Secure Group Communications in Vehicular Networks

A Software-Defined Network-Enabled Architecture and Solution

Chengzhe Lai, Haibo Zhou, Nan Cheng, and Xuemin (Sherman) Shen

As a means to improve road safety and efficiency and to provide high-performance data transmission service for vehicular networks, group-based vehicular communications (e.g., platoon) has attracted a lot of attention from both academia and industry. In this article, we introduce group-based vehicular communication and address two major security challenges: 1) securely and dynamically setting up and managing the group for a decentralized network, which guarantees the confidentiality and integrity of information being exchanged among vehicles; and 2) secure group access and mobility management for the centralized network, which enables group members to securely and efficiently access the Internet, especially while moving across heterogeneous networks. We propose an integrated network architecture for secure group communication, taking advantage of the software-defined

Digital Object Identifier 10.1109/MVT.2017.2752760
Date of publication: 30 November 2017

network (SDN) technology in fifth generation (5G) mobile networks.

The Benefits and Security Issues of 5G-VANETs

With the rapid development of information and communication technologies, equipping vehicles with radar, LIDAR, global positioning systems, and computer vision techniques is expected to be the next frontier in the automotive revolution [1]. Internet connectivity for infotainment has become an essential part of on-board communications [2]. Group-based vehicular ad hoc networks (VANETs) communication has attracted a lot of attention from both academia and industry for its ability to provide high data packet delivery ratios and throughput, reduced control packet overhead, and minimized delay and packet drop rates. For instance, an effective approach for autonomous vehicles is to change the driving pattern from individual driving to a platoon-based driving [3], [4]. Vehicles on the road with some common interests (e.g., destination, hobby, groups of friends, etc.) can cooperatively form a platoon-based driving pattern, in which a vehicle follows another one and maintains a small and nearly constant distance from the preceding vehicle. Such a platoon-based driving pattern can significantly improve road capacity and energy efficiency. In addition, the clustering algorithms in VANETs, associating vehicles into groups, which has been widely studied [5], can provide high-performance data transmission.

Currently, IEEE 802.11p [16] has been developed as the main communications standard for vehicular networking, while the emerging 5G cellular networks represent practical and convenient marketing solutions to enable ubiquitous and reliable connections to vehicles. The media-rich Internet content delivery for vehicles requires high-rate Internet access, but the existing wireless technologies, such as long-term evolution (LTE), LTE-advanced (LTE-A), and Wi-Fi, are straining to accommodate the explosively growing data traffic because of the shortage of the spectrum. The 5G wireless systems, with improved data rates, capacity, latency, and quality of service (QoS), are expected to be a promising solution in the near future.

Recently, several standards forums and organizations, including the Third-Generation Partnership Project (3GPP), Huawei Technology, and the Datang Telecom Technology and Industry Group, have engaged in cellular-assisted vehicle-to-everything (V2X) communication technology [e.g., LTE for vehicles (LTE-V)] standard development, which is one of the technologies with the most potential in the 5G era [6]. LTE-V can be further divided into two work modes: LTE-V-Cell for a centralized network and LTE-V-Direct for a decentralized network. The former is the extension of the existing cellular technology, and is designed mainly for traditional Internet service. The latter introduces the LTE device-to-device (D2D) and realizes vehicle-to-vehicle (V2V) communication. As a promising new network paradigm in 5G, SDN-based VANETs [7] enable flexible ubiquitous connections, fast rerouting, and real-time network management with the software controller. One of the main features of the SDN is the separation of the control plane and data plane and centralization of control functions. With a programmable SDN controller, network operators can easily configure new network devices and quickly deploy new applications. Vehicle users are able to access network services anywhere, anytime, regardless of the network type (e.g., Wi-Fi, LTE, LTE-A, 5G).

However, in most of the existing literature, the security issues for group-based VANETs communication are not taken into full consideration, which may decrease the reliability of the system and even present serious safety concerns for passengers and other road users. These security issues include: 1) how to securely and dynamically set up and manage the group for a decentralized network, which guarantees the confidentiality and integrity of the critical information exchanging among vehicles; and 2) how to ensure secure group access and mobility management for the centralized network so that group members can securely and efficiently access the Internet, especially when they move across different networks. In this article, we aim to address the above security issues in the SDN-based 5G-VANETs integrated networks.

Network Architecture

Figure 1 illustrates the architecture of the SDN-enabled 5G-VANET integrated network. To support this architecture, appropriate SDN Protocols, such as OpenFlow and Simple Network Management Protocol (SNMP), will be applied to base stations, wireless access points, and other network entities through an external standardized application programming interface (API). OpenFlow is in charge of data path control, and SNMP can be used for Internet Protocol Security (IPsec) establishment. The SDN controller can be placed anywhere since it is just a program running on a server.

The network architecture is designed based on the exiting 3GPP LTE evolved packet core architecture. The access network (AN) can be either 3GPP or non-3GPP. To support Mobile Internet Protocol version 6 (MIPv6), the base stations [i.e., evolved Node B (eNodeBs)] or other wireless access points function as mobile access gateways to provide vehicles with wireless access to the Internet. In the core network, the mobility management control (MM-C) plane substitutes the mobility management entity (MME) and communicates with the OpenFlow controller using an API. In our architecture, the MM-C is responsible for vehicle authentication and authorization and intra-3GPP mobility management. Different from the MME, the MM-C will not be responsible for the serving gateway (S-GW) and packet data network gateway (P-GW) selection. The S-GW can be separated into the S-GW control (SGW-C) plane and S-GW data (SGW-D) plane. SGW-C is responsible for the

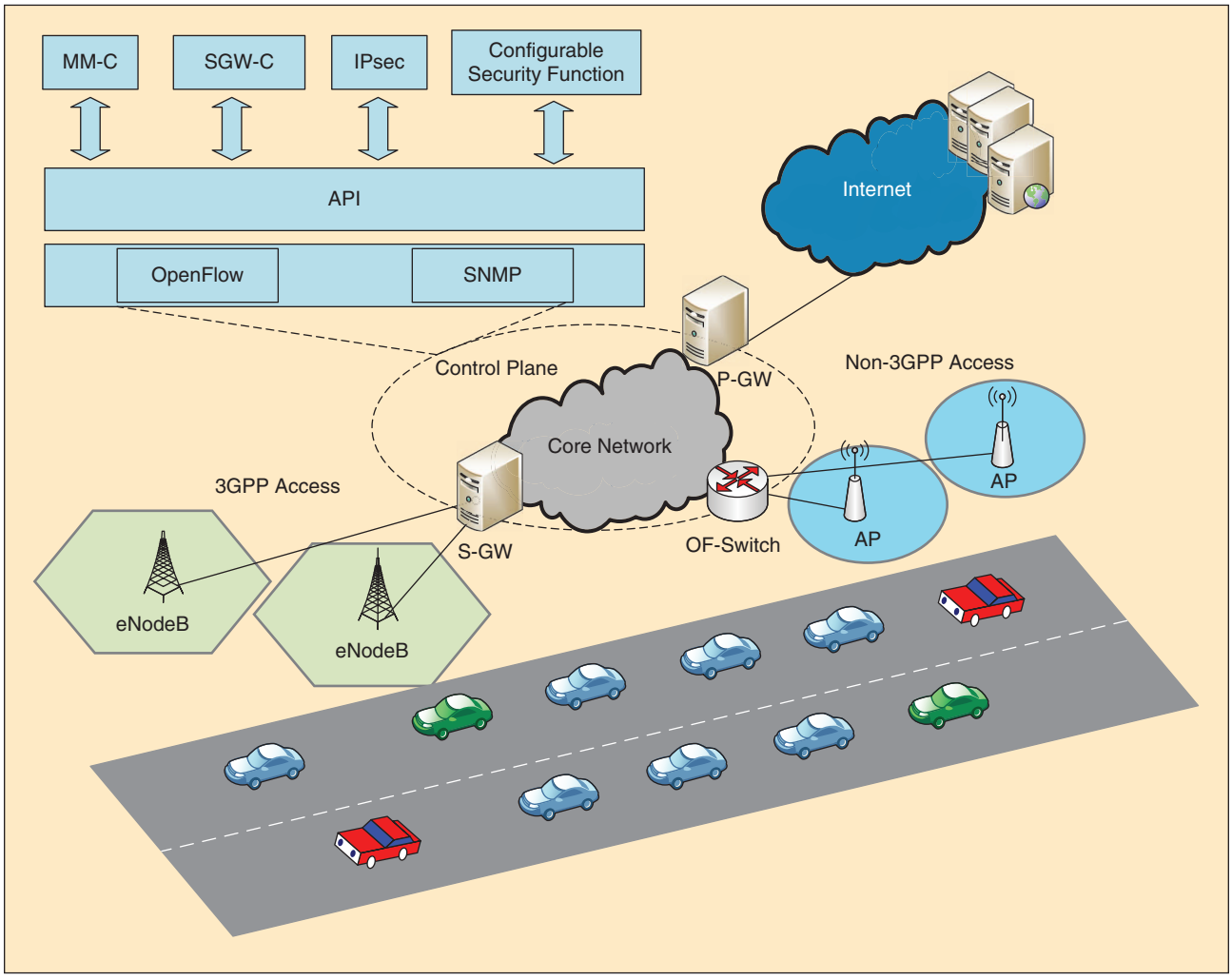

FIGURE 1 The SDN-enabled 5G-VANET integrated network architecture.

GPRS Tunneling Protocol (GTP) tunnel and IPsec establishment. SGW-D represents an advanced OpenFlow switch (OF-switch) that can encapsulate/decapsulate GTP packets. This switch applies the rules received from the OpenFlow controller. Its responsibility is just packet forwarding between eNodeBs and P-GW. P-GW still has the same function as in the 3GPP standard and acts as an anchor of mobility between 3GPP and non-3GPP technologies. Therefore, it plays a role in the local mobility anchor (LMA).

In the SDN-enabled 5G-VANET integrated network, vehicles employing LTE-V technology and equipped with a built-in cellular module can connect to the 3GPP AN via the eNodeB. LTE-V can be further divided into two work modes: LTE-V-Cell for the centralized network and LTE-V-Direct for the decentralized network. Therefore, the introduction of LTE-V-Direct can meet the requirements of low latency and high reliability among connected vehicles. Moreover, vehicles equipping other wireless communication modules can also access the core network via the non-3GPP AN. To provide secure and efficient data transmission, we define the concept of secure mobile gateways. Different from the traditional fixed gateway, a secure mobile gateway refers to the dual-interfaced vehicle that relays data from other vehicle sources to the backhaul network and guarantees the security during data transmission. The main network elements and function description are summarized in Table 1.

Security Challenges in the Group-Oriented Vehicular Environment

Figure 2 shows the two work modes of the LTE-based V2X system: V2V and vehicle-to-infrastructure (V2I). The V2I mode, which consists of LTE-V-Cell and IEEE 802.11p, is an extension of the existing technology and is designed mainly for traditional Internet service. V2V mode (LTE-V-Direct) introduces the D2D to realize the V2V communication. Consequently, there are two major security challenges for the group-oriented vehicular environment in these two modes: 1) how to securely and dynamically manage the group in the decentralized network and 2) how to control the handover signaling overload (introduced by group handover authentication and

TABLE 1 *The functions of the main network elements.*

Network Elements	*Function*
MM-C	The MM-C belongs to the control plane and is a substitute for MME. MM-C communicates with the OpenFlow controller using API. It is responsible for vehicle authentication and authorization and intra-3GPP mobility management.
SGW-C	The SGW-C belongs to the control plane. The SGW-C is separated from the S-GW and is responsible for GTP tunnel and IPsec establishment.
SGW-D	The SGW-D is separated from the S-GW and represents an advanced OF-switch. The SGW-D applies the rules received from the OpenFlow controller. Its responsibility is packet forwarding between eNodeBs and the P-GW.
P-GW	The P-GW reserves the same function as the 3GPP standard and is responsible for acting as an anchor of mobility between 3GPP and non-3GPP technologies. In fact, it plays a role in the LMA.
V_{SMG}	The dual-interfaced vehicle is a secure mobile gateway (V_{SMG}) that is different from the traditional fixed gateway. It relays data from other vehicle sources to the backhaul network and ensures security during data transmission.

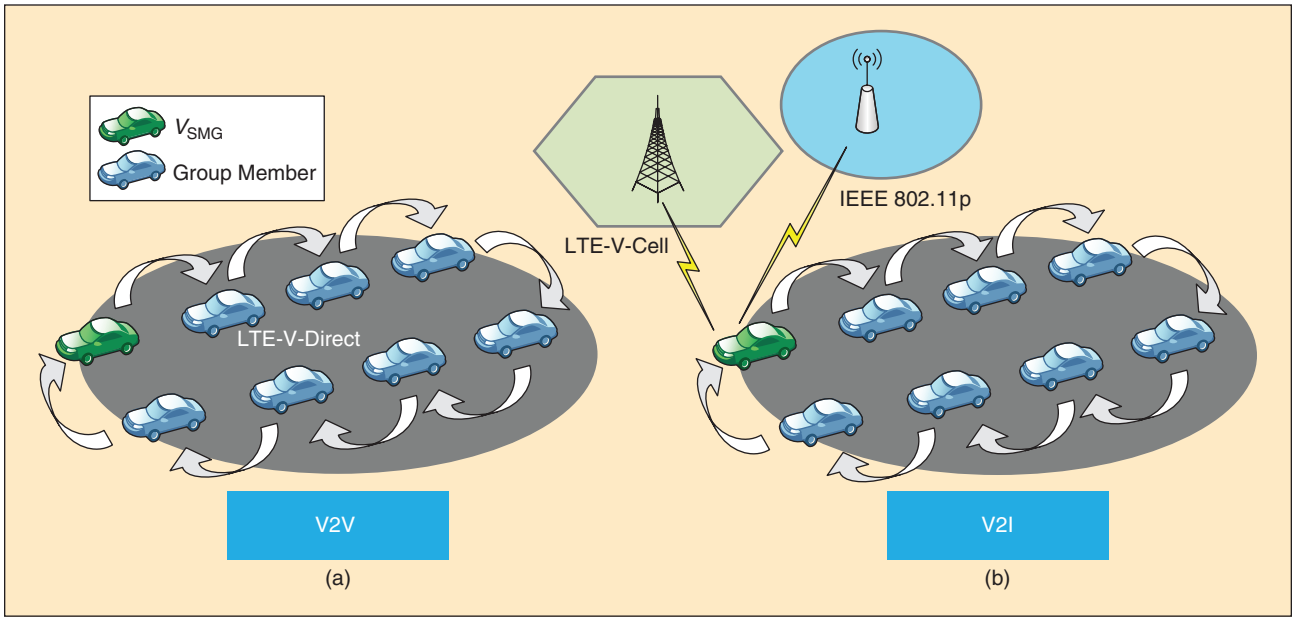

FIGURE 2 The architecture for the two work modes of the LTE-based V2X system: (a) a decentralized network and (b) a centralized network. V_{SMG}: the vehicle acts as a secure mobile gateway.

IPsec establishment) and reduce handover latency when a large number of group members need to securely access the Internet in the centralized network.

Secure Dynamic Group Management in the Decentralized Network

The vehicle group can form in a distributed manner via some sort of clustering algorithm. A VANET clustering algorithm works by associating vehicles into groups, according to some rule sets, and selecting a vehicle as the cluster head (CH). For instance, platoon-based driving, where vehicles on the road cooperatively form a platoon, can significantly improve road capacity and energy efficiency. In some applications, the CH can mediate between the cluster and the rest of the network in the same way as a wireless access point. In [5], Benslimane et al. propose a clustering-based adaptive mobile gateway management scheme in integrated VANET-3G networks to cope with some shortcomings brought by traditional fixed gateways.

However, in such a dynamic and distributed group scenario, all vehicle members are mutually distrustful, even when they've never met each other prior. Therefore, the vehicle members should first authenticate themselves before joining the group. Furthermore, the confidentiality and integrity of important information exchanged among vehicles should be guaranteed because the information involves users' privacy and even relates to users' safety. In addition, the members of the group may change quite dynamically, and vehicles may join or leave the group at any time. Consequently, managing the group in a distributed manner is a challenging issue.

Secure Group-Oriented Access and Mobility Management in the Centralized Network

It is well known that in mobility management for IP-based VANETs, the issue of seamless handover is of great importance for guaranteeing service continuity and QoS, when an automobile is handed off to another network. MIPv6 and network mobility basic support (NEMO-BS) have been developed to provide mobility management for the mobile network. However, the handover delay and mobility support for heterogeneous network roaming are still challenging issues. In the aspect of secure vehicular IPv6 communications, Fernandez et al. used IPsec and Internet key exchange version 2 (IKEv2) to secure IPv6 NEMO [8], concluding that applied IPsec and IKEv2 in vehicular communication for secure IP communications are efficient and necessary. However, the original IPsec is not suitable for a group-oriented vehicle environment because of the large communication and computation overhead.

Moreover, when a group of vehicles want to access the Internet, they first need to securely access the wireless network and should send their access authentication requests toward the core network successively over a short period, or even at the same time. These operations will lead to a communication and computation burden on the network. The recent Authentication and Key Agreement (AKA) Protocols dedicated to the 3GPP evolved packet system (EPS), known as *EPS-AKA*, or for non-3GPP ANs (e.g., Wi-Fi), known as *Extensible Authentication Protocol* (*EAP*)*-AKA*, cannot provide a group authentication mechanism. If a large number of vehicles in a group need to access the network almost simultaneously, the Traditional Authentication Protocols (e.g., EPS-AKA or EAP-AKA) will suffer from high signaling overhead, decreasing the QoS of the network, because every vehicle must perform a full AKA authentication procedure with the home subscriber server, respectively. Because the traditional AKA Protocols are not suitable for group-oriented VANETs communications, we consider designing new group-based Authentication and Key Agreement Protocols.

Security Solutions in the Group-Oriented Vehicular Environment

In this section, we introduce the solutions for secure group communication in decentralized network and centralized network, respectively.

Secure Group Management Scheme in the Decentralized Network

To achieve specific goals, vehicles need to find a suitable vehicle to act as their secure group manager (i.e., V_{SMG}) and form a group (e.g., platoon). The role of the V_{SMG} varies depending on the algorithm, i.e., it may include routing or relaying functions, and it may also be responsible for determining the group membership. Group management procedures are different based on whether the vehicle has become a V_{SMG} or member. As a V_{SMG}, the vehicle will poll the members of its group and assess the group status. As a member, the vehicle will periodically evaluate its link to its V_{SMG}, either by waiting for a poll frame from the V_{SMG} or by actively sending live messages. The secure group management scheme (SGMS) can support the following operations in the group management:

- *group joining*: a new group member can be added to the group with privacy preservation
- *group leaving*: a group member can be removed from the group
- *group merging*: an emerging group of vehicles want to be added to the group
- *group partition*: a subgroup is split from the group, as shown in Figure 3.

Although the V_{SMG} can act as the group founder and key distribution server, such a centralized method will be both expensive and unexpectedly complex and is not suitable for dynamic peer group settings. Therefore, the distributed key agreement technique is required. Contributory group Key Agreement Protocols can generate group keys based on contributions from all group members, and this technique can be a building block of secure group setup. An example scheme of SGMS design can be found in [9].

We derive the properties of the relative distributed key management frameworks in VANETs, and show the results in Table 2. The proposed SGMS follows these four properties:

- *group key secrecy*: the SGMS guarantees that it is computationally infeasible for a passive adversary to discover any group key
- *forward secrecy*: the SGMS guarantees that a passive adversary who knows a contiguous subset of old group keys cannot discover subsequent group keys
- *backward secrecy*: the SGMS guarantees that a passive adversary who knows a contiguous subset of group keys cannot discover preceding group keys
- *key independence*: the SGMS guarantees that a passive adversary who knows any proper subset of group keys cannot discover any other group key not included in the subset.

We confirm that the proposed SGMS is superior to other relevant schemes, particularly, that the proposed SGMS can securely and efficiently support the dynamic group management in VANETs in a distributed manner.

Secure Access and Mobility Management in the Centralized Network

Efficient Group Handover Authentication

Regarding handover authentication, to authenticate all vehicles simultaneously and avoid authentication signaling overload in group-based communications, there are

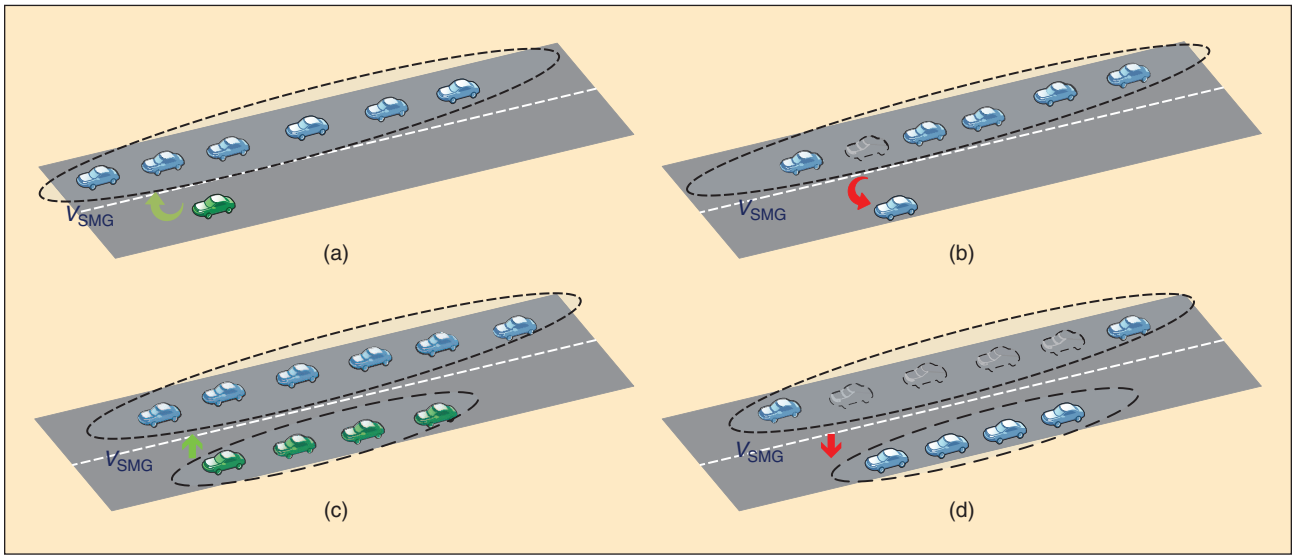

FIGURE 3 During group management, these four operations must be considered: (a) group joining, (b) group leaving, (c) group merging, and (d) group partition.

two categories of protocols: symmetric-cryptosystem-based (SC-based) and asymmetric-cryptosystem-based (AC-based) group handover authentication. Accordingly, we present two group handover Authentication and Key Agreement Protocols:

- *AC-based group handover authentication*: By utilizing the identity-based aggregate signature (IBGS) technique [13], the group-oriented handover authentication can be proposed. In an aggregate signature scheme, multiple signatures can be aggregated into a compact aggregate signature even if these signatures are on many different documents and were produced by many different signers. Particularly, in IBGS, the verifier does not need to obtain and/or store various signer public keys to verify; instead, the verifier only needs a description of who signed what, along with two constant-length tags: i.e., the short aggregate signature and the single public key of a private key generator (PKG). Therefore, the IBGS is suitable for VANETs. When each vehicle registers with the core network, it contacts the PKG, provides its identity, and then receives its private key. Only the authenticated vehicle user can get the private keys from the PKG. The PKG can be integrated with the authentication server, which has pre-established secure channels with the MM-C plane by using the Network Domain Security/IP security mechanism. By adopting the IBGS, the V_{SMG} can collect all signatures of members in the same group and aggregate them to a new signature (SIG_{agg}). Then, the V_{SMG} sends SIG_{agg} to the network and all members in the group can be authenticated at the same time. The independent session key can be negotiated between the core network and each group member. Therefore, this scheme can relieve the authentication signaling overload occurring at the network nodes significantly.
- *SC-based group handover authentication*: Constrained by the computation, battery, and storage capabilities of the vehicle-mounted devices, AC-based group handover

TABLE 2 *Comparisons among the distributed key management schemes in VANETs.*

	Scheme [10]	*DIKE [11]*	*Hao's Scheme [12]*	*SGMS*
Road-side unit assistance	Yes	Yes	Yes	Limited
Group setting	Yes	No	Yes	Yes
Privacy preservation	Yes	Yes	Yes	Yes
Group joining	Yes	Yes	No	Yes
Group leaving	Yes	Yes	No	Yes
Group merging	No	No	No	Yes
Group partition	No	No	No	Yes

DIKE: Dynamic privacy-preserving key management scheme.

IN THE PROPOSED SGMF, ALL VEHICLES IN THE GROUP FORM A PRIVATE NETWORK, IN WHICH EACH GROUP MEMBER HAS AN INNER IP ADDRESS AND UNIQUE IDENTITY THAT FORM A PRIVATE ADDRESSING IDENTIFIER.

authentication may not be suitable for resource-constrained devices due to the application of the public key system. Therefore, SC-based group handover authentication can be proposed by adopting aggregate message authentication code techniques [14]. The supplier provides a group identity (ID_{Gi}) and a group key (GK_i) to each group for authentication. Each vehicle has a preshared secret key ($K_{V\,i-j}$) with the authentication server when it is first registered in the authentication server. The V_{SMG} can collect all message validation codes of members in the same group and aggregate them to a new message authentication parameter (MAC_{agg}). Then, the V_{SMG} sends MAC_{agg} to the network and all members in the group can be authenticated at the same time. Moreover, the independent session key can be negotiated between the core network and each vehicle. Thus, SC-based group handover authentication not only can relieve authentication overhead occurring at the MM-C and eNodeB but is also suitable for resource-constrained environment.

Secure and Efficient Group Mobility Management Framework

The original IPsec is not suitable for a group-oriented vehicle environment; therefore, we adopt the modified IPsec packet and addressing method [15] to design a secure and efficient group mobility management framework (SGMF). In the proposed SGMF, all vehicles in the group form a private network, in which each group member has an inner IP address and unique identity that form a private addressing identifier (PAI). Private IP address spaces were originally defined to delay IPv4 address exhaustion, but they are also a feature of IPv6 addresses for security purposes. Group members cannot directly access the Internet by using PAI. The V_{SMG} have a public IP address and can mediate between the group members and the 5G core network.

When group members want to send or receive data to/from the Internet, they first need to communicate with the V_{SMG}. The V_{SMG} plays a role in the secure mobile gateway to provide secure and efficient data transmission for other group members. For example, when sending data, each group member generates their own packet with an inner IP header, i.e., PAI. Then they send the encrypted packets to the V_{SMG} by using the group key (Triple Data Encryption Standard/Advanced Encryption Standard). The V_{SMG} collects all encrypted packets from group members and assembles them in sequence to form an entire IP payload. The IP payload is then encapsulated into a new IP packet with a new outer IP header. For authenticating the IP packet, an Encapsulating Security Payload Authentication (ESP Auth) trailer needs to be added to the IP packet.

When IP layer (L3) handover occurs, both the handover authentication and IPsec tunnel establishment should be optimized simultaneously. Because security and mobility management-related applications (e.g., MM-C, SGW-C, and IPsec) that are implemented on top of the controller can define the behavior of the switches and eNodeBs/access points, thus creating a reconfigurable 5G-VANET, we can easily adopt the proposed group handover authentication (PGHA) running within IKEv2 between the V_{SMG} and the MM-C/SGW-C plane for authentication and key agreement. At the same time, the L3 handover process should be performed. The SDN concept of a logically centralized control can be implemented in MIPv6 Protocols, e.g., proxy MIPv6 (PMIPv6) through OpenFlow; we designed the SGMF based on PMIPv6. For instance, the controller resides in the backbone network and connects to all the gateways and the anchor. The V_{SMG}s implement the OpenFlow Protocol, after which the controller communicates with them. The V_{SMG} notifies the controller about attachment on behalf of group members through a PMIPv6 control message in the OpenFlow Protocol, and the controller performs all the PMIPv6-related mobility control signaling with the anchor on behalf of V_{SMG}. Theoretically, most of the extension and improvement schemes of PMIPv6 can be applied to the proposed framework. The complete procedure of a group handing off from a non-3GPP AN to eNodeB is presented in Figure 4. The procedure of a group handing off from eNodeB to a non-3GPP AN is similar to the procedure depicted in Figure 4, as the proposed framework is unified.

By applying the group Handover Authentication Protocols to the proposed mobility management framework, the SGMF can provide group-based authentication and key agreement, which enables vehicle members to securely and efficiently access the Internet, especially when they move across heterogeneous networks. The SGMF is secure against hostile eavesdroppers as well as various other attacks specific to group settings, such as denial of service, impersonation, and man-in-the-middle attack.

For performance evaluation, we consider two types of schemes: traditional schemes without supporting group-oriented VANET (TRADIP) and our proposed scheme. Theoretically, most of the PMIPv6 extension and improvement schemes can be applied to the proposed framework. Therefore, for the sake of analysis, we make a concrete analysis by adopting PMIPv6 to the proposed framework as TRADIP. We consider four cases: TRADIP with EPS-AKA, TRADIP with PGHA, SGMF with EPS-AKA, and SGMF with PGHA.

Figure 5 shows the comparison of the average signaling cost. We can see that the average signaling cost of

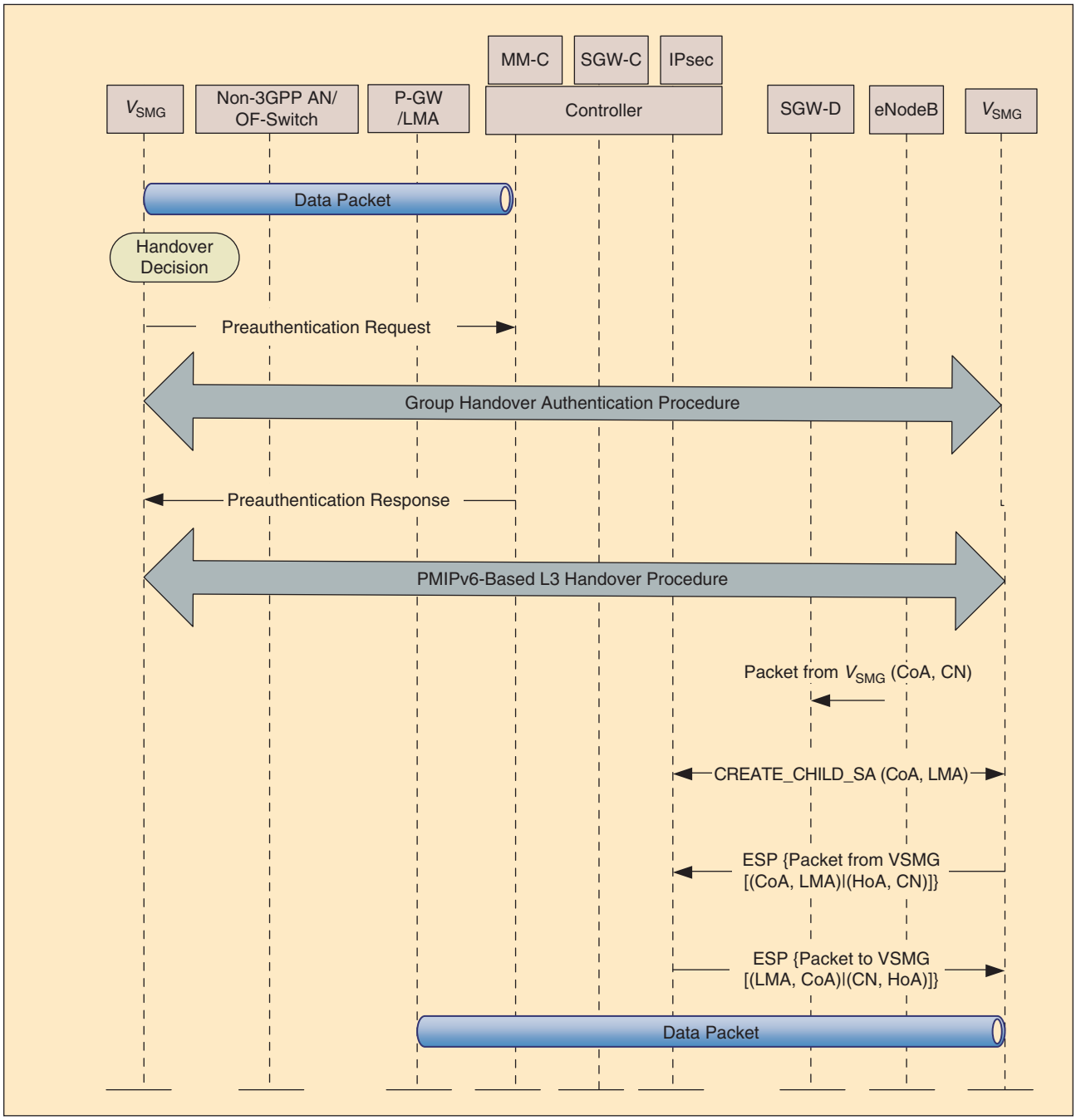

FIGURE 4 The hand-off procedure of a group from a non-3GPP AN to eNodeB. CoA: care of address; CN: corresponding node; SA: security association; HoA: home address.

the SGMF is essentially independent of the number of vehicles (n), and the average signaling cost of SGMF with EPS-AKA is larger than that of SGMF with PGHA since EPS-AKA needs to require additional authentication vectors (the number of authentication vectors is x); We can conclude that the TRADIP with EPS-AKA has the largest signaling cost; the SGMF with PGHA has the lowest signaling messages for handover compared with the other schemes, thus showing the best performance in view of handover signaling cost. Figure 6 illustrates the average handover latency comparison among four cases. The handover latencies of TRADIP with EPS-AKA and TRADIP with PGHA are significantly larger than that of SGMF with EPS-AKA and SGMF with PGHA. This is because the preauthentication is adopted in the proposed SGMF. TRADIP with EPS-AKA and TRADIP with PGHA have longer handover delays than other schemes. On the other hand, the other two schemes show nearly the same handover delay.

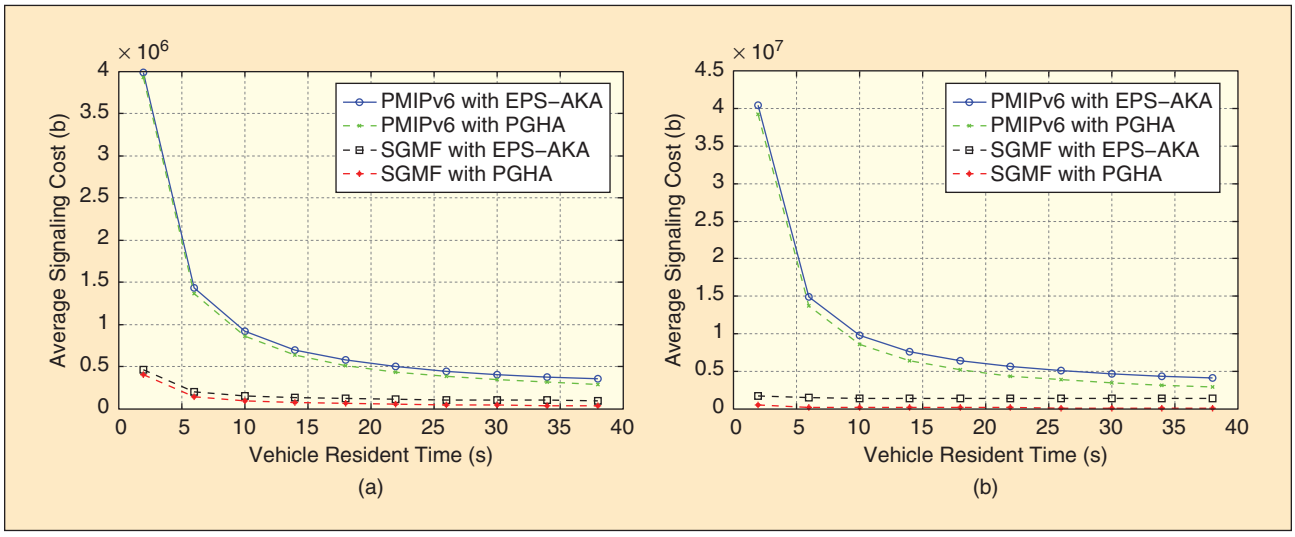

FIGURE 5 A comparison of the average signaling cost between TRADIP and SGMF: (a) $n = 10$, $x = 10$ and (b) $n = 100$, $x = 20$.

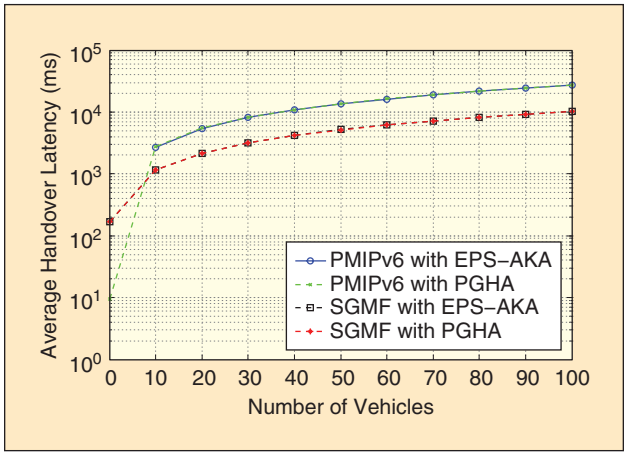

FIGURE 6 A comparison of the average handover latency between TRADIP and SGMF.

Conclusions

In this article, we have investigated secure group communications in SDN-based 5G-VANETs, which aim to address major security challenges in both decentralized and centralized networks. We have proposed a unified communication approach for group-oriented vehicular environment. The performance evaluation demonstrated that our approach outperforms other mobility management schemes with the handover authentication in terms of handover signaling overhead and latency.

Future Directions

Round-efficient group key agreement is important for the distributed key management, especially in VANETs, since the dynamic and multihop nature of VANET communication impacts the stability of links. The fewer rounds there are, the higher the success rate for group key agreement. Therefore, designing the round-efficient group Key Agreement Protocol for VANETs is still a challenge. In addition, vehicles on the road with some common interests (e.g., destination, hobby, groups of friends, etc.) can cooperatively form a group for some specific goals; hence, setting up the group with privacy preserving when considering the vehicles' social attributes is an attractive topic. Due to the human factor, the rational secure multiparty computation is a candidate solution. There are also a set of mobility management and secure IP communications schemes for group-oriented vehicular environments, which could be improved. The SDN-based MIPv6 Protocol should be investigated, since most existing MIPv6 Protocols are designed based on a traditional network architecture and have a series of limitations. Also, the more flexible and lightweight secure IP communication scheme in the high-mobility scenario should be proposed to replace IPsec that have some inherent shortcomings. Finally, the proposed cross-layer authentication mainly occurs above the physical layer (e.g., L2 and L3), and a more efficient cross-layer authentication mechanism involving physical layer could be proposed, which can further significantly reduce the handover authentication latency. We hope this article sheds more light on secure and efficient group communication for autonomous vehicles.

Acknowledgments

We thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China research grants 61502386 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 International Science and Technology Cooperation and Exchange Plan in the Shaanxi Province of China under 2015KW-010.

Author Information

Chengzhe Lai (lcz.xidian@gmail.com) received his B.S. degree in information security from Xi'an University of Posts and Telecommunications, China, in 2008 and his Ph.D. degree from Xidian University, Xi'an, China, in 2014. He is an associate professor with the School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications and with the National Engineering Laboratory for Wireless Security, Xi'an. He is also a visiting researcher of the State Key Laboratory of Integrated Services Networks, Xi'an, and State Key Laboratory of Information Security, Beijing, China. His research interests include wireless network security, privacy preservation, and vehicular ad hoc network security. He is a Member of the IEEE.

Haibo Zhou (h53zhou@uwaterloo.ca) received his Ph.D. degree in information and communication engineering from Shanghai Jiao Tong University, China, in 2014, after which he worked as a postdoctoral fellow with the Broadband Communications Research Group, Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada. He is an associate professor with the School of Electronic Science and Engineering, Nanjing University, China. His research interests include resource management and protocol design in cognitive radio networks and VANETs. He is a Member of the IEEE.

Nan Cheng (n5cheng@uwaterloo.ca) received his B.S. and M.S. degrees from Tongji University, China, in 2009 and 2012, respectively. He obtained his Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada, in 2016. He is currently a postdoctoral fellow with the Department of Electrical and Computer Engineering, University of Toronto, Canada. His research interests include vehicular communication networks, cellular traffic offloading, cognitive radio networks, and device-to-device communications. He is a Member of the IEEE.

Xuemin (Sherman) Shen (sshen@uwaterloo.ca) received his B.Sc. degree from Dalian Maritime University, China, in 1982 and his M.Sc. and Ph.D. degrees from Rutgers University, New Brunswick, New Jersey, in 1987 and 1990, respectively, all in electrical engineering. He is a professor and University Research Chair and the Associate Chair for Graduate Studies with the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada. He is an elected member of the IEEE Communications Society Board of Governors and the chair of the Distinguished Lecturers Selection Committee. He was also the editor-in-chief of *IEEE Internet of Things Journal, IEEE Network, Peer-to-Peer Networking and Application*, and *IET Communications*; a founding area editor of *IEEE Transactions on Wireless Communications*; an associate editor of *IEEE Transactions on Vehicular Technology, Computer Networks*, and *ACM/Wireless Networks*; and the guest editor of *IEEE Journal on Selected Areas in Communication, IEEE Wireless Communications, IEEE Communications Magazine*, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a registered Professional Engineer of Ontario, Canada; an Engineering Institute of Canada Fellow; a Canadian Academy of Engineering Fellow; a Royal Society of Canada Fellow; and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grids, and VANETs. He is a Fellow of the IEEE.

References

[1] N. Lu, N. Cheng, N. Zhang, and X. Shen, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.

[2] T. H. Luan, X. Ling, and X. Shen, "MAC in motion: Impact of mobility on the MAC of drive-thru Internet," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 305–319, Feb. 2012.

[3] H. Peng, D. Li, K. A. Abboud, H. Zhou, H. Zhao, W. Zhuang, and X. Shen, "Performance analysis of IEEE 802.11p DCF for multiplatooning communications with autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2485–2498, Mar. 2017.

[4] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 2016.

[5] A. Benslimane, T. Taleb, and R. Sivaraj, "Dynamic clustering-based adaptive mobile gateway management in integrated VANET-3G heterogeneous wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 559–570, Mar. 2011.

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

[7] K. Liu, J. K. Y. Ng, V. C. S. Lee, and H. S. Sang, "Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network," *IEEE/ACM Trans. Networking*, vol. 24, no. 3, pp. 1759–1773, June 2016.

[8] P. Fernandez, J. Santa, F. Bernal, and A. Gomez-Skarmeta, "Securing vehicular IPv6 communications," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 46–58, Jan./Feb. 2016.

[9] Y. Kim, A. Perrig, and G. Tsudik, "Group key agreement efficient in communication," *IEEE Trans. Comput.*, vol. 53, no. 7, pp. 905–921, July 2004.

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

[11] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

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

[13] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Proc. 9th Int. Workshop Public Key Cryptography*, New York, Apr. 2006, pp. 257–273.

[14] V. Kolesnikov, W. Lee, and J. Hong, "MAC aggregation resilient to DoS attacks," in *Proc. IEEE SmartGridComm*, Brussels, Belgium, Oct. 2011, pp. 226–231.

[15] C. Lai, R. Lu, and D. Zheng, "Achieving secure and seamless IP Communications for group-oriented software defined vehicular networks," in *Proc. 12th Int. Conf. Wireless Algorithms Systems and Applications*, Guilin, China, June 2017, pp. 356–368.

[16] *IEEE Standard for Information Technology*, IEEE Standard 802.11p, 2014.

VT