]–[108]. However, the SDN and network slicing in the vehicular network domain are not mature. More efforts should be put into making rational criteria for network slicing and a proper design for SDN. Besides SDN, cloud computing, fog computing, and mobile edge computing are utilized in 5G networks to empower the capacity of the network [109]. Although security issues for these techniques have been studied in [110]–[112], more attention should be paid to V2X related applications.

Security is still a big issue for the successful deployment of 5G-V2X communications. A security architecture summarized by [107] is shown in Fig. 9. Entities in this figure are UE, the next generation NodeB (gNB), User Plane Function (UPF), Data Network (DN), Access and Mobility Management Function (AMF), Security Anchor Function (SEAF), Security Context Management Function (SCMF), Session Management Function (SMF), Security Policy Control Function (PCF), Application Function (AF), Authentication Server Function (AUSF), Authentication credential Repository and Processing Function (ARPF), and Unified Data Management(UDM). The major new element in this 5G architecture is the introduction of SEAF in AMF. The main function of SEAF is that it creates a unified anchor key which is used to protect subsequent communications between the UE and the serving network. SCMF, which is located the same as SEAF in AMF, is responsible to generate specific keys to further access networks. Detailed explanations of all these entities could be found in [113], [114]. However, the application security is out of the scope of existing standards. For the application of V2X communications, new application layer security protocols can be added to enhance security and privacy protection over users. Recently, the 3GPP standardization endeavored to solve problems in several domains as shown below [107].

1) Increased home control
2) Privacy concerns about the enhanced international mobile subscriber identity (IMSI)
3) Security in RAN, network slicing, termination point of user plane
4) Security issues in UE storage, processing of credentials, and eSIM
5) Authentication and authorization

Ferrag *et al.* surveyed authentication and privacy preserving schemes for 4G and 5G cellular networks. Discussed security provision methods in aspects of cryptography methods, humans factors, and intrusion detection methods [115]. Ahmad *et al.* surveyed security challenges and solutions from 2G to 5G, and even the post-5G technologies [116]. However, they mainly focus on the security issues in wireless technologies, leaving the V2X services barely discussed. Considering that little work has been done in studying 5G V2X security, Lautenbach *et al.* made a preliminary security assessment [117]. In [117], authors analyzed the security requirements of V2X use cases introduced by European Telecommunication Standards Institute (ETSI), and explored some security implications in V2X applications with 5G. Lai *et al.* studied general security and privacy issues in 5G-enabled vehicular networks [118]. Some counter measurements are discussed and analyzed through a case study of an autonomous platooning scenario. Since [118] is a magazine paper, the number of references is limited. So, in the following context, we will discuss recent advances in securing cellular based V2X services, which may not be included in other existing surveys.

Zhang *et al.* proposed a cross-physical-application-layer protocol to enhance the V2V communications [119]. In [119], the symmetric key used in the upper layer is derived from the physical layer according to the channel-based key agreement, which leverages the channel state information and received signal strength. Then the symmetric key will be authenticated by the physical-layer entity authentication. If the authentication passes, the symmetric key can be sent to the upper layer to perform secure communications. This cross layer design eliminates the key management process and complex encryption methods in application layer but it requires symmetric random channel characteristics. Ahmed *et al.* evaluated the LTE based V2X architecture defined in 3GPP release 14 and tailored a security scheme to accommodate the discovered issues [120]. In the proposed scheme, two sets of keys are used to provide security and privacy, namely long-term and short-term key. The long term key is used to request pseudonym seed from authorities and a short term key is used to sign the V2X messages. performance analysis shows that the proposed scheme has lower communication and computation overhead, and be scalable in high-density scenario. To prevent the DoS attack that caused by the complicated initial authentication process, Liu *et al.* proposed a puzzle-based co-authentication protocol, which greatly increases the hardness to launch the DoS attack in 5G-V2X communications [121]. In [121], a hash puzzle should be solved before a message is sent. The puzzle is to find a bitstream that when the bitstream is concatenated with the message as the input of a hash function, an arbitrary number of bits at the end of the output are all zeros. Although this method relieves the system from DoS attack, it reduces the capability of each entity to send messages and requests. Moreover, this protocol wastes computational resources and energy resources. Eiza *et al.* proposed a scheme focusing on providing secure video transmission service in 5G-V2X communications [122]. In that paper, vehicles first need to get pseudonyms and certificates from the video reporting services. After that, vehicles can encrypt the video using the symmetric key and then transmit the encrypted video to the server. The symmetric key is encrypted by the attribute based encryption algorithm so that only the authorized V2X entities can restore the symmetric key, i.e. have the access to the video. Liu *et al.* designed a service-oriented authentication framework to secure the D2D group communications in 5G based V2X services [123]. The UE is first authenticated by the network operator through the 5G-AKA process. Then a temporary mobile subscriber ID will be issued to the UE, which will be further used to request V2X service from AMF. The AMF will conduct security check and communicate with service provider to generate a group membership credential. Then the AMF will send the group membership credential and a secure session encryption key to the UE, after which the UE can have secure communications within a group that have the same service. The security of this scheme is based on a classical assumption named LRSW [124] and security analysis shows that the proposed scheme can achieve unforgeability, anonymity, traceability, and adaptive likability. However, the proposed scheme cannot be directly applied to secure V2I and V2N communications. Similarly, Gharsallah *et al.* proposed a security scheme to authenticate a group of vehicles simultaneously in 5G networks [125]. The proposed scheme in [125] is mainly based on the EPS-AKA authentication protocol with some adaptions. The RSU gathers authentication requests for a short time period and forwards all requests to the HSS. The HSS maintains a table that contains an authentication history of all vehicles, and uses the table to check if the new authentication request matches the record. If the authentication pass, the HSS will generate secret parameters, which will be used to establish a session key between the group of vehicles and MME, for each of the vehicle in the group. Their performance analysis shows that the proposed scheme has much lower overhead compared to both the EPS-AKA and an improved protocol named SE-AKA [126] when the number of authentication devices is high.

Besides these new security solutions proposed for cellular based V2X communications, researchers have also concerned security in other V2X services. As computation offloading is enabled in cellular based V2X, secure the offloaded data from eavesdropping is very important. Qiu *et al.* pointed out that using the interference generated by D2D communication can protect offloaded data from eavesdropping [127]. Since the perfect channel state information can be hardly achieved in dynamic vehicular networks, they proposed a novel dynamic threshold based access scheme using imperfect channel

state information. But this paper only limited one vehicle to offload data at one time. The scenario that allows multiple vehicles to offload data simultaneously is more practical and needs to be further studied. In cruise control and platooning services, provide privacy guarantees for users while maintaining the utility of a predictive controller is critical. Zhang *et al.* designed a privacy preserving scheme to protect the platoon header's privacy for the application of predictive speed planning scenario [128]. To achieve differential privacy of the broadcast data from the platoon header, the convex combination of the previous broadcast data and the fresh true date will be generated as the first step. Then a noise will be added, which has zero-mean Gaussian distribution. The performance analysis shows that the proposed method can achieve higher accuracy with same privacy guarantee when compared with other mechanisms. B. Brecht *et al* proposed a credential management system, in which five types of certificate are designed to support different V2X services [129]. In [129], the system is held through many network components, where each component is responsible for a specific job. For example, the Enrollment Certificate Authority only issues enrollment certificates, the Location Obscurer Proxy mainly hides the location of devices, and the Registration Authority is responsible for validating the request from devices. In such a way, the inside attackers can hardly get accurate information of a specific user unless it compromised multiple components at the same time. How ever, the efficiency and feasibility of the scheme has not been discussed. Ahmed *et al.* found that the resource allocation method for V2X period message delivery over the LTE PC5 link may leak location privacy [131]. So, they designed a secure resource allocation mechanism for four different kinds of messages to preserve location privacy while reducing the resource allocation collisions. The main idea is that the vehicle of the next control frame will explore the piggyback message to inform the vehicle of the previous control frame about the allocated Dedicated Radio Bearer. Their performance analysis shows that the proposed scheme has a relatively higher success rate, resource utilization, and the packet reception ratio, which outperforms the methods used in 3GPP Release 14 mode 4 and Release 12 mode 2.

VII. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

V2X communications are regarded as one of the major components of ITS. However, in order to achieve the full potential of V2X communications, many challenges and open issues still need to be solved. In this section, we aim to elaborate the remaining challenges and future research directions toward secure and robust V2X communications.

A. EFFICIENCY OF THE AUTHENTICATION SCHEME

According to the DSRC [26] and IEEE 1609.2 [43] standard, each vehicle is required to send safety related message at every 300 ms interval imposing a burden on each vehicle and the RSU by verifying hundreds of messages every second. Based on this concern, the authentication schemes must be efficient enough to accommodate the stringent delay constrain.

In the discussions of previous sections, we can clearly see that researchers mainly focus on reducing the computation and communication overhead in vehicular networks. Indeed, many schemes supporting batch verification have already achieved good performance for efficient message verification. However, there are some issues in batch verification, such as the low success probability of batch verification and inefficient rebatch algorithm. Since a success batch verification result requires that all the signatures are valid with no transmission error, a single mistake will cause the failure of batch verification. Under the ultra dense scenario, both the large number of signatures and the high level noises exist in data transmission process may severely degrade the performance of batch verification. Thus, an efficient rebatch algorithm is expected for the batch verification schemes.

B. HEAVY RELIANCE ON TPD

Most of the state-of-the-art security and privacy solutions for V2X communications utilize the TPD to store cryptographic parameters of the system. This design can greatly reduce the communication overhead and solve the key distribution problem. However, the utilization on TPD may cause the single point of failure problem. Once a TPD is decoded, the whole system could be compromised. Moreover, the installation of the TPD on each vehicle will greatly increase the price of vehicles, which may not be accepted by consumers. Thus, future security solutions tend to have less reliance on TPD or not use the TPD at all. Our recent work obtains a preliminary result, which achieves secure and efficient authentication without using the idealized TPD [24].

C. EFFICIENT REVOCATION MECHANISMS

Another challenge for vehicular networks is the revocation issue. Once a vehicle is identified malicious, both the vehicle and all the messages sent from this vehicle should be recognized and excluded from the vehicular networks. The revocation scheme adopted by IEEE 1609.2 uses the CRL, where the sender's pseudonym in each message should be checked. Obviously, this approach is inefficient because of the one-by-one processing strategy [25]. Furthermore, the delay for communications increases rapidly when the revocation list grows longer. Consequently, it is critical to find an efficient revocation scheme to speed up both revocation procedure and communication verification process.

D. INTEGRATION OF CRYPTOGRAPHY AND TRUST

The authentication schemes based on cryptography are necessary to prevent the outside attackers. But for inside attackers and some specific attacks, e.g. DoS and black hole attacks, it is hard to achieve security by only using cryptography based protocols. For trust based solutions, it is more efficient to handle the key distribution problem, DoS attacks, and selection of the best routing node. Therefore, trust management could be applied as a complementary tool of cryptography to fulfill a robust and secure vehicular communication system. However, how to combine these two types of solutions into one efficient

and scalable system is a promising topic. Cui *et al.* managed to integrate the trust management with cryptographic method to provide lightweight message authentication for vehicular networks [130]. A multi-weighted reputation system is adopted to update the vehicle's reputation score. Only if the vehicle's reputation score exceeds a threshold value, the vehicle will be issued a credential record from the TA. The credential record will be used to sign and verify the transmitted messages. In this way, the number of untrusted messages can be greatly reduced and the authentication process is highly efficient. However, some important issues need to be further studied, e.g. how to select a proper threshold to maximize the network performance.

E. PRIVACY PRESERVATION

Privacy is critical in vehicular networks. It should be considered from two aspects of identity privacy and location privacy. For protecting the location privacy, additional strategies should be applied besides authentication. Until now, most of the methods proposed for LBS is based on making a cloaking region surround the user vehicle so that attackers can hardly distinguish the target from a set of fake information. An alternative way is to eliminate location related information to be sent so as to lower the security and privacy risks. However, reduce the number of location related messages degrades the accuracy of LBSs. Hence, a location preserving protocol that can balance the security and privacy as well as considering the energy saving and storage capacity aspects are considered as the future research direction to protect the location privacy from applications of LBS. Since authentication must be guaranteed for security and pseudonyms are applied for privacy, those pseudonyms based authentication schemes should be compatible with proper pseudonyms changing strategies to better preserve the privacy in vehicular networks.

F. COMPATIBILITY TOWARDS THE HETEROGENEOUS NETWORKS

In the future, 5G-V2X is like to be the major radio access technology for V2X services, thus new security solutions should consider the heterogeneity of 5G environment. Moreover, the V2X services also belong to the big family of Internet of Things, in which the heterogeneity of the network must be considered. From another point of view, 5G-V2X not only brings challenges but also attributes, like ultra low latency and high data transmission rate. Thus, new solutions may be relieved from constrains in DSRC and take the advantage of the new network architecture.

G. INTRUSION DETECTION MECHANISM

No matter how strong the added security mechanism is, attackers may still break into the system successfully. In that case, effective and efficient intrusion detection mechanisms should be implemented in the network to quickly identify attackers. Moreover, the intrusion detection mechanism can detect and prevent inside attackers. Many works can be found in the literature for intrusion detection, and some recent works have shown that a high detection rate could achieve using machine learning based methods [132], [133]. However, the efficiency of these kinds of schemes could be further improved to fit V2X applications.

H. SECURITY IN AUTONOMOUS DRIVING

Autonomous driving is becoming more and more popular in recent years, and security is still the most important requirement. Autonomous driving is an integration of many technologies, e.g. GPS, light detection and ranging (LiDAR), cameras, operating systems, cloud platforms, etc [134]. So, to secure such a complicated autonomous driving system, various aspects should be considered. Obviously, securing V2X services is one of the most important issues, which has been thoroughly discussed in this paper. Besides that, three other aspects are worth attention, i.e. sensors, operating systems, and control systems. Sensors mounted on autonomous vehicles are responsible for collecting surrounding information, which will be the input to various algorithms. Protect the sensors from jamming, spoofing and DoS attacks remains a big challenge. As for the operating systems and control systems, the main issue is to design a proper authentication method to prevent attackers from hijacking the vehicle through any port in hardware.

I. SIMULATION PLATFORM

In almost all security papers in V2X services, simulation conditions vary a lot. Most of the papers conduct their simulation under a specific scenario, which may not be typical, or may result in unfair comparisons [135]. Thus, determine a general simulation platform that contains typical vehicular network scenarios and V2X uses cases is in great need to provide fair evaluations and comparisons. Moreover, with such a generalized simulation platform, security analysis and scalability study could be done systematically.

J. USING THE UNMANNED AERIAL VEHICLE

The technology of unmanned aerial vehicle (UAV) has a great development in recent years. It is possible to integrate UAVs into vehicular networks to improve security and privacy. Shang *et al.* proposed a preliminary idea to enhance the physical layer security of V2X communications with UAVs [136]. In [136], when eavesdropper is unknown in a certain region, the UAV can act as a friendly jammer in the sky by sending artificial noise to keep the region's signal to interference and noise ratio at a low level. If an eavesdropper is identified, the UAV can act as a relay to transmit messages between vehicles so as to reduce content leakage. Although [136] only provided a rough idea, the UAV may play an important role to secure the V2X communications and preserve vehicle's location privacy, if used properly. For example, multiple UAVs can work as an intermediate layer between vehicles and the LBS server to hide the real location of the vehicle from known by the network operator while reporting accurate feedback to vehicles.

VIII. CONCLUSION

To facilitate the ITS deployment, security and privacy issues in V2X communications must be handled properly. In this paper, security solutions based on cryptography and trust management have been reviewed and discussed. For cryptography based solutions, we analyzed and compared the state-of-the-art batch verification schemes as well as non-batch verification schemes. As the complimentary of cryptography based schemes, we highlighted advantages and disadvantages of trust based schemes. For privacy concerns, we analyzed solutions from aspects of identity privacy and location privacy. Besides the DSRC based V2X communications, we illustrated security architectures and existing solutions for cellular based V2X communications. At the end, we discussed remaining challenges and future research directions for security and privacy in V2X communications.

REFERENCES

[1] ETSITR302637, *Intel. Tran. Syst. (ITS); Veh. Comm.; Basic Set of Appl.; Part 2: Specific. of Coope. Aware. Basic Serv.*, ETSI Std. ETSI ITS Specification TR 302 637 version 1.3.1, Sept. 2014.

[2] X. Shen, X. Cheng, L. Yang, R. Zhang, and B. Jiao, "Data dissemination in VANETs: A scheduling approach," *IEEE Tran. Intell. Transp. Syst.*, vol. 15, no. 5, pp. 2213–2223, Oct. 2014.

[3] Y. Qian and N. Moayeri, "Design of secure and application-oriented VANETs," in *Proc. IEEE Veh. Technol. Conf.*, Singapore, 2008, pp. 2794–2799.

[4] S. Xu, Y. Qian, and R.Q. Hu, "Data-driven edge intelligence for robust network anomaly detection," *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/TNSE.2019.2936466.

[5] M. Raya, J. -P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur., Special Issue Secur. Ad Hoc Sensor Netw.*, vol. 15, no. 1, pp. 39–68, 2007.

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

[7] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[8] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 1229–1237.

[9] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in *Proc. 27th IEEE Conf. INFOCOM.*, 2008, pp. 246–250.

[10] M. Raya, P. Papadimitratos, V. D. Gligor, and J. -P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE 27th Conf. Comput. Commun.*, Phoenix, AZ, USA, 2008, pp. 1238–1246.

[11] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[12] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *Proc. IEEE IEEE Conf. Comput. Commun.*, Toronto, ON, USA, 2014, pp. 754–762.

[13] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. IEEE Conf. Comput. Commun.*, 2015, pp. 1017–1025.

[14] B. Liu, W. Zhou, T. Zhu, L. Gao, T. H. Luan, and H. Zhou, "Silence is golden: Enhancing privacy of location-based services by content broadcasting and active caching in wireless vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9942–9953, Dec. 2016.

[15] S. Xu, Y. Qian, and R. Q. Hu, "Privacy-preserving data preprocessing for fog computing in 5G network security," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, UAE, 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647912.

[16] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[17] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

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

[19] E. A. M. Anita and J. Jenefa, "A survey on authentication schemes of VANETs," in *Proc. Int. Conf. Inf. Commun. Embedded Syst.*, Chennai, India, 2016, pp. 1–7.

[20] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 17, no. 1, pp. 228–255, Jan.–Mar. 2015.

[21] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Compu. Netw.*, vol. 151, pp. 52–67, 2019.

[22] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.

[23] P. Papadimitratos *et al.*, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[24] J. Huang, Y. Qian, and R. Q. Hu, "Secure and efficient conditional privacy-preserving authentication scheme for 5G software defined vehicular networks," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2020.2996574.

[25] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop*, 2005, pp. 11–21.

[26] 5.9 GHz DSRC connected vehicles for intelligent transportation systems, [Online]. Available: https://ecfsapi.fcc.gov/file/7520943378.pdf

[27] IEEE 802.11p, *Amend. to Stdandard for Inf. Tech.-Telecomm. and Inf. Exch. Btw. Syst.-Local and Metropol. Area Net.-Specific req. - Part 11: Wl. LAN Medium Acc. Ctrl. (MAC) and Phy. Layer (PHY) Spec.-Amend. 7: Wl. Acc. in Veh. Env.*, IEEE Stdandard IEEE 802.11p, version 2010, 2010.

[28] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[29] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surv. Tut.*, vol. 20, no. 3, pp. 1858–1877, Jul.–Sep. 2018.

[30] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular Ad Hoc networks," in *Proc. MobiQuitous*, Philadelphia, PA, USA, Aug. 2007, pp. 1–8.

[31] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surv. Tut.*, vol. 13, no. 2, pp. 245–257, Apr.–Jun. 2011.

[32] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3474–3484, Apr. 2020.

[33] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020.

[34] S. Xu, "Data-driven network intelligence for anomaly detection and information privacy," Ph.D. dissertation, Univ. Nebraska-Lincoln, Lincoln, NE, USA, Aug. 2019.

[35] Z. Lei, W. Qian, A. Solanas, and J. Domingo, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Tran. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[36] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surv. Tut.*, vol. 13, no. 4, pp. 584–616, Oct.–Dec. 2011.

[37] J. Huang, Y. Qian, and R. Q. Hu, "Security provision for vehicular fog computing," in *Proc. IEEE VTC Spring*, Antwerp, Belgium, May 25–28, 2020.

[38] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

[39] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine learning and reputation based misbehavior detection in vehicular communication networks," *IEEE Trans. Veh. Commun.*, to be published, doi: 10.1109/TVT.2020.2996620.

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

[41] D. Chaum and E. Van Heyst, "Group signatures," in *Proc. 10th EUROCRYPT Annu. Int. Conf. Theory Appl. Cryptogr. Tech.*, 1991, pp. 257–265.

[42] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[43] *IEEE Stdandard for Wl. Acc. in Veh. Env. Sec. Ser. for Appl. and Mgmt. Msg.*, IEEE Stdandard 1609.2–2013 (Revision of IEEE Stdandard 1609.2–2006), Apr. 2013, pp. 1–289.

[44] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 103–108.

[45] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[46] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3339–3348, Sep. 2013.

[47] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[48] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[49] X. L. Zheng, C. T. Huang, and M. Matthews, "Chinese remainder theorem based group key management," in *Proc. 45th ACMSE*, Winston-Salem, NC, USA, 2007, pp. 266–271.

[50] J. Zhou and Y. H. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme," *J. Chin. Inst. Eng.*, vol. 32, no. 7, pp. 967–974, Oct. 2009.

[51] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Secur. Privacy*, 2003, pp. 197–213.

[52] J. A. M. Naranjo, J. A. L. Ramos, and L. G. Casado, "A suite of algorithms for key distribution and authentication in centralized secure multicast environments," *J. Comput. Appl. Math.*, vol. 236, no. 12, pp. 3042–3051, Jun. 2012.

[53] A. Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 78–89, Jan. 2013.

[54] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil Pairing," in *Proc. 21st Ann. Int. Cryptol. Conf. Adv. Cryptol.*, 2001, pp. 213–229.

[55] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.

[56] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 1, pp. 8–15, Oct. 2006.

[57] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533–549, Feb. 2010.

[58] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[59] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[60] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," *IEEE Trans. Parallel Distribution Syst.*, vol. 25, no. 11, pp. 2794–2803, Nov. 2014.

[61] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Proc. Netw. Distribution Syst. Secur. Symp.*, 2000, pp. 143–154.

[62] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[63] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 896–911, Feb. 2016.

[64] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017.

[65] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. Asiacrypt*, 2001, vol. 2248, pp. 514–532.

[66] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications" *Wireless Netw.*, vol. 17, no. 8, pp. 1851–1865, 2011.

[67] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

[68] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Netw.*, vol. 19, no. 6, pp. 1441–1449, 2013.

[69] J. Zhang, M. Xu, and L. Liu, "On the security of a secure batch verification with group testing for VANET," *Int. J. Netw. Secur.*, vol. 16, no. 5, pp. 355–362, 2014.

[70] S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[71] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.

[72] S. J. Horng *et al.*, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[73] K. A. Shim, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

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

[75] N. W. Lo and J. L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016

[76] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[77] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.

[78] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad hoc network reputation system," in *Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, 2005, vol. 1, pp. 454–456.

[79] Q. Li, A. Malip, K. M. Martin, S. L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[80] L. M. S. Jaimes, K. Ullah, and E. dos Santos Moreira, "ARS: Anonymous reputation system for vehicular ad hoc networks," in *Proc. 8th IEEE Latin-Amer. Conf. Commun.*, 2016, pp. 1–6.

[81] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.

[82] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[83] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Xi'an, China, 2013, pp. 210–214.

[84] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks," *IEEE Syst. J.*, vol. 8, no. 2, pp. 384–394, Jun. 2014.

[85] I. Ullah, A. Wahid, M. A. Shah, and A. Waheed, "VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET," in *Proc. Int. Conf. Commun. Technol.*, Rawalpindi, Pakistan, 2017, pp. 132–137.

[86] J. Cui, J. Wen, S. Han, and H. Zhong, "Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3491–3498, Oct. 2018.

[87] J. Lim, H. Yu, K. Kim, M. Kim, and S. Lee, "Preserving location privacy of connected vehicles with highly accurate location updates," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 540–543, Mar. 2017.

[88] S. Gyawali, "Misbehavior detection and privacy in cellular based vehicular communication networks," Ph.D. dissertation, Univ. Nebraska-Lincoln, Lincoln, NE, USA, Aug. 2020.

[89] S. Chen *et al.*, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, 2017.

[90] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: A survey and future perspectives," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 98–104, Feb. 2016.

[91] "3rd generation partnership project; Technical specification group services and system aspects; study on security aspects for LTE support of V2X services," 3GPP, Sophia Antipolis Cedex, France, TR 33.885, Rel-14 V14.1.0, Sep. 2017.

[92] J. Huang and Y. Qian, "A secure and efficient handover authentication and key management protocol for 5G networks," *J. Commun. Inf. Netw.*, vol. 5, no. 1, pp. 40–49, Mar. 2020.

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

[94] N. Singh and M. Singh Saini, "A robust 4G/LTE network authentication for realization of flexible and robust security scheme," in *Proc. IEEE 3rd Int. Conf. Comput. Sustain. Global Develop.*, 2016, pp. 3211–3216.

[95] A. Daniel, A. Kiening, and F. Stumpf, "PAL - privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication," in *Proc. 10th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl.*, 2013, pp. 1–10.

[96] H. Choi, C. Han, and D. Choi, "Improvement of security protocol for machine type communications in LTE-advanced," in *Proc. Int. Wireless Commun. Mobile Comput. Conf.*, 2015, pp. 1301–1306.

[97] K. J. Ahmed and M. J. Lee, "Secure, LTE-based V2X service," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3724–3732, Oct. 2018.

[98] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE—A networks," *IEEE Commun. Surv. Tut.*, vol. 16, no. 1, pp. 283–302, Jan.–Mar. 2014.

[99] M. Fallgren *et al.*, "Fifth-generation technologies for the connected car: Capable systems for vehicle-to-anything communications," *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 28–38, Sep. 2018.

[100] E. Uhlemann, "Initial steps toward a cellular vehicle-to-everything standard [connected vehicles]," *IEEE Veh. Technol. Mag.*, vol. 12, no. 1, pp. 14–19, Mar. 2017.

[101] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[102] D. Fang and Y. Qian, "On 5G wireless security and privacy—Architecture and flexible mechanisms," *IEEE Veh. Technol. Mag.*, vol. 15, no. 2, pp. 58–64, Jun. 2020.

[103] Z. He, J. Cao, and X. Liu, "SDVN: Enabling rapid network innovation for heterogeneous vehicular communication," *IEEE Netw.*, vol. 30, no. 4, pp. 10–15, Jul. 2016.

[104] J. Liu, J. Wan, B. Zeng, Q. Wang, H. Song, and M. Qiu, "A scalable and quick-response software defined vehicular network assisted by mobile edge computing," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 94–100, Jul. 2017.

[105] S. Gyawali, Y. Qian, and R. Q. Hu, "Resource allocation in vehicular communications using graph and deep reinforcement learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013594.

[106] D. A. Chekired, M. A. Togou, and L. Khoukhi, "Hierarchical wireless vehicular fog architecture: A case study of scheduling electric vehicle energy demands," *IEEE Veh. Technol. Mag.*, vol. 13, no. 4, pp. 116–126, Dec. 2018.

[107] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in *Proc. IEEE Conf. Standards Commun. Netw.*, 2017, pp. 181–186.

[108] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8421–8434, Sep. 2019.

[109] J. Huang, Y. Qian, and R. Q. Hu, "A vehicle-assisted data offloading in mobile edge computing enabled vehicular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013760.

[110] A. Arora, A. Khanna, A. Rastogi, and A. Agarwal, "Cloud security ecosystem for data security and privacy," in *Proc. 7th Int. Conf. Cloud Comput., Data Sci. Eng.. Confluence*, Noida, India, 2017, pp. 288–292.

[111] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of Vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[112] S. Xu, Y. Qian, and R. Q. Hu, "A data-driven preprocessing scheme on anomaly detection in big data applications," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Atlanta, GA, USA, 2017, pp. 814–819.

[113] "System architecture for the 5G system," 3GPP, Sophia Antipolis Cedex, France, TS 23.501, v.15.4.0, Dec. 2018.

[114] "Security architecture and procedures for 5G system," 3GPP, Sophia Antipolis Cedex, France, TS 33.501, v.15.3.1, Dec. 2018.

[115] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, 2018.

[116] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surv. Tut.*, vol. 21, no. 4, pp. 3682–3722, Oct.–Dec. 2019.

[117] A. Lautenbach, N. Nowdehi, T. Olovsson, and R. Zaragatzky, "A preliminary security assessment of 5G V2X," in *Proc. IEEE 89th Veh. Technol. Conf.*, Kuala Lumpur, Malaysia, 2019, pp. 1–7.

[118] C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar./Apr. 2020.

[119] A. Zhang and X. Lin, "Security-aware and privacy-preserving D2D communications in 5G," *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, Jul./Aug. 2017.

[120] K. J. Ahmed and M. J. Lee, "Secure LTE-based V2X service," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3724–3732, Oct. 2018.

[121] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.

[122] M. Hashem Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016.

[123] D. Liu, J. Ni, H. Li, and X. S. Shen, "Achieving adaptive linkability for cellular V2X group communications in 5G," in *Proc. IEEE Global Commun. Conf.*, Abu Dhabi, United Arab Emirates, 2018, pp. 1–7.

[124] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. Cryptographers Track RSA Conf.*, 2016, pp. 111–126.

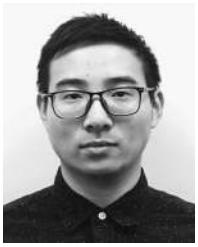
[125] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Inf. Secur.*, vol. 14, no. 1, pp. 21–29, Jan. 2020.

[126] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, 2013.

[127] B. Qiu, H. Xiao, A. T. Chronopoulos, D. Zhou, and S. Ouyang, "Optimal access scheme for security provisioning of C-V2X computation offloading network with imperfect CSI," *IEEE Access*, vol. 8, pp. 9680–9691, 2020.

[128] X. Zhang, C. Huang, M. Liu, A. Stefanopoulou, and T. Ersal, "Predictive cruise control with private vehicle-to-vehicle communication for

improving fuel consumption and emissions," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 91–97, Oct. 2019.
[129] B. Brecht *et al.*, "A security credential management system for V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3850–3871, Dec. 2018.
[130] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6417–6428, Aug. 2019.
[131] K. J. Ahmed and M. J. Lee, "Secure resource allocation for LTE-based V2X service," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11324–11331, Dec. 2018.
[132] S. Gyawali and Y. Qian, "Misbehavior detection using machine learning in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun.*, Shanghai, China, 2019, pp. 1–6.
[133] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.
[134] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, "Edge computing for autonomous driving: Opportunities and challenges," in *Proc. IEEE*, vol. 107, no. 8, pp. 1697–1716, Aug. 2019.
[135] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) communication platforms," *IEEE Trans. Intell. Veh.*, to be published, doi: 10.1109/TIV.2020.2987430.
[136] B. Shang, L. Liu, J. Ma, and P. Fan, "Unmanned aerial vehicle meets Vehicle-to-Everything in secure communications," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 98–103, Oct. 2019.



JIAQI HUANG (Student Member, IEEE) received the B.S. degree in spatial informatics & digitalized technology from the University of Electronic Science and Technology of China in 2016. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering at University of Nebraska-Lincoln. His research interests include cybersecurity and network security, vehicular networks, 5G networks, fog computing, and Internet of Things.

DONGFENG FANG (Member, IEEE) received the B.S. degree in control theory and control engineering from the Harbin Institute of Technology, China, in 2009, the M.S degree in control theory and control engineering from Shanghai University, China, in 2013 and the Ph.D. degree in electrical and computer engineering from the University of Nebraska - Lincoln, USA, in 2019. She is an Assistant Professor in the Department of Computer Science and Software Engineering, California Polytechnic State University, USA. Her current research interests include cybersecurity (wireless security, cyber-physical security, critical infrastructure security, 5G security, IoT security, and privacy), wireless communications and networks, and public safety communications.

YI QIAN (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Clemson University. He is a Professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln (UNL). His research interests include communications and systems, and information and communication network security. Prof. Yi Qian is a Fellow of IEEE. He was previously Chair of the IEEE Technical Committee for Communications and Information Security. He was the Technical Program Chair for IEEE International Conference on Communications 2018. He serves on the Editorial Boards of several international journals and magazines, including as the Editor-in-Chief for IEEE WIRELESS COMMUNICATIONS. He was a Distinguished Lecturer for IEEE Vehicular Technology Society. He is currently a Distinguished Lecturer for IEEE Communications Society.

ROSE QINGYANG HU (Fellow, IEEE) received the B.S. degree from the University of Science and Technology of China, the M.S. degree from New York University, and the Ph.D. degree from the University of Kansas. She is a Professor in the Electrical and Computer Engineering Department and Associate Dean for research of College of Engineering at Utah State University. She also directs Communications Network Innovation Lab at Utah State University. Her current research interests include next-generation wireless system design and optimization, Internet of Things, cyber physical system, mobile edge computing, V2X communications, artificial intelligence in wireless networks, wireless system modeling and performance analysis. Besides a decade academia experience, she has more than 10 years of R&D experience with Nortel, Blackberry, and Intel as a Technical Manager, a Senior Wireless System Architect, and a Senior Research Scientist, actively participating in industrial 3G/4G technology development, standardization, system level simulation, and performance evaluation. She has published extensively in top IEEE journals and conferences and also holds numerous patents in her research areas. Prof. Hu is currently serving on the editorial boards of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the *IEEE Communications Magazine* and the IEEE WIRELESS COMMUNICATIONS. She also served as the TPC Co-Chair for the IEEE ICC 2018. She is an IEEE Communications Society Distinguished Lecturer Class 2015–2018 and a recipient of prestigious Best Paper Awards from the IEEE GLOBECOM 2012, the IEEE ICC 2015, the IEEE VTC Spring 2016, and the IEEE ICC 2016. Prof. Hu is a Fellow of IEEE and a member of Phi Kappa Phi Honor Society.