Security and Privacy Challenges in 5G-Enabled Vehicular Networks

Chengzhe Lai, Rongxing Lu, Dong Zheng, and Xuemin (Sherman) Shen

Abstract

Recently, many academic institutions and standardization organizations have conducted research on vehicular communications based on LTE or 5G. As the most important standardization organization of cellular systems, the 3rd Generation Partnership Project (3GPP) has been developing the standard supporting vehicle-to-everything (V2X) services based on LTE, and has already prepared the roadmap toward 5G-based V2X services. With the emergence of new technologies and applications, such as connected autonomous vehicles, 5G-enabled vehicular networks face a variety of security and privacy challenges, which have not been fully investigated. In this article, we first present the infrastructure of 5G-enabled vehicular networks. Then the essential security and privacy aspects of V2X in LTE specified by 3GPP are introduced. After that, as a case study, we investigate the security and privacy issues of a 5G-enabled autonomous platoon, and propose several candidate solutions, including secure group setup with privacy preservation, distributed group key management, and cooperative message authentication. Finally, we discuss the security and privacy challenges in 5G-enabled vehicular networks.

Introduction

Vehicular communication is one of the key technologies in intelligent transportation systems (ITS) to provide wireless connectivity among vehicles, roadside devices, passengers, and pedestrians. Currently, the mainstream vehicular communications technology can be divided into two categories: dedicated short-range communications (DSRC) and Long Term Evolution (LTE)-based vehicle-to-everything technology (i.e., LTE-based V2X or LTE-V). The former has already been defined by the IEEE 802.11p and IEEE 1609 standards for Wireless Access for Vehicular Environment (WAVE), and the latter is based on cellular network technologies standardized by the 3rd Generation Partnership Project (3GPP). LTE-based V2X communications can make use of high capacity, large cell coverage range, and widely deployed infrastructure to support various vehicular communication services for safety and non-safety applications. Technical organizations like 3GPP and Qualcomm have already prepared the roadmap toward 5G-based V2X services.

5G features extreme high bandwidth, ultra low latency, and high density connections, which can accommodate promising V2X services. Although many recent research activities have been performed to address technical issues of 5G for supporting V2X communications (physical layer structure, synchronization, resource allocation, etc.), it still faces a variety of security and privacy challenges. Recently, Lu *et al.* [1] investigated the security, privacy, and trust management challenges in vehicular ad hoc networks (VANETs) based on IEEE standards. Karnouskos *et al.* [2] preliminarily examined the privacy and data integrity issues of autonomous vehicles. However, the potential security and privacy aspects are not fully discussed in the 5G era due to the emergence of new techniques and applications related to connected autonomous vehicles. To break through the latency and capacity limitations of current vehicular communication systems and effectively support automatic driving, the 5G-enabled vehicular network has evolved in several significant aspects [3]. In the access network, current DSRC and 4G technologies will coexist with the new 5G radios to cooperatively provide high-quality services. In the core network, the cloud computing and software defined networking (SDN) technologies are adopted, which can dynamically and efficiently orchestrate and re-configure resources. In addition, the data volume required, generated, collected, and transmitted for a variety of promising applications and services related to automatic driving has seen an exponential escalation, and vehicular networks have entered the big data driven era [4]. Consequently, new security and privacy challenges, including secure mobility management for group-oriented autonomous platoons, reliable cooperative driving, efficient and privacy-preserving vehicular big data sharing and processing, and so on, should be further investigated in 5G vehicular networks.

In this article, we first present the infrastructure of 5G-enabled vehicular networks. Then the essential security and privacy aspects of V2X in LTE specified by 3GPP are introduced, including security requirements and solutions. As a case study, we investigate the security and privacy issues of an autonomous platoon and propose several candidate solutions. Finally, we discuss the security and privacy challenges in 5G-enabled vehicular networks, and conclude this article.

Chengzhe Lai and Dong Zheng are with Xi'an University of Posts and Telecommunications; Rongxing Lu is with the University of New Brunswick; Xuemin (Sherman) Shen is with University of Waterloo.

Digital Object Identifier:
10.1109/MNET.001.1900220

0890-8044/20/$25.00 © 2020 IEEE

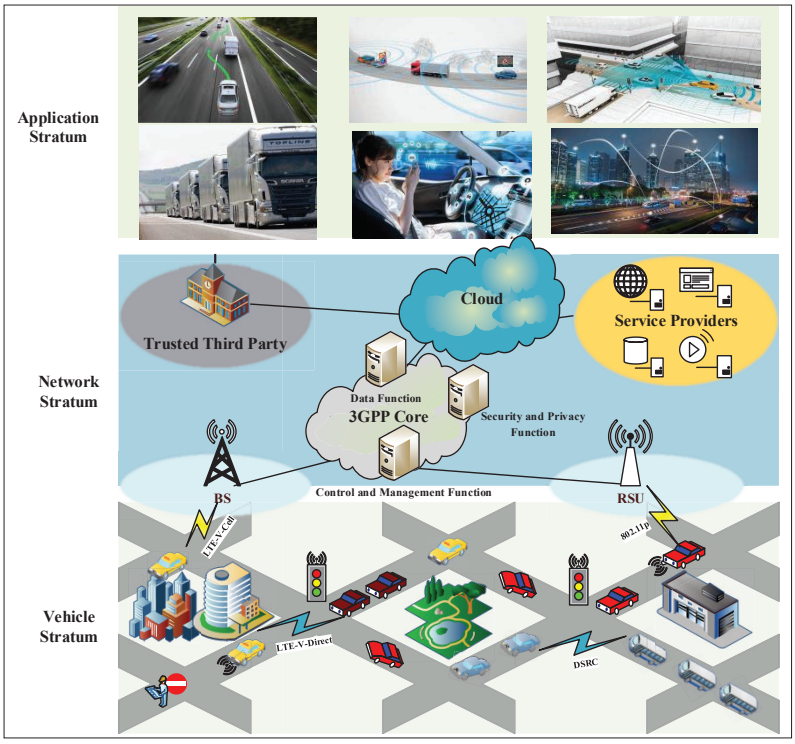

FIGURE 1. Architecture for 5G-enabled vehicular networks.

Architecture for 5G-Enabled Vehicular Networks

3GPP has been actively standardizing LTE-V and providing solutions for V2X communications. LTE-V includes LTE-V-Cell mode, which is TD-LTE centralized enhancements, and LTE-V-Direct mode, which is the TD-LTE decentralized design. Compared to DSRC, LTE-V-Direct is a new decentralized architecture that modifies the TD-LTE physical layer so that it can keep short-range direct communication function, and also provides low latency and high reliability improvements. In the near future, LTE-based technologies and DSRC will coexist [3]. Figure 1 illustrates the architecture for 5G-enabled vehicular networks, which can be divided into three stratums: vehicle, network, and application.

In the vehicle stratum, 5G-enabled vehicles with various sensors can communicate with each other via DSRC, LTE-V-Direct, or device-to-device (D2D) millimeter-wave (mmWave). They can also perceive and collect information from traffic signaling, pedestrians, and so on. In addition, they can further access the 3GPP core network that belongs to the network stratum by the 4G/5G base stations (BSs) or roadside units (RSUs). The network stratum includes all entities of the 3GPP core network, trusted authority, service providers, and cloud. The 3GPP core network plays the key role in the network stratum. 5G-enabled vehicles can access the cloud via the 3GPP core network. In the architecture, the entities of the 3GPP core network contain three main functions by network function virtualization (NFV): the control and management function (CMF), data function (DF), and security and privacy function (SPF). CMF further includes access and mobility management, session management, policy control, authentication and authorization service (e.g., performing access authentication and secure channel establishment procedures, etc.) functions. DF's main responsibility is packet forwarding. SPF can provide security and privacy related services when vehicles access the core network, including storing important key materials. The trusted third party (TTP) consists of two entities: a certificate authority (CA), used to manage certificates, and a trusted identity manager (TIM), used to manage real identities of vehicles for a variety of applications. There are four specific types of V2X application support in 3GPP, including vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), vehicle-to-network (V2N), and vehicle-to-pedestrian (V2P).

Security and Privacy Requirements and Solutions Defined by 3GPP

3GPP specifies the security aspects of V2X in LTE, including essential security requirements on the network entities that are used to support V2X services, as well as the procedures and solutions that are provided to meet those requirements [5].

Security

Security defined in 3GPP mainly includes confidentiality, integrity, authenticity, and resistance to replay attack.

Confidentiality:

- The transmission of data between V2X network entities shall be confidentiality protected.
- The transmission of configuration data between the V2X control function and the onboard equipment (OBE) shall be confidentiality protected.
- The transmission of data between two different V2X entities in the V2X system should be confidentiality protected if needed for the V2X application.
- The transmission of OBE identity should be confidentiality protected.

Integrity:

- The transmission of data between V2X network entities shall be integrity protected.
- The transmission of configuration data between the V2X control function and the OBE shall be integrity protected.
- The transmission of data between different V2X entities in the V2X system should be integrity protected.

Authenticity:

- The V2X network entities shall be able to authenticate the source of the received data communications.
- The V2X-enabled OBE and its V2X control function shall mutually authenticate each other.
- The V2X system entities should be able to authenticate and verify that the sender of the received data communications was authorized to send the data.

Replay Attack:

- The transmission of data between V2X network entities shall be protected from replays.
- The transmission of configuration data between the V2X control function and the OBE shall be protected from replays.

- The transmission of data between different V2X entities in the V2X system should be protected from replays.

Solutions: For all interfaces between network elements, IPsec should be adopted to secure signaling messages on the reference points, and public key infrastructure (PKI) can be applied regarding the use of certificates with the security mechanisms of IPsec.

Between the OBE and network function, for OBE initiated messages, Transport Layer Security pre-shared key (TLS-PSK) ciphersuites with generic bootstrapping architecture (GBA) including the option of the co-located bootstrapping server function (BSF) and network application function (NAF) are used for OBE initiated messages between the OBE and proximity-based service (ProSe) function. The V2X control function plays the role of the ProSe function. For network initiated messages, one of the following mechanisms should be utilized: If a TLS-PSK connection has been established and is still available, the available TLS-PSK session should be used. Otherwise, TLS-PSK with GBA push-based shared key-based mutual authentication between the OBE and the network function should be performed. The network function (pushNAF) shall request user security settings (USS) from the BSF when requesting GBA push information (GPI), and the network function should check in the USS if the Universal Subscriber Identity Module (USIM) is authorized to be used for V2X services. If the authorization in the network function fails, the network function must refrain from establishing TLS-PSK with GBA push. If a TLS connection is released, it can only be re-established by the OBE, even though the TLS session including security association would be alive on both sides.

For security of V2X application data, because V2X applications aim to improve road safety and travel mobility by issuing timely warnings to the driver or providing information about road hazards and congestion, emergency vehicles, and so on, it is of utmost importance that the safety messages broadcasted by OBEs be trusted. The recipients of these messages (i.e., OBEs that are within communication range of the sending OBE) are not known in advance to a transmitting OBE, and thus a priori (e.g., network assisted) security association establishment between OBEs is not feasible to support. This is the nature of this point-to-multipoint communication within a dynamically changing set of OBEs. Neither current LTE security nor ProSe one-to-many communication security is applicable. 3GPP does not consider a specific application-layer security mechanism (e.g., secure autonomous platoon management, real-time map updating) since it is outside the scope of 3GPP. Hence, we investigate some specific application-layer security issues and provide several candidate solutions in 5G-enabled vehicular networks.

Privacy

Subject to regional regulatory requirements and/or operator policy for a V2X application, the data sent in the transmission should not allow OBE identity to be tracked or identified by any other OBE or non-V2X entity beyond a certain short time period required by the V2X application. Subject to regional regulatory requirements and/or operator policy for a V2V/V2I application, the data sent in the transmission should not allow a single party (operator or third party) to track an OBE identity in that region. In addition, the identifiers in the V2X messages should minimize the risk of leaking the OBE or user permanent identities. OBE pseudonymity should be provided to conceal personal data from attackers. The application layer OBE identity in the V2X messages should be protected from eavesdropping.

If an OBE is using the same identity in several broadcast messages, it is possible to track the vehicle and compromise its privacy. Privacy may be supported at the application layer by employing identifiers and credentials that are not linked to long-term OBE or user identifiers. These credentials would be refreshed periodically. The change of application layer identities and credentials for using the V2X service is out of the scope of 3GPP. The OBE shall change and randomize the source layer 2 ID, and the source IP address (in the case of IP-based V2X communication) when indicated by the V2X application that the application layer identifier has changed. The OBE shall also provide indication to the V2X application layer when the source layer 2 ID or/and the source IP address (in case of IP-based V2X communication) are changed.

Researches suggest that grouping vehicles into platoons is an efficient method of increasing the capacity of roads, which can decrease the distances between cars or trucks using electronic, and possibly mechanical, coupling. In the autonomous driving, this driving pattern will be extensively adopted by autonomous driving fleets.

A Case Study: Security and Privacy for an Autonomous Platoon

Autonomous driving is the key application in the 5G era. Research suggests that grouping vehicles into platoons is an efficient method of increasing the capacity of roads, which can decrease the distances between cars or trucks using electronic, and possibly mechanical, coupling. In autonomous driving, this driving pattern will be extensively adopted by autonomous driving fleets. Currently, several companies, such as Volvo, are testing automated technology in semi trucks. A group of autonomous driving vehicles on the highway share a similar itinerary over a period of time and form a vehicle fleet train, coordinated by a platoon leader, which facilitates the potential cooperative communication applications and significantly improves the performance of vehicular networking. The future intelligent transportation will benefit from this driving pattern; however, we must give top priority to the security and privacy issues; otherwise, these techniques cannot be put on the market.

As a case study, we investigate the security and privacy issues of an autonomous platoon and propose several solutions. There are two cases for the formation of a platoon, including the fixed trusted member scenario and dynamic untrusted member scenario. The former is suitable for all vehicles managed and controlled by a company (e.g., transport fleet); thus they have a pre-es-

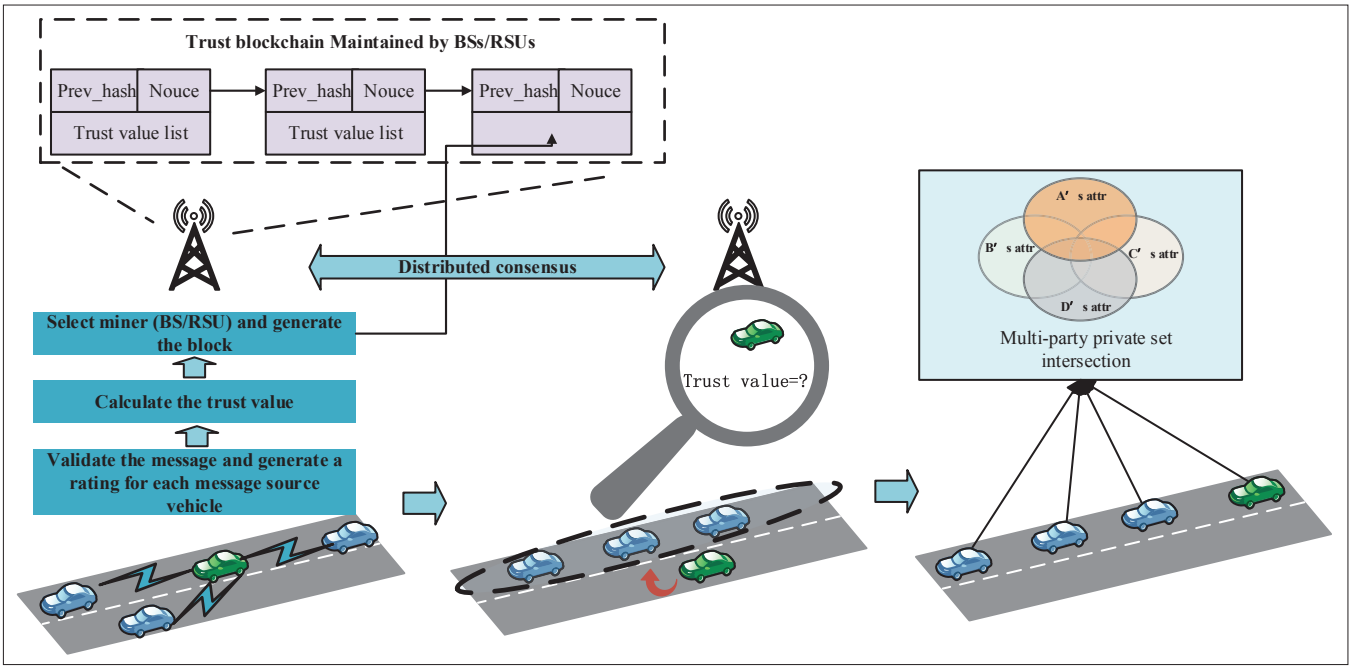

FIGURE 2. Secure group setup with privacy preservation.

tablished trusted relationship, while the latter is a general case in which vehicles belong to individuals and can establish weak ties only when they are proximal for a certain period of time. Therefore, the relationship among them is temporary and untrusted. We mainly consider the second case in this section.

Secure Group Setup with Privacy Preservation

In 5G-enabled vehicular networks, benefiting from autonomous driving, travelers have more time for social activities [6] These vehicles can establish a temporary fleet only when they are proximal for a certain period of time. When a 5G-enabled autonomous vehicle initially joins the road network and decides that it is willing to participate in a fleet, passengers need to first perform an algorithm to check whether they have some similar social attributes, which is the motivation to collaborate. Only if they have high motivation for cooperation will they continue to set up the group and share important information. To facilitate this process, each vehicle is required to indicate its attributes represented by a cooperation attribute set *CAS*. Each element of *CAS* is a variable indicating one specific attribute, such as travel goals, interests of trips, and social background. The cooperation attribute set of each vehicle can be input manually during neighborhood discovery. The vehicles can decide whether to cooperate by evaluating the similarity of their attributes.

However, this mechanism brings two challenges. First, in most situations, all vehicles have mutual distrust, especially if they have never met each other before. When these vehicles seek to participate in a group, they must make sure that the cooperative vehicles have high credibility. To this end, a trust management system based on blockchain techniques [7] can be proposed. Vehicles can verify the received messages from neighboring vehicles. Based on the verification result, the vehicle can generate a rating for each message source vehicle and upload them to BSs or RSUs. With the received ratings for one vehicle, BSs or RSUs can compute its trust value and pack the result into a block. Then each BS/RSU will try to add its block to the trust blockchain by mining. The trust blockchain is maintained by all the BSs/RSUs via a consensus mechanism. When a vehicle wants to join a new group, all members of this group will decide whether to allow it to join by evaluating its credibility. Second, before becoming members of the same group, each vehicle cannot know others' attributes. Even if they become the temporary partner, what they can know is only the similarity of their attributes. For example, there are 10 attributes for each vehicle. We can set a threshold (e.g., 6), and these vehicles are willing to collaborate if the similarity of their attributes exceeds 6. To this end, we can design the privacy-preserving cooperation attribute matching algorithm by using multi-party private set intersection (PSI) [8], which allows two or more participants, each of whome holds a dataset, to compute the intersection of those datasets without revealing anything about other items. Figure 2 illustrates the procedures of secure group setup with privacy preservation.

Distributed Group Key Management

Lai *et al.* [9] present a secure group management framework in integrated vehicular ad hoc network (VANET)-cellular networks, which considers two cases: SEGM-I and SEGM-II. SEGM-I is proposed for the fixed trusted member scenario, and SEGM-II is designed for a general case (i.e., the dynamic untrusted member scenario). For SEGM-II, due to inherent topology, the members of an autonomous driving fleet may change quite dynamically, and autonomous vehicles may join or leave the fleet at any time. Therefore, how to design distributed group key management supporting flexible

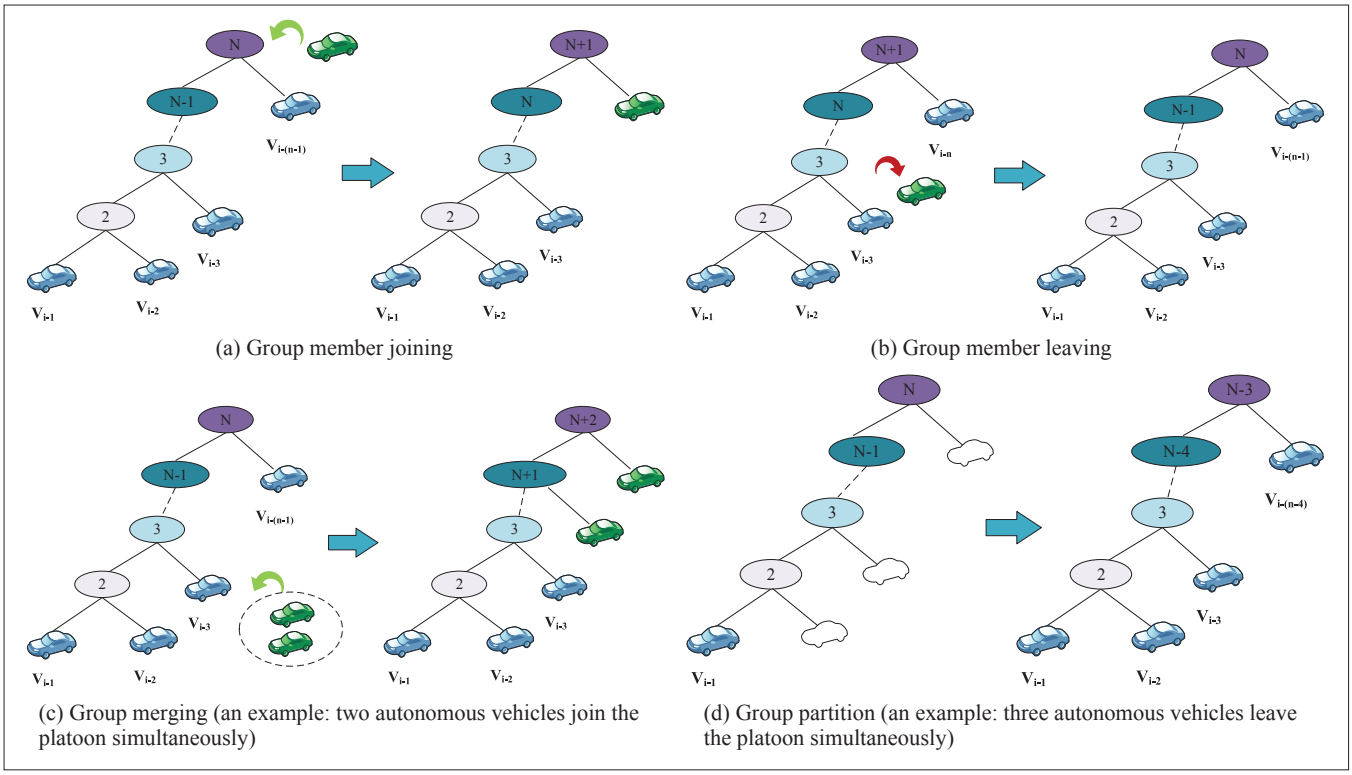

FIGURE 3. Distributed group key management: a) group member joining; b) group member leaving; c) group merging (e.g., two autonomous vehicles join the platoon simultaneously); d) group partition (e.g., three autonomous vehicles leave the platoon simultaneously).

autonomous vehicle fleet management is a challenging issue.

Contributory key generation protocols (CKGPs) can be applied to this scenario. In CKGP-based distributed group key management, all the participants can make sure that their contributions are generated by themselves randomly; hence, all other participants cannot obtain certain participants' secret keys or calculate the final group key without contributions from all group members. For this reason, CKGP is fair enough since all group members equally participate in the key generation process. The proposed distributed group key management can support the following operations [10], including:

- Group member joining: A new autonomous vehicle can join the fleet with a credit mechanism and privacy-preserving attribute matching.
- Group member leaving: An autonomous vehicle can be removed from the fleet due to malicious behaviors or other reasons.
- Group merging: An emerging group of autonomous vehicles want to be added to the existing fleet.
- Group partition: A subgroup is split from the fleet in some conditions.

A Skinny TRee (STR) is adopted to manage the group. An example of distributed group key management for an autonomous platoon is shown in Fig. 3, where V_{i-j} represents the jth vehicle of the ith group.

Cooperative Message Authentication

All autonomous vehicles share their status and road conditions with neighboring vehicles by periodically generating notification messages for cooperative driving. To provide reliable services for an autonomous platoon, the message authentication is an essential feature. The existing authentication protocols have shortcomings in practice, including high communication and computation costs during the authentication [11]. To overcome these shortcomings, we can divide cooperative message authentication for autonomous driving fleet into two types based on the following fact: the autonomous vehicles may belong to different groups and have different relationships (i.e., fixed trusted member scenario and dynamic untrusted member scenario). The first type is appropriate for the fixed trusted member scenario, and autonomous vehicles having common attributes can form a cooperation group (e.g., a fleet of cars belonging to the same company). They can pre-share a group key through a group key agreement mechanism and then perform the cooperative message authentication by utilizing message authentication messages (MACs) among the group members.

The second type is suitable for the dynamic untrusted member scenario. In such a scenario, the anonymous message authentication is desirable since periodic broadcast messages from a vehicle can be used to track its location. Thus, the linkable ring signature technique [12] can be applied to cooperative message authentication among the groups. A ring signature technique allows members of a group to sign the messages on behalf of the group without revealing their real identities (i.e., providing signer anonymity), traceable ring signatures allow the two signatures to be linked, and the identity of the signer will be revealed by the trusted third party when neces-

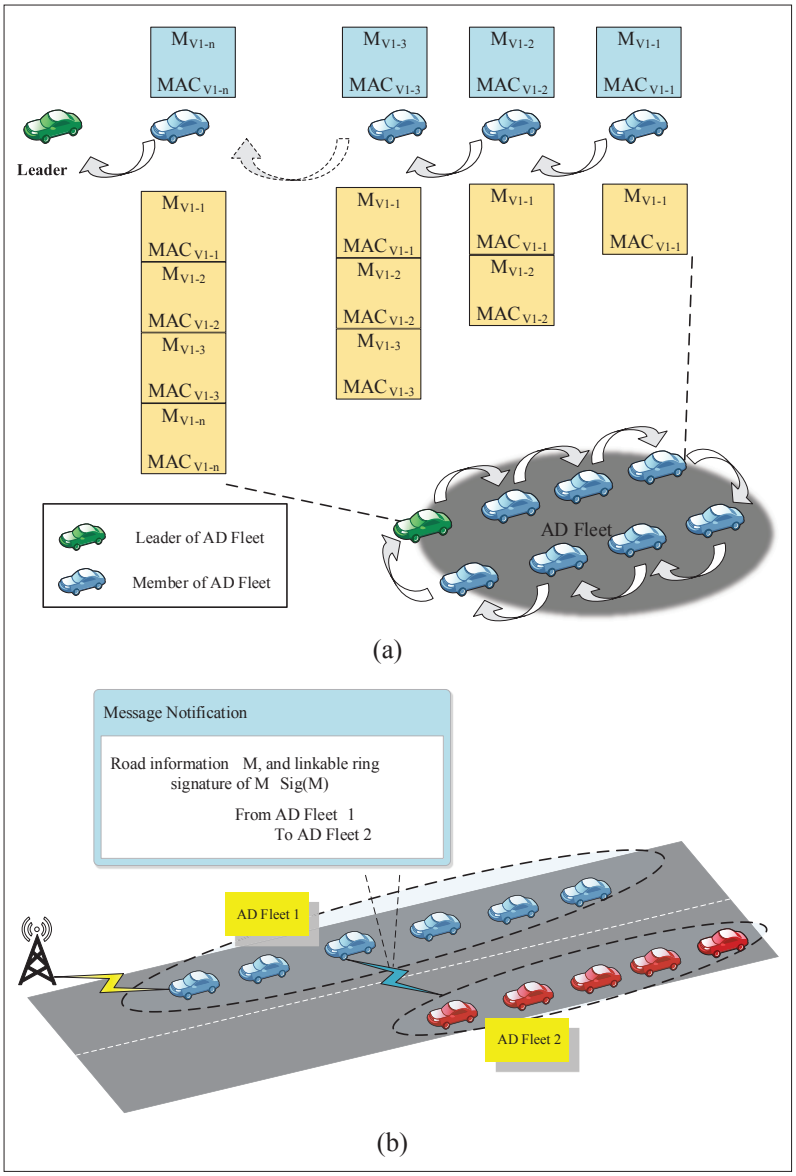

FIGURE 4. Cooperative message authentication: a) cooperative message authentication between the group members]; b) cooperative message authentication between the groups.

sary. The aggregate signature technique combines *n* signatures from *n* different signers on *n* different messages into one signature of unit length, which can be adopted and reduce the communication costs.

Compared to the existing schemes, the messages for authentication decrease significantly since most of the existing schemes require each vehicle to broadcast its message, but our scheme performs authentication by taking the fleet as the unit. In addition, the symmetric-cryptography-based authentication mechanism will be used between the group members, and public-key-cryptography-based authentication technology will be applied between groups, which can effectively reduce the communication and computation overhead of authentication. The basic idea of cooperative message authentication between group members and between groups are shown in Figs. 4a and 4b, respectively.

Open Challenges in 5G-Enabled Vehicular Networks

Despite the fact that many research efforts and technical standardizations have been made for secure vehicular networks, some critical security and data protection challenges and issues still need to be further investigated for 5G-enabled vehicular networks in the autonomous driving era, which are of paramount importance for both vehicle customers and corporations. Figure 5 illustrates the challenges of security and privacy in 5G-enabled vehicular networks.

Security

5G-enabled vehicles can communicate with the core network via V2I service and other vehicles via V2V service. For V2I service, the access authentication and key agreement protocols have been widely studied by both academia and industry. However, secure and efficient mobility management will face a great challenge due to frequent handover and large-scale vehicular machine-to-machine (M2M) communications. The European Telecommunications Standards Institute for Intelligent Transport Systems has defined general security services for vehicular cooperative systems. However, the integration of Internet Protocol Version 6 (IPv6) to the existing work has not been done well. Reference [13] uses Internet Protocol security (IPsec) and Internet Key Exchange version 2 (IKEv2) to secure IPv6 Network Mobility (NEMO). A challenging issue is a secure handoff scenario between LTE and 802.11p. 3GPP has not dealt with further optimizations to efficiently manage handovers between LTE and 802.11p and to reduce the overhead of security signaling. However, this case might occur frequently for fast moving autonomous vehicles across different network operator domains. Therefore, further optimization of cross-domain handover authentication would be useful and could improve resource utilization and quality of service (QoS). Currently, standardized 3GPP tunneling options, — GPRS Tunneling Protocol, Generic Routing Encapsulation-Based (GRE) Proxy Mobile Internet Protocol, and IPsec — strongly rely on centralized anchor nodes and cannot support cross-domain handover authentications. Meanwhile, the existing secure mobility management schemes cannot efficiently support group-oriented communication scenarios.

For V2V service, a new application scenario in 5G vehicular networks is cooperative driving, which allows autonomous vehicles to drive in a platooning pattern to reduce fuel consumption and risks associated with driver mistakes. However, the Sybil attack (through falsification of multiple identities) and message falsification in vehicular platooning will harm V2V service, which could cause serious traffic accidents. Boeira *et al.* [14] describe several attack models, including falsification, covert falsification, emergency braking obstruction, vehicle position hijacking to falsify the leader, and vehicle position hijacking to falsify members. In order to deal with various attacks, the message authentication must be applied, all messages should be transmitted without being changed, and each message should be verified, to confirm its origin. Moreover, the batch verification technique is usually used in cooperative message

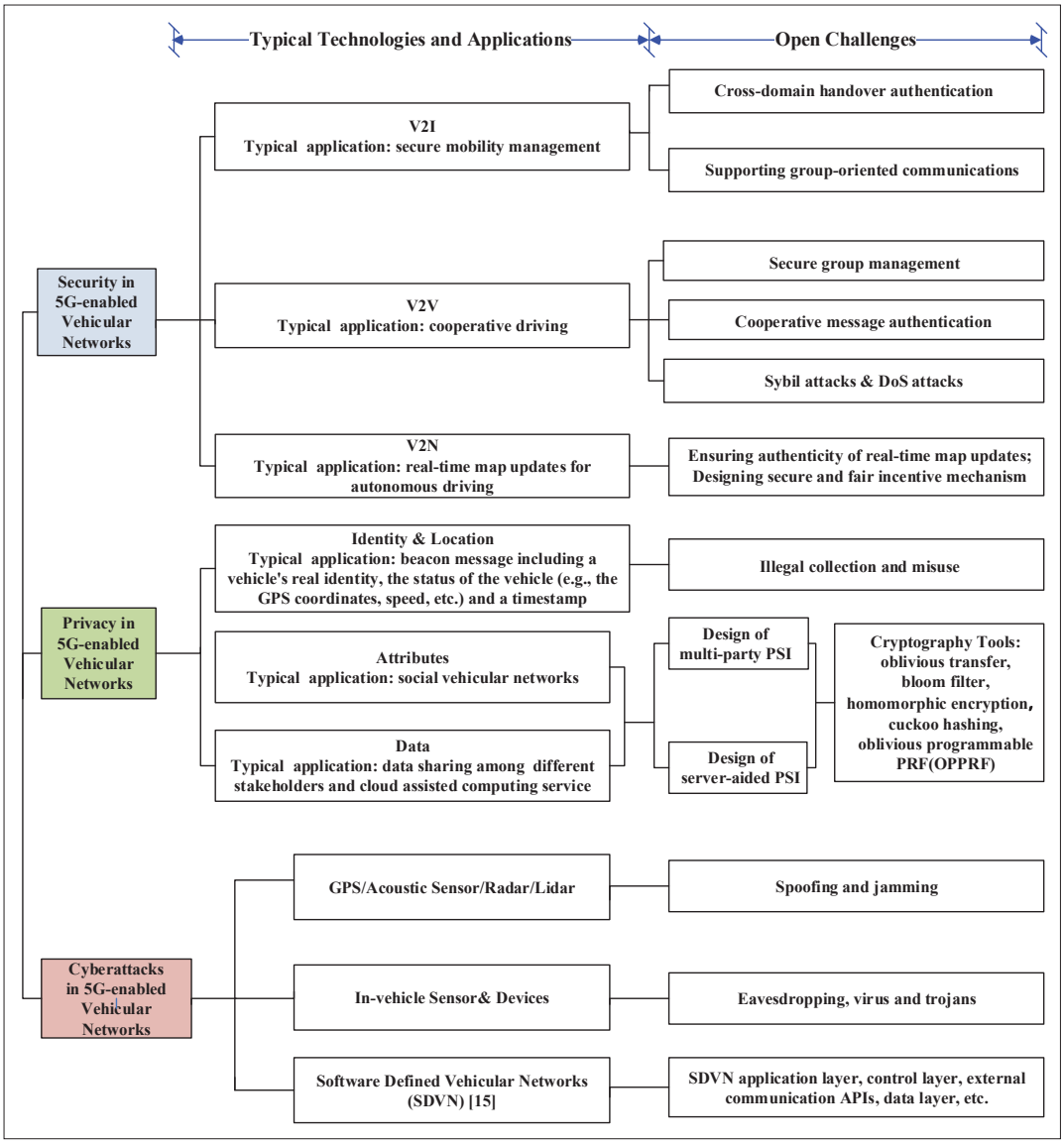

FIGURE 5. Challenges in 5G-enabled vehicular networks.

authentication, but a challenge is how to identify a bad signature. To identify invalid signatures in a batch of signatures, a high-efficiency group testing technique should be proposed, which can find invalid signatures with a few batch verifications.

For V2N service, a typical application scenario in 5G vehicular networks is real-time map updates for autonomous driving. Taking advantage of high-precision maps, the precise navigation of the autonomous vehicle and other auxiliary services for autonomous driving can be achieved. Potential attacks [2] launched by the sender of an update may include forged identification (i.e., an autonomous vehicle could provide a forged identity, e.g., disguising as other existing vehicles), forged location (i.e., an autonomous vehicle could provide a forged location when updating, e.g., give false information of the city it is in), forged event (i.e., an autonomous vehicle could provide a forged or tampered event when updating, e.g., reporting an accident on a highway where actually it never happened). Therefore, corresponding countermeasures should be proposed to resist these attacks and ensure message integrity.

Also, cyberattack is one of the biggest threats to the vehicle industry. Although a major malicious cyberattack on a vehicle has yet to take place, the potential danger will occur at any time. Hackers can already remotely intrude into a vehicle and control its system, including accelerator, brake, and so on. Maybe in the near future, hackers could write a virus that would be transmitted vehicle to vehicle, which poses a great threat to 5G-enabled vehicles. Furthermore, most SDN-specific cyberattacks will exist in vehicular SDN, such as denial of service (DoS) and distributed DoS (DDoS), man in the middle (MITM) attacks, scanning attacks, unauthorized access, and privilege escalation. The security of vehicular SDN was investigated in [15]. Figure 5 gives some potential cyberattacks targeted at 5G-enabled vehicles.

Privacy

The privacy and security issues of 5G-enabled vehicular networks should be discussed separately. Privacy first means only authorized users can access and control vehicle-related information,

A large number of different types of vehicles may access the 3GPP network and obtain services from multiple service providers, which means enormous amounts of data will be produced every moment. Therefore, in the whole vehicular networking industry chain, different stakeholders will have a variety of data about vehicles and their passengers.

such as a vehicle's real identity and location profile. The method to hide a vehicle's real identity is anonymity, which can be provided by pseudonyms. Most of the applications for vehicular networks depend on the beacon messages broadcasted periodically by vehicles [1]. A message includes a vehicle's real identity, the status of the vehicle (the GPS coordinates, speed, etc.), and a timestamp. Cooperatively exchanging information between vehicles and infrastructure can avoid collision and provide location based services (LBSs). However, there is a severe privacy threat for vehicles since the state and location information of a vehicle in broadcasted messages could be collected and misused. Any individual, company, government sector, or even criminal can obtain detailed location profiles of vehicles and consequently their passengers by analyzing these messages. It is very dangerous for a passenger if his/her tracks are exposed to malicious criminals.

Furthermore, the integration of social networks into the Internet of Vehicles (IoV) brings some novel applications in 5G-enabled vehicular networks, mainly related to safety and entertainment. In the future, the passengers in 5G-enabled autonomous vehicles can have more time for business and/or leisure. Therefore, these vehicles have some social attributes [6]. Unlike traditional online social networks, passengers in autonomous cars are anonymous and unknown to each other before cooperation. They are driven to connect due to constrained wireless connectivity and the potential of cooperation. In this situation, the key issue is how to efficiently explore common attributes for cooperation among autonomous vehicles in proximity. In addition, as this process may expose passengers' personal information to the unknown public in some ways, it is of paramount importance to protect the sensitive privacy information of passengers.

A large number of different types of vehicles may access the 3GPP network and obtain services from multiple service providers, which means enormous amounts of data will be produced every moment. Therefore, in the whole vehicular networking industry chain, different stakeholders will have a variety of data about vehicles and their passengers. These data need to be transferred and analyzed for a variety of purposes. For instance, when these stakeholders want to cooperate to share partial data, they will be faced with the problem of the leakage of sensitive information. In addition, some special application scenarios in 5G-enabled vehicular networks, such as high-precision real-time map updates for autonomous driving, vehicles need to report real-time traffic information. However, due to limitation of computing and storage capacity, this information needs to be authenticated with the assistance of the server, which can ensure the authenticity of the message before use. Therefore, the server will require some key information of vehicles, such as location. The server will compare this information to confirm the authenticity of the messages, for instance, determine if the traffic information uploaded by vehicles in the same area are consistent; meanwhile, the privacy information of the vehicle cannot be leaked. In other words, the server cannot obtain the detailed information on each vehicle. For the privacy-preserving data sharing, the more secure, efficient, and practical multi-party private set intersection (PSI) protocols supporting big data processing need to be designed.

Conclusions

In this article, we have studied security and privacy issues in 5G-enabled vehicular networks. First, we have presented the architecture for 5G-enabled vehicular networks. Then the security and privacy aspects of V2X in LTE specified by 3GPP have been introduced. After that, as a case study, we have considered the security and privacy issues of a 5G-enabled autonomous platoon and proposed several candidate solutions, including setting up a trusted group with privacy preservation by adopting blockchain and multi-party PSI, securely managing the group by using contributory key generation protocol, and performing classified cooperative message authentication by using the message authentication code and ring signature technique. Finally, we have discussed the security and privacy challenges brought by a variety of promising applications and services related to automatic driving, and indicated the future work in 5G-enabled vehicular networks.

Acknowledgments

We thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China research grants 61872293 and 61772418, the National Key Research and Development Program of China under 2017YFB0802002, the Innovation Ability Support Program in the Shaanxi Province of China under 2017KJXX-47, and the Shaanxi STA International Cooperation and Exchanges Project under 2017KW-011.

References

[1] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Trans. Intelligent Transportation Systems*, 2018.
[2] S. Karnouskos and F. Kerschbaum, "Privacy and Integrity Considerations in Hyperconnected Autonomous Vehicles," *Proc. IEEE*, vol. 106, no. 1, 2018, pp. 160–70.
[3] K. Katsaros and M. Dianati, "A Conceptual 5G Vehicular Networking Architecture," *5G Mobile Commun.*, 2017, pp. 595–623.
[4] N. Cheng *et al.*, "Big Data Driven Vehicular Networks," *IEEE Network*, 2018.
[5] 3GPP TS 33.185, "Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services," Rel. 15, 2018.
[6] T. H. Luan *et al.*, "Social on the Road: Enabling Secure and Efficient Social Networking on Highways," *IEEE Wireless Commun.*, vol. 22, no. 1, Feb. 2015, pp. 44–51.
[7] Z. Yang *et al.*, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things J.*, 2018.
[8] V. Kolesnikov *et al.*, "Practical Multi-party Private Set Intersection from Symmetric-key Techniques," *Proc. 2017 ACM SIGSAC Conf. Computer and Commun. Security*, 2017, pp. 1257–72.
[9] C. Lai *et al.*, "SEGM: A Secure Group Management Framework in Integrated VANET-Cellular Networks," *Vehic. Commun.*, vol. 11, 2018, pp. 33–45.

[10] C. Lai *et al.*, "Secure Group Communications in Vehicular Networks: A Software-Defined Network-Enabled Architecture and Solution," *IEEE Vehic. Tech. Mag.*, vol. 12, no. 4, 2017, pp. 40–49.
[11] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable Cooperative Authentication for Vehicular Networks," *IEEE Trans. Intelligent Transportation Systems*, vol. 19, no. 4, 2018, pp. 1065–79.
[12] E. Fujisaki, "Sub-Linear Size Traceable Ring Signatures without Random Oracles," *Cryptographers' Track, RSA Conf.*, 2011, pp. 393–415.
[13] P. J. Fernandez *et al.*, "Securing Vehicular IPv6 Communications," *IEEE Trans. Dependable and Secure Computing*, vol. 13, no. 1, 2016, pp. 46–58.
[14] F. Boeira *et al.*, "Effects of Colluding Sybil Nodes in Message Falsification Attacks for Vehicular Platooning," *IEEE Vehic. Net. Conf.*, 2017, pp. 53–60.
[15] A. Akhunzada and M. K. Khan, "Toward Secure Software Defined Vehicular Networks: Taxonomy, Requirements, and Open Issues," *IEEE Commun. Mag.*, vol. 55, no. 7, July 2017, pp. 110–18.

Biographies

Chengzhe Lai [M'15] (lcz_xupt@163.com) received his B.S. degree in information security from Xi'an University of Posts and Telecommunications in 2008 and a Ph.D. degree from Xidian University in 2014. He was a visiting Ph.D. student with the Broadband Communications Research (BBCR) Group, University of Waterloo from 2012 to 2014. At present, he is with Xi'an University of Posts and Telecommunications and the National Engineering Laboratory for Wireless Security, Xi'an, China. His research interests include wireless network security, privacy preservation, and VANET security.

Rongxing Lu [S'09, M'11, SM'15] (RLU1@unb.ca) received his Ph.D. degree in computer science from Shanghai Jiao Tong University, China, in 2006, and his Ph.D. degree (awarded the Canada Governor General's Gold Medal) in electrical and computer engineering from the University of Waterloo, Ontario, Canada, in 2012. He was an assistant professor at Nanyang Technological University, Singapore. Since 2016, he has been an assistant professor in the Faculty of Computer Science, University of New Brunswick, Canada. His research interests include computer, network, and communication security, and applied cryptography.

Dong Zheng (zhengdong@xupt.edu.cn) received an M.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1988, and a Ph.D. degree in communication engineering from Xidian University, in 1999. He was a professor in the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a professor at Xi'an University of Posts and Telecommunications and is also connected with the National Engineering Laboratory for Wireless Security, Xi'an, China. His research interests include provable security and new cryptographic technology.

Xuemin (Sherman) Shen [F'09] (sshen@uwaterloo.ca) is a university professor, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on resource management, wireless network security, social networks, smart grid, and vehicular ad hoc networks. He is an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Royal Society of Canada Fellow. He was a Distinguished Lecturer of the IEEE Vehicular Technology Society and the IEEE Communications Society.