Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions

Xiaojie Wang, Zhaolong Ning, MengChu Zhou, *Fellow, IEEE*, Xiping Hu, Lei Wang, Yan Zhang, *Senior Member, IEEE*, Fei Richard Yu, *Fellow, IEEE*, and Bin Hu, *Senior Member*

***Abstract*—Vehicular social networks (VSNs), viewed as the integration of traditional vehicular networks and social networks, are promising communication platforms based on the development of intelligent vehicles and deployment of intelligent transportation systems. Passengers can obtain information by searching over Internet or querying vehicles in proximity through intra-vehicle equipment. Hence, the performance of content dissemination in VSNs heavily relies on inter-vehicle communication and human behaviors. However, privacy preservation always conflicts with the usability of individual information in VSNs. The highly dynamic topology and increasing kinds of participants lead to potential threats for communication security and individual privacy. Therefore, the privacy-preserving solutions for content dissemination in VSNs have become extremely challenging, and numerous researches have been conducted recently. Compared with related surveys, this article provides the unique characteristics of privacy-preserving requirements and solutions for content dissemination in VSNs. It focuses on: 1) a comprehensive overview of content dissemination in VSNs; 2) the privacy issues and potential attacks related to content dissemination; and 3) the corresponding solutions based on privacy consideration. First, the characteristics of VSNs, content dissemination and its solutions in VSNs are revealed. Second, the privacy issues for content dissemination in the current VSN architecture are analyzed and classified according to their features. Various privacy-preserving content dissemination schemes, attempting to resist distinct attacks, are also discussed. Finally, the research challenges and open issues are summarized.**

***Index Terms*—Vehicular social networks, content dissemination, potential attacks, individual privacy, attack resistance.**

Manuscript received March 12, 2018; revised August 10, 2018 and October 6, 2018; accepted November 9, 2018. Date of publication November 19, 2018; date of current version May 31, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61733002, Grant 61502075, Grant 61632014, Grant 61772508, and Grant 81401570, in part by the National Basic Research Program of China under Grant 2014CB744600, in part by the Fundamental Research Funds for the Central University under Grant DUT17LAB16, Grant DUT2017TB02, and Grant DUT17RC(4)49, in part by China Postdoctoral Science Foundation under Grant 2018T110210, in part by the Shenzhen–Hong Kong Innovative Project under Grant SGLH20161212140718841, in part by the Guangdong Technology Project under Grant 2016B010108010, Grant 2016B010125003, and Grant 2017B010110007, in part by the Shenzhen Technology Project under Grant JCYJ20170413152535587, Grant JSGG20160331185256983, and Grant JSGG20160229115709109, in part by the Tianjin Key Laboratory of Advanced Networking, and in part by the School of Computer Science and Technology, Tianjin University, Tianjin, China. *(Corresponding authors: Zhaolong Ning; Xiping Hu; Lei Wang; Bin Hu.)*

X. Wang and L. Wang are with the Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, School of Software, Dalian University of Technology, Dalian 116620, China (e-mail: lei.wang@dlut.edu.cn).

Z. Ning is with the Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, School of Software, Dalian University of Technology, Dalian 116620, China, and also with the College of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: zhaolongning@dlut.edu.cn).

M. Zhou is with the Institute of Systems Engineering, Macau University of Science and Technology, Macau 999078, China, and also with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102 USA (e-mail: zhou@njit.edu).

X. Hu is with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China (e-mail: xp.hu@siat.ac.cn).

Y. Zhang is with the Department of Informatics, University of Oslo, 0316 Oslo, Norway (e-mail: yanzhang@ieee.org).

F. R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: richardyu@cunet.carleton.ca).

B. Hu is with the School of Information Science and Engineering, Lanzhou University, Lanzhou 730000, China (e-mail: bh@lzu.edu.cn).

Digital Object Identifier 10.1109/COMST.2018.2882064

I. Introduction

VEHICULAR Ad Hoc Networks (VANETs) have attracted significant attention in both research and industrial communities. In a VANET, vehicles equipped with wireless transceivers are leveraged for data exchange with neighbors [1], [2]. Packets can be routed through neighboring vehicles to destinations. Generally, the message propagation in VANETs occurs through two ways: a) Vehicle-to-Vehicle (V2V), where links are built among vehicles dynamically, and an end-to-end path is formed by randomly selecting next-hop vehicles; b) Vehicle-to-Infrastructure (V2I), which utilizes fixed Road-Side Units (RSUs) to assist a message forwarding process, with the objective of improving message transmission efficiency [3], [4]. VANET potentially enables applications ranging from road safety improvement to entertainment.

Vehicles have changed significantly over the past few years. A brand new design space for vehicular applications has been opened up by the deep integration of sensors and communication technologies [6], [7]. The inspiration of employing wireless communication among vehicles stemmed from 1980s, whereas allocating wireless spectrum for communication among vehicles has been conducted recently. Standards, e.g., IEEE 1069 Wireless Access in Vehicular Environments (WAVE) based on IEEE 802.11p, have been designed for adoption. Traditional vehicular networks are mainly leveraged for data sensing, data collecting and message transmission. Meanwhile, with the rapid evolution of social

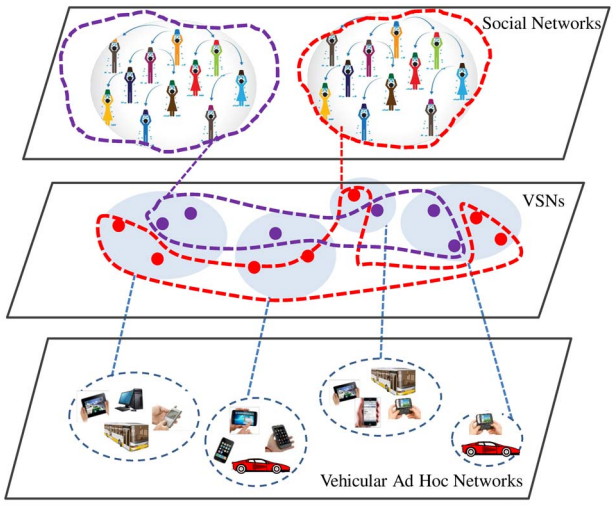


Fig. 1. A schematic diagram of VSNs [5].

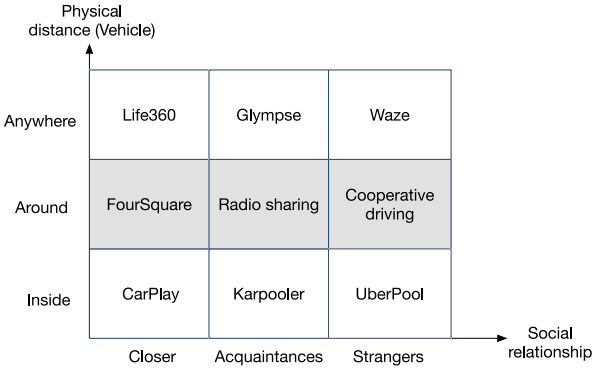


Fig. 2. Some existing applications of VSNs [10].

networks, applications in vehicular networks have been greatly developed. As new paradigms, Vehicular Social Networks (VSNs) exploit social properties of vehicles to improve the performance of vehicular networks [8]. As shown in Fig. 1, a VSN not only includes traditional V2V and V2I communication patterns, but also contains human factors affecting vehicular connectivities, such as human mobilities, selfishness and individual preferences [9].

Recently, the development of VSNs has gained strong support, with increasing number of applications for VSNs occupying people's daily life. Existing applications based on physical distances and social relationships in VSNs are illustrated in Fig. 2. With these applications, individuals can share information with others efficiently, e.g., having fun with family members through *CarPlay*, sharing restaurant views with friends by *FourSquare*, tracking locations of folks via *Life360*, scheduling a carpool with workmates through *KarPooler*, sharing real-time locations with acquaintances by *Glympse*, providing a ride-sharing with others by *UberPool*, driving with neighboring cars via *Cooperative driving*, and broadcasting traffic information to strangers through *Waze* [10].

Meanwhile, many countries all over the world are paying attention to the establishment of VSNs. ERTICO-ITS, a public/private partnership, promotes the development and deployment of Intelligent Transportation Systems (ITSs) in Europe. These European countries are positive to improve transportation safety, network security and efficiency, and reduce environmental impacts [11]. In addition, they unite public authorities, infrastructure operators, industrial players, national ITS associations and individuals together to enforce the implementation of ITS. Japanese government has also taken actions to promote the ITS deployment. Over 1000 RSUs have been installed mainly along a highway, and they serve passing-by vehicles based on the 5.9 GHz Dedicated Short Range Communications (DSRC) spectrum in Japan [12]. In industry, worldwide automakers, e.g., BMW, GM, Volvo, Toyota and Honda, have developed V2V communication testbed systems.

With prevalent personalized applications, multiple types of content can be delivered in VSNs, such as real-time news, weather report, movies and music. Since vehicles have opportunities to share information with others during their short contact time, an urgent demand for feasible and efficient content dissemination strategies is increasing. It addresses not only end-to-end delay, resource consumption and transmission efficiency, but also users' satisfaction based on their interests and preferences [13]. Apart from the convenience brought by VSNs, some challenges are caused by their highly dynamic topology. For example, continuous changes of the network topology may cause ineffective and interrupted communications; the vehicle truthfulness is hard to estimate since relationships among vehicles may be temporary; attackers may collude with RSUs to control the network operation without the awareness of vehicles [14]. Therefore, the individual privacy may be leaked and exposed to the malicious participants, resulting in a personal loss more or less.

A. Prior Related Surveys

Recently, the state-of-arts of VSNs are reviewed in some survey papers. The majority of existing researches focus on applications, communication architectures and social relationships of vehicular networks [5], [8], [15]–[17]. For example, VSN is viewed as a specific instance of Mobile Social Networks (MSNs) in [15], and is applicable to safety improvement, traffic management and infotainment. A comprehensive study on social inspired vehicles, communication techniques and potential applications is presented in [8]. Particularly, Alam *et al.* [16] identify the social structures of VSNs and highlight their relationships and interactions. VSNs are introduced from the perspective of communication architectures and prospective applications in [17]. In addition, Ning *et al.* [5] mainly study the mobility patterns in VSNs.

Some articles address the privacy and security in vehicular networks, mainly for VANETs. Qu *et al.* [11] classify the security threats to VANETs, and specify the security requirements and the secure process along with its involved authentication approaches. The privacy and security requirements for Location-Based Service (LBS) in vehicular networks are analyzed in [18]. In particular, the privacy enhancing approaches and cryptographic techniques are studied to guarantee location privacy for vehicles. Possible traffic monitoring and privacy

issues for vehicular networks are discussed in [19], while security services and their countermeasures in vehicular networks are investigated in [20]. Fog-based vehicular crowdsensing as well as its infrastructure, promising applications, privacy and security requirements are studied in [21]. Privacy-preserving schemes for ad hoc social networks from 2008 to 2016 are surveyed in [22], especially for the common issues related to MSNs and VSNs. Jin *et al.* [23] outline the architecture of VSNs, and investigate the privacy and security requirements for vehicular networks.

Furthermore, a couple of researches focus on recent advance for data dissemination in the context of VSNs. Information-centric networking in vehicular networks is studied in [3], including content retrieval, data caching and multicast support. Communication and application challenges in VANETs are surveyed in [24], where a qualitative comparison among some general protocols is provided. Chaqfeh *et al.* [25] summarize the existing data dissemination approaches and modeling technologies in VANETs. In addition, optimization methods under the push and pull modes are studied. The content delivery solutions in VANETs are classified into four categories: delivery scheduling, content announcement, reverse request path and periodic broadcast according to their architectural design [26]. Mezghani *et al.* [27] provide a general process for content dissemination solutions in VSNs, including three steps, i.e., information processing, content delivery and performance evaluation. Yang and Wang [10] study the direct and indirect trust modeling approaches from the perspective of social networks, and discuss the research challenges to achieve trustworthy information sharing in VSNs. Despite the fact that some researches have provided overviews of VSNs from different aspects, no prior comprehensive survey has discussed the unique characteristics of privacy-preserving requirements and solutions for content dissemination in VSNs.

B. Contributions

To the best of our knowledge, this article is the first survey to provide a comprehensive review of existing researches on privacy-preserving requirements and solutions for content dissemination in VSNs. Specifically, the contributions of this article are as follows:

- We first introduce the specific characteristics of VSNs by comparing them with MSNs, Online Social Networks (OSNs) and Social Internet of Vehicles (SIoV). In addition, we also analyze the characteristics, typical scenarios and routing methods for content dissemination in VSNs, based on which the factors related to privacy exposure for content dissemination in VSNs are discussed.
- We analyze the unique privacy issues for content dissemination in VSNs, and discuss how to cope with them based on the current network structure. In addition, we investigate the potential attacks for content dissemination in VSNs, and classify them based on the network structure and attack targets, i.e., Onboard Unit (OBU) attacks, RSU attacks and server attacks.
- We summarize various approaches and countermeasures for privacy-preserving content dissemination schemes in VSNs. We also refine the general models and processes for each kind of solutions, and provide the corresponding learned lessons. A side-by-side comparison is provided for the state-of-arts of privacy-preserving schemes in VSNs.
- We discuss the research challenges of privacy-preserving content dissemination in VSNs, and highlight the future research directions regarding privacy requirements and principles in distinct aspects of VSNs.

C. Methodology

The purpose of this survey is to summarize the existing approaches of privacy-preserving content dissemination for VSNs in a structured and comprehensive manner. In particular, we explore the specific characteristics of packet forwarding, privacy requirements and solutions for content dissemination in VSNs under the circumstances that some vehicles exhibit malicious behavior to pursue benefits through attacking or disrupting network rules. In Section II, we introduce content dissemination in VSNs with the purpose of stating the necessity of designing privacy-preserving content dissemination mechanisms in VSNs. Specifically, we study VSN characteristics, content dissemination in VSNs, and the factors affecting the privacy in VSNs. Next, we analyze major privacy concerns and potential attacks for content dissemination in VSNs in Section III, aiming to state their privacy-preserving requirements. In particular, we classify potential attacks into three types according to the architecture, major components and attack targets of VSNs, i.e., OBU attacks, RSU attacks and server attacks. The privacy issues and potential attacks are summarized. Furthermore, we study privacy-preserving solutions for content dissemination in VSNs in Section IV, mainly including seven kinds of countermeasures: pseudonym schemes, cryptographic solutions, signature schemes, trust establishment, game theoretic approaches, location-based solutions and physical layer security techniques. We also provide a comprehensive comparison among these schemes. We believe that this survey can provide a guideline for readers devoting to VSN research to effectively deal with privacy concerns for content dissemination-related vehicular applications in smart cities.

In the following sections, we elaborate on each aspect described above and discuss the related issues. We first describe the special characteristics of content dissemination in VSNs in Section II. Then, we investigate the privacy issues and potential attacks for content dissemination in VSNs in Section III, followed by the corresponding solutions in Section IV. The research challenges and guidances are stated in Section V. At last, we conclude this survey in Section VI.

II. Content Dissemination in VSNs

Content dissemination is of great importance for information sharing among vehicles in VSNs. In this section, we deeply analyze the characteristics of content dissemination in VSNs. We describe the characteristics of VSNs by making comparison with MSNs, OSNs and SIoV, followed by illustrating the unique characteristics of content dissemination in VSNs. Then, we summarize routing strategies in VSNs. At the end, we overview influence factors for privacy in VSNs.

A. Characteristics of VSNs

The concept of VSNs is first proposed in [28], where a VSN-based system (named RoadSpeak) is designed to allow vehicles to automatically join VSNs along their daily routes. A communication protocol is provided for drivers and passengers to participate in the discussion of a voice chat group. Next generation intelligent vehicles and main features of VSNs are discussed, including the emerging technologies, social characteristics, network formulation, main issues and challenges [8]. Generally, VSNs can be viewed as a kind of social networks, involving human factors, such as the connections and social relationships of drivers and passengers. Such networks can be utilized for users to socialize on roads, communicate and share data with others in other vehicles, and even join in different discussion groups.

Generally, VSNs can be divided into three categories: content-based VSNs, position-based VSNs and relationship-based VSNs. Content-based VSNs are networks that vehicles can access based on relevant discussed topics, e.g., the traffic condition, discount shopping information and strategies for playing games. For position-based VSNs, a vehicle can decide whether to access a network when several VSNs are in its neighborhood. In addition, when the vehicle moves away from a VSN, it can decide whether to maintain the relationships with other network members. The driver or passengers in a vehicle can also access a relationship-based VSN with common interests, e.g., workmates or members in a social community.

In order to deeply understand the characteristics of VSNs, we compare VSNs with three similar kinds of networks, i.e., OSNs, MSNs, and SIoV. For OSNs, users are always static, and they do not need to walk around to contact with each other, since the link between two participants is fixed and does not change. The online relationships are always built upon individual relationships in real-world, such as family members and classmates. Users can also access the network whenever they want and wherever they are.

In an MSN, users walk around by carrying mobile devices, and their speeds are normally slow. The contact durations are longer than those in VSNs, since MSN users gently leave the signal coverage. As a result, the topology range of an MSN is small, since mobile users just walk around a campus or a few streets due to their limited speeds. Typically, nodes are formed by mobile terminals, such as smart phones and tablet computers. They are with limited hardware and power, such that nodes may drop packets or deny relaying messages for others (named as selfish behaviors). MSN communications are generally in a node-to-node form.

SIoV mainly focuses on network connectivity and sustainability, while involving some human factors to realize network functions, e.g., data sensing and collection, routing planning, traffic management. Therefore, in SIoV, vehicles are the major social entities and adopt certain social attributes to establish V2V and V2I communications.

In a typical VSN, vehicles on the highway move at a high speed, and the contact duration is quite short (even in seconds). With high mobilities, network topologies are dynamic. The topology range of a VSN is larger than that of an MSN, since vehicles move around a city or an urban area. It is difficult for a vehicle to establish social ties with others, because vehicles on roads may be strangers and only have a temporal relationship. All types of intelligent vehicles, including the bus, car and taxi, can be involved into VSNs. Typically, vehicles are with strong powers and large storage capacities. The communication mainly occur among vehicles, or between vehicles and infrastructures.

In order to deeply understand the characteristics of VSNs, we take daily travel routes of a vehicle as an example. When a vehicle moves along the path from home to office in each morning, it can access various kinds of VSNs. For instance, it can interact with other vehicles towards the same direction for a short time to share interesting information, e.g., the discount shopping information in content-based VSNs. When a vehicle comes across a traffic accident in a special position, it can broadcast a message to other vehicles through beacon information to inform them about road conditions in location-based VSNs. When the vehicle approaches the office, it can interact with workmates to assign tasks or receive reports through relationship-based VSNs.

For a VSN, a vehicle can access it not only by traditional V2V and V2I communication patterns, but also by V2X communication mode, e.g., vehicle-to-pedestrian and vehicle-to-sensors. In addition, when a vehicle decides to join in a VSN, it can send a *request* message. If the message is accepted by the network manager, the vehicle joins in the VSN for a limited time period according to its journey and location. A vehicle can also establish a discussion group, specify the related topic and define the access policy for other vehicles.

As demonstrated in Table I, we summarize the above distinctions among VSNs, MSNs, OSNs and SIoV from five aspects: topology-based, social-based, node-based and privacy-based characteristics and applications. Topology-based characteristics are defined by the features of network topology, while the socially-based ones are based on social relationships and node behaviors. Node-based ones are about the properties of clients.

Overall, VSNs are a kind of social networks for individuals based on vehicular communication technologies, including V2V and V2I communication patterns. Their topologies are high-dynamic, and the communication is affected by vehicles' mobility. The social relationship is established based on common interests instead of real-world relationships. The application for VSNs is to allow drivers and passengers to socialize on their roads.

B. Characteristics of Content Dissemination in VSNs

Content dissemination in VSNs refers to the delivery of information or relevant contents, e.g., traffic alerts, real-time news and service advertisements, to interested individuals. Generally, it relies on two kinds of strategies: push and pull. In a push strategy, information servers initiate a communication request, while a pull strategy makes customers act the role of a communication initiator. In addition, both periodic and aperiodic communications are available. Specifically, a

TABLE I
THE COMPARISON AMONG VSNS, MSNS, OSNS AND SIOV

Network	Topology-based characteristics				
	Node mobility	**Contact/link duration**	**Internet access**	**Topology changes**	**Coverage area**
VSNs	High speed	Short	RSU	High dynamic	A whole city, urban area
MSNs	Low speed	Long	Base station	Dynamic	A campus, part of a city
OSNs	No speed	Unlimited	Routers	Constant	Almost anywhere
SIoV	High speed	Short	RSU	High dynamic	A whole city, urban area
Network	**Social-based characteristics**				
	Social relationships	**Node behaviors**		**Interaction with humans**	
VSNs	Weak	Partly selfish		Mainly depend on the decisions of human beings	
MSNs	Strong	Mostly selfish		Mainly depend on the decisions of human beings	
OSNs	Very strong	Cooperative		Mainly depend on the decisions of human beings	
SIoV	Weak	Partly selfish		Largely depend on decisions of machine, e.g., self-driving	
Network	**Node-based characteristics**				
	Node type	**Resources**	**Communication type**	**Data acquisition**	
VSNs	All kinds of intelligent vehicles, e.g. buses, cars, taxis	Almost no constraint	V2V, V2I, V2X	Interaction with humans	
MSNs	Mobile terminals, e.g. smart phones, tablet computers	Limited hardware, power	Node to node	Interaction with humans	
OSNs	Fixed terminals, e.g. computers	Almost no constraint	Wired link	Interaction with humans	
SIoV	All kinds of intelligent vehicles, e.g. buses, cars, taxis	Almost no constraint	V2V, V2I, V2X	Sensor data collection	
Network	**Privacy-based characteristics**				
	Privacy leak				
VSNs	Safety beacon information exchanges; in-vehicle applications; compromised RSUs and OBUs; semi-trusted servers.				
MSNs	Through third parties; exchange information with others; spammers.				
OSNs	Malware; spammers; phishing site; cross-site scripting attacks.				
SIoV	Safety beacon information exchanges; in-vehicle applications; compromised RSUs and OBUs; semi-trusted servers.				

push strategy is commonly utilized in VSNs, such as the publish-subscribe mode, which enables a published message to be only delivered to the subscribing vehicles whose interests match it. Therefore, the traditional routing algorithm depending on node identifiers does not work, since these identifiers are not specified in messages for applications based on content dissemination. On the contrary, routing algorithms based on message characteristics, such as topics or contents, are desired to be investigated.

The process of content dissemination in VSNs mainly focuses on three aspects: how to treat data/content, how to deliver data/content, and how to record reward or stimulate nodes to relay messages for others. Data treatment is an important preprocessing step for content dissemination, which affects system performance. In order to minimize bandwidth consumption and maintain information quality, contents from multiple sources need to be combined and aggregated, especially beacon messages exchanged among vehicles for safety applications [29], [30]. After receiving the aggregated information, relay vehicles split the data into proper flows and transmit them cooperatively with others to ensure the Quality of Service (QoS), especially for video streams [31].

Data delivery is the necessary process of content dissemination in VSNs, and many investigations have been devoted to this field, e.g., [32] and [33]. Through VSNs, it is possible to achieve flexible communications among vehicles. The process of data delivery requires: a) the knowledge of nodes' locations and pseudonyms; and b) a routing protocol that specifies a packet forwarding method. The development of dissemination technology should be made to match vehicle mobility, communication resources and application requirements [34].

When dealing with relay nodes in VSNs, researches should consider the issue of noncooperative forwarding behavior because of resource constraints, security, and connectivity [35], which usually leads to selfish or even malicious behaviors. Hence, cooperation-based mechanisms have drawn

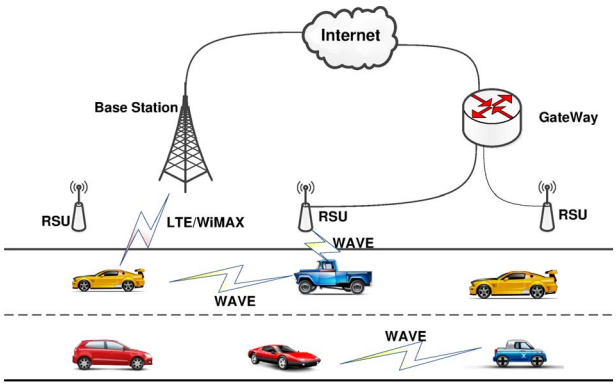


Fig. 3. Network structure for a specific highway.

great attention, aiming to alleviate the problem of selfishness by stimulating selfish and malicious nodes to forward messages based on either incentive or punishment-based mechanisms.

In addition, current studies focusing on content dissemination in VSNs mainly contain two scenes, i.e., highway [36] and urban environments [37], [38]. Fig. 3 illustrates the network structure of a specific highway, while Fig. 4 represents that of an urban area.

Various kinds of information can be delivered to passengers via VSNs, e.g., music, videos and movies, making their trips enjoyable, especially during a long highway journey. Besides traditional V2V and V2I communications, VSNs also support V2X communication patterns currently. V2X represents all types of communication methods applicable to roads and vehicles, e.g., vehicle-to-Internet, and vehicle-to-nomadic (i.e., the communication between a vehicle and a mobile equipment) [39]. For vehicle-to-Internet, Wi-Fi and cellular networks are two promising candidates for the Internet access by RSUs and base stations correspondingly [40]. The cellular network faces several problems for direct utilization in VSNs, although it is the most common method for Internet access of mobile devices with its ubiquitous coverage. First, it is prohibitively costly for downloading bulk data, such as video clips and movie trailers. Moreover, there are severe traffic overloading problems caused by excessive mobile data demands for cellular networks. As a result, offloading a portion of cellular traffic through RSUs is a promising solution. Drive-thru Internet refers to the Internet access provided by RSUs, which has recently drawn overwhelming attention from both academic and automobile industry. However, it may suffer intermittent link connections based on the high mobility of vehicles. Therefore, for the cooperative dissemination of contents in a highway, VSN is necessary and has drawn more and more attention.

Different from highway scenarios where vehicles obtain wireless connections to Internet through fixed RSUs, public transportations in an urban environment can be equipped with Mobile Routers (MRs), which can provide wireless access for mobile users. In Fig. 4, buses are equipped with MRs, and passengers inside carry smart terminals (e.g., intelligent phones and tablet computers) to connect Internet through MRs. When a mobile user gets off a bus at a station, its terminal device switches the wireless connection from an MR to a fixed RSU. The hand-offs in an urban environment are usually frequent when users travel from one access network to another. Consequently, how to guarantee the fluency of traffic flows when users switch the Internet access from one network to another deserves deep investigations.

C. Routing in VSNs

Routing algorithms are important for content dissemination-based applications to deliver information to interested subscribers. For constructing smart cities and ITSs, VSNs are promising platforms to establish temporal connections and spread information between servers and vehicles. The realization of a data delivery framework has drawn much attention. Al-Turjman *et al.* [41] integrate Wireless Sensor Networks (WSNs) and Radio-frequency identification (RFID) tags into a new network paradigm to enable delay-tolerant routing. Heterogeneous devices and nodes can also be leveraged in the network to route data efficiently [42]. The communications among these devices can be formed as a pricing model to meet the cost requirement for relaying resources. To simultaneously meet the requirements of multi-users, WSNs are leveraged to collect information, while data delivery paths are dynamically planned based on cognitive nodes, which can interact with sensor nodes and users [43]. Another routing algorithm considering resource limitation has been proposed in [44] for disaster management. The sensors can be deployed over parking areas, airports and even traffic infrastructures.

The major force to promote the development and innovation of networking technologies is the requirement for various multimedia applications, which poses updated constraints on QoS and Quality of Experiences (QoE) in modern networks, especially VSNs with highly dynamic topologies. Routing protocols are key factors to meet different QoE and QoS requirements of applications. A multi-path routing approach is proposed to satisfy QoS requirements of real-time media in [45]. A mathematical model based on a Lagrangian relaxation method is established to find the optimal path by controlling hop-by-hop QoS. Hasan *et al.* [46] provide a survey of multi-path routing protocols to guarantee QoS for real-time applications. This kind of routing algorithms can improve the utilization of network resources and raise network capacity. In addition, other approaches, such as caching for fog computing to guarantee data fidelity and reduce the delay of requested information, can also be utilized to guarantee QoS requirements [47], [48].

For routing algorithms, secure data access and communication are important to keep users' privacy and data integration [55]. Currently, dozens of researches have focused on security-based methods, such as error detection, secure authentication and communication. A security-based Device-to-Device (D2D) communication framework is proposed to guarantee a secure communication environment by introducing a jamming service to disturb eavesdroppers [51]. Hierarchical interactions between two different service providers are modeled as Stackelberg games. A novel error detection algorithm

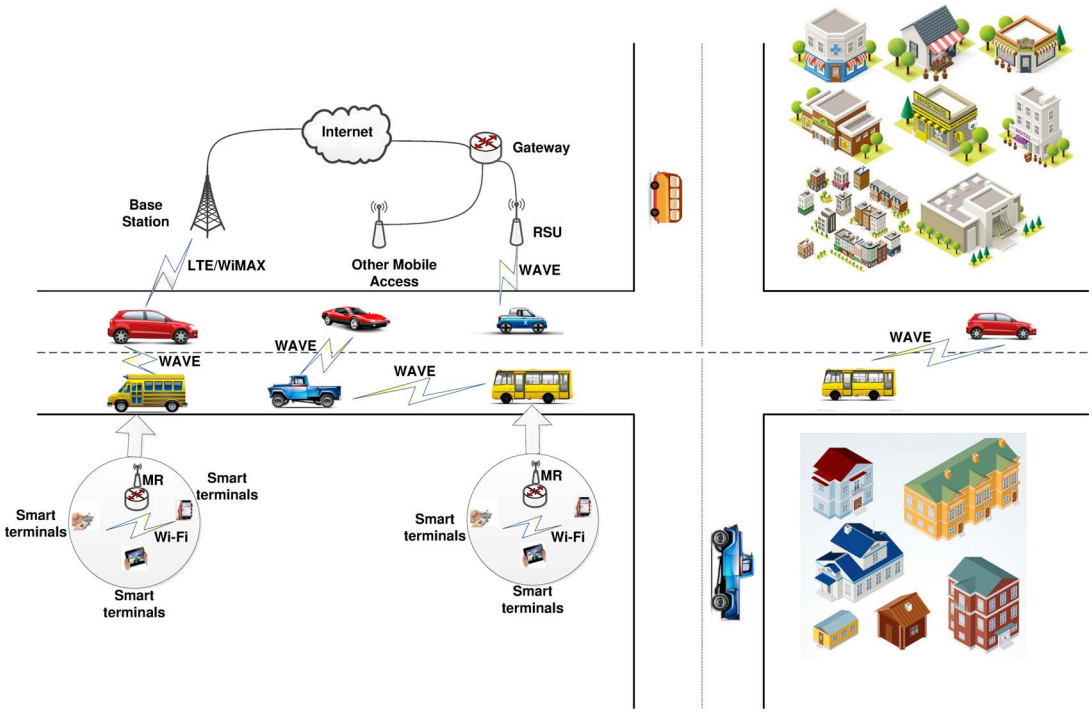


Fig. 4. Network structure for an urban area.

is presented in [52], which has a low computational complexity and is suitable for wireless mobile networks. Compared with traditional correction codes such as Hamming, it not only decreases encoding computational loads, but also lowers decoding loads. Al-Turjman *et al.* [53] design a security-based authentication approach based on elliptic curve and bilinear pairing cryptosystems in a mobile communication environment. It can resist several kinds of potential attacks, such as key impersonation and password guessing. Different from a single authentication mode, mutual authentication based on a Hashing function is proposed to provide a secure interaction for each pair of users in a healthcare application [54]. It reduces the time consumed for authentication in each interaction in comparison with the prior methods. We compare the characteristics of these routing-relevant algorithms in Table II.

D. Influence Factors for Privacy in VSNs

For VSNs, privacy problems are caused by many factors. With the emergence of intelligent vehicles and the development of Internet of Things (IoTs), many potential attacks may be launched by adversaries. In the following, we discuss several situations that may expose private information and are vulnerable to attackers.

Exchanging warning and beacon messages: In order to be detected and communicate with other vehicles, the beacon messages including the real-time locations are periodically broadcasted by vehicles [56]. Therefore, one of the most important issue for designing a location privacy-preserving scheme is to guarantee the QoS requirement, especially for traffic efficiency and safety applications that require frequent state update. As shown in Fig. 5, vehicles *A* and *B* periodically exchange beacon messages to obtain information, including exact vehicle location and speed. If a global external eavesdropper keeps monitoring vehicles' wireless communication channel, they can be easily tracked. For example, Ying *et al.* [57] and Emara *et al.* [58] consider that a global attacker launches a passive attack to collect pseudonym information and obtain location traces of vehicles in a network. A trade-off is made between QoS and location privacy in [58], while dynamical mix zones are formed to support a pseudonym changing process in [57].

Interaction with the cloud: With the development of ubiquitous computing, cloud and edge computing are promising for vehicle-based services, e.g., real-time navigation, which requires intensive computing resources. However, cloud servers are always semi-trusted and curious about the private information stored in the buffer. In addition, the malicious entities can upload fake information to a cloud server to mislead it to make false decisions. For example, vehicle *D* can send fake information to the cloud server through RSU_j in Fig. 5. A privacy-preserving data forwarding scheme is proposed by establishing an outsourced aggregated transmission evident in cloud-based IoT systems [59]. The cloud server can compute the evidence by a selected symmetric homomorphic mapping in the ciphertext domain without revealing any plaintext. To resist attacks where malicious nodes upload fake information to a cloud server, a privacy-aware incentive scheme is proposed for cloud-based VSNs [60]. Normal vehicles collaborate with RSUs to take photos in the location of interest and anonymously send them to the cloud infrastructure. By using appropriate keys and pseudonyms to sign and encrypt messages, a secure communication environment can be created between clouds and vehicles.

TABLE II
ROUTING PROTOCOLS IN VSNs

Ref.	Design objective	Proposed solution	Application				Application scenario
			Industrial Internet	Green cities	Disaster management	Smart cities	
[41]	Providing an optimized framework for node placement and delay tolerant routing	Linear optimization under load balancing and link-capacity constraints	×	×	×	√	Context-aware services
[42]	Data routing based on the integration of heterogeneous IoT nodes	An adaptive routing approach to dynamically launch communication among users	×	×	×	√	Context-aware services
[49]	Data delivery while satisfying the quality-of-information requirements of users	Leveraging learning and reasoning strategies in the network	×	×	×	√	Quality-of-information-aware services
[44]	Message forwarding in large-scale networks	Leveraging learning and reasoning strategies in the network	×	×	√	×	Message forwarding among energy-constraint devices
[45]	Selecting an optimal path to deliver radio resources for intensive media	Adaptive switching control among QoS-based routing schemes by the Lagrangian relaxation method	×	×	×	√	Multimedia applications
[50]	Cognitive caching for fog computing	A replacement approach by considering values of contents	×	×	×	√	Content-oriented services
[51]	A secure D2D communication framework	Hierarchical interaction exploitation for the D2D transmitter and the base station based on Stackelberg games	×	√	×	×	Energy-constraint services
[52]	A forwarding error correction scheme for IoT applications	Designing a simple error correction code with low complexity	×	√	×	×	Energy-constraint services
[53]	User authentication for mobile users	Building cryposystems based on bilinear pairing and elliptic-curve encryption technologies	×	×	√	×	Post-disaster management
[54]	A context-sensitive identity provisioning framework	A secure mutual authentication approach based on a Hash function	√	×	×	×	Healthcare applications

("√" if the protocol satisfies the property, "×" if not)

Information sharing with common-interest vehicles: When a vehicle joins a VSN or communicates with other vehicles through V2V communication patterns, it is not avoidable to share contents with others. If an adversary compromises a member in VSNs, it may obtain potential private information of network members based on the exchanged messages. As illustrated in Fig. 5, vehicles C and D meet at a social-spot, e.g., outside a shopping mall, and they can share the discount or new-arrival information of the commodities based on their common interests. Thus, if vehicle D is malicious, it can infer individual information of vehicle C from their exchanged content. To achieve conditional privacy preservation for drivers and passengers, a privacy-preserving data forwarding algorithm based on personal-social behaviors is proposed in [61]. Anonymous credentials are utilized, which allow an authenticated vehicle to anonymously send messages to others. When a vehicle receives a message, it can retrieve the message without exposing the personal information to the adversary. The misbehaving vehicles can also be traced by Trusted Third Authority (TTA) in the system.

Emerging mobile applications: With more and more mobile or vehicle-based applications popping up, they bring convenience and efficiency for users. The negative side is that they may violate the privacy requirements of users. Adversaries can discover bugs of an application, and launch attacks to get useful information for their malicious purposes. For instance, vehicle D can leverage intra-vehicle applications to achieve different purposes, including navigation, video watching and information broadcasting, as shown in Fig. 5. If an attacker compromises the application server or implants a virus, the private information can be leaked without attention. To improve the privacy level and application utility, a privacy mechanism can be decoupled from the application logic and deliberately managed by another TTA [62]. Different privacy mechanisms can be binded with applications in a user's mobile terminals, acting as plug-in components. External behaviors and information flows of applications can be monitored by privacy-safeguarding components [63].

Increasing number of electric vehicles: As the next-generation vehicles, electric vehicles will play dominant roles to relieve environmental pollution [64]. The privacy-preserving charging management is necessary to satisfy their security requirements. As shown in Fig. 5, a secure communication between electric vehicles and the charing infrastructure should

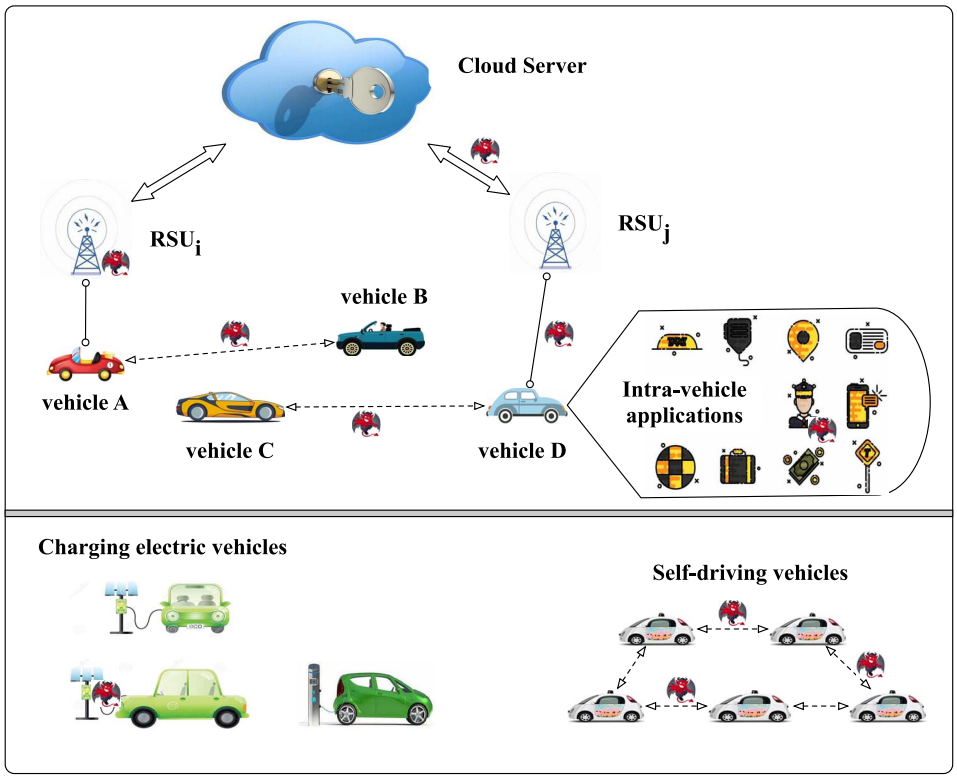


Fig. 5. An example of threats in VSNs.

be guaranteed for proper billing and efficient charging. If a malicious vehicle pretends to be a normal one by using another legal identity, the charging fees can be transferred to a legal vehicle, resulting in the decrease on the utility and extension of a charging service. To overcome the above drawbacks, an efficient authentication protocol is proposed for charging pads to authenticate electric vehicles' identities [65]. It allows them to charge among different charging sections, and a fast authentication algorithm based on vehicles' locations and symmetric keys is designed for moving vehicles. Different from sending charging requests to a global controller by vehicles, a local charging scheme for decision making based on a publish/subscribe communication framework is proposed to avoid information exchanging between vehicles and the global controller [66]. Therefore, vehicles' information, such as location and identity, cannot be released through communication processes.

Vehicles with the ability of self driving: Many researches are investigating the ability of self driving or auto parking of vehicles (e.g., [67]). This ability can largely reduce the requirements of drivers and play as an assistant for intelligent driving. Nevertheless, an attacker can compromise the information source used to determine the location and make plans on the trajectory of an automated vehicle [68]. In addition, when a vehicle detects an obstacle (may be a person) on roads, the vehicle can record it and report without the consensus of the involved person, which violates individual privacy. Therefore, it is desirable to investigate approaches to guarantee security for communications of self-driving vehicles. A system is established in [69] to protect the inter-communications among self-driving vehicles, as illustrated in Fig. 5. Packet dropping attacks can be detected by designing a mechanism based on fuzzy Petri nets. Another effective method to protect vehicles from attacks is a collaborative decision-making technique, where a group of vehicles are available and they coordinate with each other. A vehicle in the group can monitor the behavior of others and check anomalies based on the received data from the group members [70].

Therefore, some principles should be followed when designing content dissemination approaches in VSN systems: 1) the privacy of vehicles should be kept; 2) individual privacy in the semi-trusted third parties should be protected; 3) the security of communications among vehicles should be guaranteed; and 4) the vehicle acting as a proxy or router for passengers to access Internet should be trustful.

This section mainly presents the characteristics of content dissemination in VSNs. When designing a scheme in VSNs, we should take the short communication duration, the establishment of relationship and trustiness, and highly changes of locations into consideration. Overall, the privacy issues for content dissemination in VSNs are complex since the usability of VSNs is in contradiction with the privacy requirements.

III. Privacy in VSNs

Privacy issues are the primary concerns for the application of VSNs. Malicious entities may launch attacks and even reveal users' privacy-sensitive information to pursue profit. With the increasing security awareness of individuals, privacy

must be guaranteed to ensure the willingness of users for participation. In this section, we focus on the privacy requirements and provide a detailed analysis for VSNs.

A. Privacy Issues

The privacy-preserving concern has grown as an unprecedentedly urgent issue, since unauthorized data disclosures harm users' benefits. Regulators in Australia, Canada and the European Union enforce comprehensive laws, which govern the collection, dissemination and utilization of private information. Those in the United States rely on sectoral laws by focusing on specific sectors, including banking, education and health care services [71].

The emphasis on privacy includes three aspects: a) sensitive data; b) controlling methods for the disclosure of sensitive data; and c) methods to protect entities (e.g., the original owners or creators of a message) from being affected by the disclosure [72]. Because of the social relationship establishment pattern and message exchange mode in a VSN, the privacy concerns mainly arise from three aspects: location and trace privacy, personal and common interest privacy and community privacy. In the following, we provide a deep analysis of these aspects.

1) Location and Trace Privacy: With the purpose of keeping safety, real-time locations, speeds and acceleration of vehicles need to be broadcasted periodically by authenticated safety beacon messages through a control channel [73]. Surrounding neighbors would be aware of other vehicles' position and dangerous situations by these beacon messages, while threatening the location privacy of vehicles [74]. An LBS provides spatial data for drivers through some Location Providers (LPs) [75]. For example, a driver can query like "where is the most popular coffee bar near this shopping mall?" or "Is the traffic busy on the 1st Avenue?". However, semi-trusted LPs may reveal individual privacy including locations and profile information, which makes attackers easily initiate attacks, e.g., Sybil attack.

Consequently, there should be a trade-off between the location privacy and utilization for applications [76]. When considering location privacy in a VSN, we can analyze: a) communication among vehicles, and b) information between third parties and vehicles. A communication system is designed to avoid the eavesdropping of adversaries, such that these adversaries are unable to track the traces of vehicles [77]. It allows users to retrieve nearby Points of Interest (PoI) without disclosing their vehicles' exact locations to LPs.

2) Personal and Common Interest Privacy: Interest privacy is regarded as an important privacy requirement for vehicular communications in [78]. It allows a vehicle to identify others with the common interest, and protects the common privacy of vehicles from others with different interests on the road. Users' social attributes are leveraged in a possible socially-assisted solution, based on which the dissemination strategy along with privacy mechanisms can be designed in a mobile environment [79]. Transaction privacy is considered in [80], where a trade system is established in VSNs. An iterative double auction mechanism is utilized to maximize social welfare during the transaction process. A service-access system is designed for common interest privacy in [81], focusing on quality optimization and reliability assurance. Social relationships among vehicles are estimated based on a dynamic access service evaluation scheme.

3) Community Privacy: Community privacy and privacy threats (e.g., adversarial community detection) have been discussed in [82]. The leakage of community privacy is defined as the situation that users from the same community can be linked, and their social relations are exposed. For instance, an eavesdropper may learn whether a user passing by a shopping mall belongs to a community in a rich neighborhood. Furthermore, community privacy also affects data and location privacy, because it is easy for an adversary to infer information about an individual if his/her community privacy is revealed. Du *et al.* [83] establish a game theoretic framework to model the interactions and influence the decisions of users for privacy protection.

4) Other Privacy Issues: Despite the above three privacy issues, many studies focus on other privacy aspects. For example, identity privacy is considered in [84], where a dual authentication algorithm is developed for privacy-preserving and security in VSNs. It requires that the real identities of vehicles should be kept secret from the unauthorized entities in the network. For various applications in VSNs, the identity of a vehicle is always sent to other vehicles or RSUs in plaintext. By monitoring communication channels, a powerful adversary can track a vehicle based on its identity. The leakage of traveling routes may result in serious consequences.

A secure mechanism to keep data privacy for big data collection in large scale networks is put forward [85], aiming at improving security performance. During the data collection process, two different secure protocols are investigated, while a distributed scheme is designed for data storage. Therefore, data privacy not only refers to the content, but also relates to the way that vehicles interact with each other in content exchange. Vehicles may prepare to share their information with some specific receivers in some cases, while keeping them undisclosed to others.

Therefore, we discuss the primary privacy issues in this article, and much efforts deserve to be made in VSNs to discover plenty of unexploited areas. The summarization of privacy issues is listed in Table III.

B. Potential Attacks

Although VSNs offer facilities to users via applications for security, driver assistance, passenger comfort and online entertainment, the wireless medium has its own drawbacks due to open access, making them vulnerable to various attacks, such as jamming, eavesdropping and interference [86]. In addition, given the vehicular network architecture involving seven layers of the Open System Interconnection (OSI) reference model, vulnerabilities and attacks stretch from the physical layer to the application layer [87].

Similar to OSNs and MSNs, VSNs are also exposed to various threats and attacks [88]. The feasibility of attacks is mainly affected by two characters, i.e., the almost unlimited energy

TABLE III
PRIVACY ISSUES

Privacy issue	Ref.	Specification
Location and trace privacy	[73]–[77]	• Refer to the real-time locations and traces of vehicles • Can be exposed based on the periodical exchange of beacon information • A trade-off must be made between the location privacy and utilization for applications
Personal and common interest privacy	[78]–[81]	• Allow a vehicle to identify others with the common interest • Require protecting the common privacy of vehicles from others with different interests on the road
Community privacy	[82], [83]	• Refer to the common information and social relations of users from the same community • Should not be linked by the users not belonging to the same community
Other privacy	[84], [85]	• Refer to other privacy issues, such as traditional privacy concern in VANETs including identity privacy and data privacy

of vehicles along with the strong computing and processing capacities of OBUs. Thus, some attacks in OSNs and MSNs are impossible for VSNs, e.g., energy attack. However, the dynamic and high speed of vehicles make attackers difficult to be detected. It is also difficult to evaluate the trustiness of nodes based on the weak social relationships among vehicles. Moreover, several classifications of malicious attacks have been proposed in the literature. Some are from the prospect of network requirements [87], and some are at the point of direct participation of network agents [29].

In order to comprehensively understand the communication and operating principles, we classify the potential attacks in VSNs from the view of network framework and major components. In general, we can divide the components of VSNs into three categories: OBU-related, RSU-related and server-related equipments. As a result, we concentrate on the following three types: OBU attack, RSU attack and server attack according to the attack target. In this section, we will provide their detailed analysis.

1) OBU Attack: In a VSN, vehicles are equipped with a unit called OBU, which is able to receive and dispatch messages, display content and interact with drivers [89]. Theoretically, the capacity and power of OBUs are considered to be unlimited. In this article, OBUs refer to both the vehicle and its driver.

We can classify vehicles into three kinds: normal, selfish and malicious ones. Normal ones behave normally and obey the network regulations, whereas selfish ones prefer to help users with close relationships, e.g., classmates and family members. Malicious ones may launch attacks to satisfy their own purpose, and perhaps harm other vehicles' benefits. Due to the lack of total network states and high mobility, vehicles are vulnerable to attacks. The opportunistic contact makes vehicles difficult to authenticate each other. Consequently, OBU attack is relatively easy to launch but hard to be detected.

In this article, we define OBU attacks in VSNs as the case that the attacks are launched by the adversary on the vehicle side, and can directly or indirectly affect the functions or judgments of OBUs. Therefore, we categorize OBU attacks into five classes according to the detailed attack subjects, i.e., eavesdropping, denial-of-request, vehicle-based attack, message-based attack and communication channel interruption.

a) Eavesdropping is a passive attack of which its victims are not aware. The attackers monitor the network, collect information, and try to extract the maximum useful information for their own purposes. From the macro view point, there is no attack target. However, several entities can be the attack targets in the micro view point. For example, traffic analysis attack is a kind of eavesdropping, which intercepts and examines traffic between two vehicles to deduce information from communication patterns [90].

b) Denial-of-request refers to the attack that attackers totally or partly deny to satisfy a sender's request. The attack targets can be viewed as requests from all entities. The black/gray hole attacks fall into this category. In addition, *Promise-then-drop* is also a kind of denial-of-request, in which the attacker first promises to forward packets for other nodes with the objective of receiving a high trust from its neighbors, and then silently drops these packages [91]. *Denial-of-service* attack generally results from black/gray hole attack and invalid signatures, which can be viewed as a kind of denial-of-request [36].

c) The attack targets of vehicle-based attack are mainly vehicles (or OBUs). Attackers can directly compromise a vehicle, or tamper its reputation, rewards and other related information to make profits from normal vehicles. Targeting-oriented node compromise attack is a kind of vehicle-based attacks and is developed based on node compromise attacks, since the attacker is able to compromise nodes by observing network conditions [92]. Edge insertion attack refers to the case that a malicious node attempts to forge a sybil node for winning extra rewards in the system [93].

d) Message-based attack targets at transmitting messages to modify the content, inject even fake and false messages. For example, FINE considers the attack that modifies the communication data between LBS providers and honest users [94]. Content modification attack is considered in [93], in which attackers try to tamper the content of the report messages containing the information like the receiving and transmitting time.

e) Communication channel interruption is defined as the attack to disrupt the communication channels, e.g., jamming attack, aiming to block the exchange for beacon messages by broadcasting interfering radio signal in the communication channel [95].

2) RSU Attack: RSUs are installed along roads, serving as intermediate interfaces for vehicles and servers. They have numerous authorities granted by servers, including updating keys, to provide Internet access and authentication for vehicles and so on. They also serve as gateways to deliver information to valid OBUs. As a result, compromising an RSU can benefit attackers a lot, because attackers can easily obtain users' private information containing identity, tracing, preference and so on. Furthermore, this kind of attack is not easy to be detected and vehicles do not have the ability to validate RSUs.

We define RSU attacks in VSNs as the ones that are launched on the intermediate interface, which not only refers to RSUs, but also includes other kinds of wireless and cellular access points. Currently, RSU attacks mainly include two kinds: compromise and impersonation. If an RSU is compromised, it can play a role as an internal adversary and has the same target with the external one, such as observing the identities and locations of other vehicles, and even capturing or modifying the message content. If an attacker launches an impersonation attack, it pretends to be a valid RSU. The unauthenticated OBUs lack the ability of validating the identity of an RSU, and may be easily cheated by a fake RSU.

A method to resist RSU compromise attack has been proposed in [96]. An innovative system model for a 5G-enabled vehicular network has been investigated, which enables security and privacy-aware real-time video reporting services. In the studied system, vehicles acquire a group of short-lived pseudonyms and communicate with RSUs to renew them later. If an RSU is compromised, the pseudonymous-based certificates can be linked with the real identity of a vehicle on target by attackers. Pseudonymous authentication schemes have been designed for validating the identity of RSUs. Attacks on RSUs have been considered in [97], which compromises the storage of RSUs. The responsibilities of a normal RSU are: (i) verifying the base and short term pseudonyms, and (ii) providing the base pseudonyms of misbehaving vehicles, and reporting their short term pseudonyms to servers. As a result, the real identity of vehicles may be leaked to the adversary by compromising RSUs.

The study in [98] takes RSU impersonation into consideration. Its primary objective is to allow the utility for verifying vehicles' message integrity, and also to check the identities of senders for correct billing. Authentication of vehicles alone is not enough, because an attacker may impersonate an RSU without further authentication. Consequently, authentication between vehicles and RSUs acts as an important security primitive for network operations.

3) Server Attack: In a typical VSN network, there may exist several TTAs served as servers. Generally, TTA is a trusted management center. It plays a role as a registration and certificate management center for vehicles and RSUs, and provides various value-added services. The region in the network can also be divided into several domains by TTA, and it can generate secure materials and send them to RSUs in the domain through a secure channel. As a result, TTA is assumed to be powerful with sufficient storage capacity and infeasible to be compromised by attackers. However, with the development of hacker technology and the endless desire, the adversary has been seeking efficient methods to compromise servers.

Recently, plenty of researches have developed server attack resistance solutions. SALVE [99] prevents server impersonation attacks even if a remote adversary possesses the secret keys of a target server. It designs a server authentication solution, which overcomes shortages of traditional server authentication methods by using transport layer security and public key certificates. These traditional server authentication drawbacks are caused by TTA compromise and flaws in the current trust models, which commonly employ the public key infrastructure and may result in server impersonation attack. Current methods for mitigating attacks, such as certificate revocation or short-lived certificates, mainly focus on reducing the time window of attacks, while generally neglecting the situation that an attacker may learn the secret key of the server. Fortunately, SALVE takes the location-based proof as a second supplemental authentication method.

A mobile application, named MASHaBLE, allows users to detect and communicate with encountered individuals belonging to the same secret community to avoid server attacks [100]. They use direct peer-to-peer communication based on Bluetooth low energy, to reduce the heavy dependence on servers. Restricted passive adversary is considered in the design of MixGroup in a vehicular network [101]. The restricted passive adversary, such as a compromised service provider, can conduct the attack of location tracking in a certain place. It can eavesdrop RSUs and estimate vehicles' locations. At the same time, the tracking region of the restricted passive adversary depends on the transmission range of vehicles and the distance between two neighbor RSUs. In this section, we deeply analyze the potential attacks in VSNs and provide a summary in Table IV.

IV. Solutions for Privacy-Preserving Content Dissemination

Pursuing to resolve the security and privacy issues mentioned in the last section, many solutions have been proposed. Broadly, current security and privacy mechanisms can be classified into seven main categories: pseudonym schemes, cryptographic solutions, signature schemes, trust establishment, game theoretic approaches, position-based solutions and physical layer security techniques. Next, we summarize the well-known schemes in each category and illustrate their corresponding models. The important notations related to the model established in each category are presented in Table V.

A. Pseudonym Schemes

To meet the specific security and privacy requirements in VSNs, both ETSI 102941-v1.1.1 and IEEE 1609.2-2013 describe the employment of pseudonyms, i.e., each vehicle has a base identity, which is a pre-installed certificate, to request pseudonyms from a certificate authority [19]. Actually, each vehicle uses a pseudonym validated by the certificate authority to sign messages. Therefore, only the signed messages can be accepted.

TABLE IV
POTENTIAL ATTACKS

Potential attacks	Classification	Specification
OBU attacks	Eavesdropping [90] Denial-of-request [91], [36] Vehicle-based attack [92], [93] Message-based attack [94], [93] Communication channel interruption [95]	• Attacks are launched by the adversary on the vehicle side • Directly or indirectly affect the functions or judgments of OBUs
RSU attacks	RSU compromise [96], [97] RSU impersonation [98]	• Attacks are launched on the intermediate interface • Not only refer to RSUs, but also include other kinds of wireless and cellular access points
Server attacks	Server compromise [99] Server impersonation [100]	• Attacks targeting at the server side, such as cloud servers and location-based service servers • Hard to be detected and harmful to the network

TABLE V
IMPORTANT NOTATIONS

Notation	Description
$\overrightarrow{D} = \{d_1, d_2, d_3, ...\}$	A multi-dimensional characteristic vector related to a pseudonym changing process
$\overrightarrow{D^s}, \overrightarrow{D_1}, \overrightarrow{D_2} \subset \overrightarrow{D}$	Different subsets of $\overrightarrow{D}$, respectively
$C_{1,2}$	The cosine-based similarity between $\overrightarrow{D_1}$ and $\overrightarrow{D_2}$
ξ	A small threshold for the cosine-based similarity
$H(\cdot), H^{'}(\cdot)$	Hash functions
V_i	The i_{th} value in a one-way hash chain
MAC_i	Message authentication code of message i
G_0, G_1, G_T	Three additive cyclic groups
q	The primary order of a cyclic group
e	A bilinear map
$K, \mathbb{P}$	The secret key and the public key, respectively
OBU_i	Vehicle i
P, S, U	The set of players, strategies and payoff functions, respectively
$u_i(s), b_i(s), c_i(s)$	The payoff, benefit and cost of player i based on strategy s, respectively
$br_i(s_{-i})$	The best bargain function of player i to the strategies of other players
S^*	A pure strategy Bayesian Nash equilibrium

However, merely employing pseudonym cannot fully solve security threats to vehicles, because vehicles can be re-identified with enough time. Adversaries are able to track the movements of vehicles easily by collecting the signed messages of vehicles at different locations. Therefore, current researches regard that vehicles need to keep a pool of pseudonyms ahead, and they are changed according to certain pseudonym-changing methods.

In a VSN, pseudonyms have a common abstract lifecycle [102], i.e., issuance, use, change, resolution and revocation, as illustrated in Fig. 6. Generally, a pseudonym changing process is always defined by a multi-dimensional characteristic vector $\overrightarrow{D} = \{d_1, d_2, d_3, \ldots, \}$. The factors in $\overrightarrow{D}$ represent the characteristics of vehicles related to a pseudonym process. For instance, $\overrightarrow{D} = \{d_1, d_2, d_3, \ldots, \}$ represents factors $\{Time, Location, Velocity, \ldots, \}$. For an attacker, it can obtain a subset of factors in $\overrightarrow{D}$, where $\overrightarrow{D^s} = \{d_1^s, d_2^s, d_3^s, \ldots, \}$, and $\overrightarrow{D^s} \subset \overrightarrow{D}$. It is considered that, if the adversary monitors two vehicles and gets part of their characteristic vectors of pseudonym changing processes $\overrightarrow{D_1}$ and $\overrightarrow{D_2}$. Then, the cosine-based similarity between $\overrightarrow{D_1}$ and $\overrightarrow{D_2}$ can be computed by:

$$C_{1,2} = \cos\left(\overrightarrow{D_1}, \overrightarrow{D_2}\right) = \frac{\overrightarrow{D_1} \bigodot \overrightarrow{D_2}}{|\overrightarrow{D_1}| \cdot |\overrightarrow{D_2}|}. \quad (1)$$

Obviously, if $\overrightarrow{D_1}$ and $\overrightarrow{D_2}$ are identical, $C_{1,2} = 1$. If $|1 - C_{1,2}| \leqslant \xi$, where ξ is a small threshold, the two changing processes of pseudonyms can be considered as two subsets from a complete process in the eye of the adversary. Therefore, unlinkable pseudonym changing processes are desired to be investigated.

In order to achieve unlinkable pseudonym changing processes, i.e., $|1 - C_{1,2}| > \xi$, a proper scenario that allows multiple indistinguishable pseudonym changing processes to take place simultaneously can be investigated. For example, an effective strategy for a pseudonym changing process with different social spots in VANETs is designed in [103]. The places where vehicles always gather together are called social spots, such as a crossroad and a parking area. If all of the gathered vehicles conduct a pseudonym changing process just before leaving a social spot, all the beacon messages broadcasted by vehicles contain the same items, e.g., *Location* = *current spot*, and *Velocity* = 0. Then, the social spot acts as a role of a *mix zone*, and the individual privacy can be protected.

Another possible solution is expanding the diversity of pseudonyms to avoid their reutilization, which enhances the similarity between $\overrightarrow{D_1}$ and $\overrightarrow{D_2}$. A promising technique is to enable a shuffling process among different entities. Both of researches in [104] and [105] allow RSUs to shuffle the pseudonym sets amongst themselves to maximize anonymity

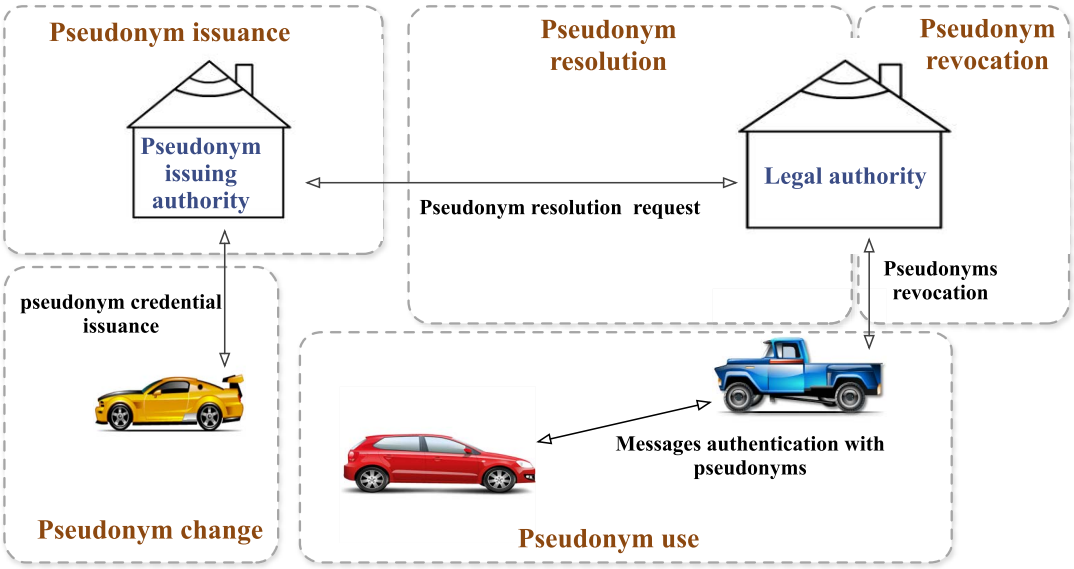


Fig. 6. A common abstract pseudonym lifecycle for VSNs [102].

for vehicles. Specifically, the work in [104] has conducted a framework to provide anonymity for vehicles during the communication process in VANETs. It leverages RSUs to receive the originally generated pseudonym sets from TTA, and then distributes them to vehicles. During some special periods, RSUs shuffle the pseudonym sets amongst themselves. The shuffling process is as follows: each RSU has n pseudonyms to shuffle at each interval. Then, the RSU should send all the n pseudonyms to part or all of the other RSUs, and receive the same number of pseudonyms at the same time. Since the number of pseudonyms given to each RSU is more than the required number, a maximum number of pseudonyms can be set up. Therefore, an optimization issue can be formed, whose objective is to maximize the percentage of pseudonyms received by each RSU. The constraints contain three aspects: a) the total number of transmitted pseudonyms for each RSU is no more than that an RSU has; b) the total number of pseudonyms sent by RSUs is equal to the total number of the received pseudonyms; c) the number of transmitted pseudonyms should not be negative.

Similar to the assumption in [104], each RSU in [105] possesses a pseudonym pool and pseudonyms inside can also be shared among different pseudonym pools. It utilizes a two-sided matching theory to solve the problem of pseudonym resource allocation among different pseudonym pools, where different cloud-based RSUs are enabled in vehicular networks. Different from the work in [104], Huang *et al.* [105] consider some social features in the pseudonym sharing process, e.g., the willingness of RSUs to provide pseudonyms to others. The goal of each RSU is to maximize its utility. The global controller in the central cloud utilizes a two-sided matching allocation policy for pseudonyms.

Integrating pseudonym schemes with public key cryptography is also an efficient approach to improve the anonymity while ensuring the non-repudiation of vehicles by TTAs. ACPN [106] is an innovative authentication framework to provide conditional privacy-preservation for VANETs. A novel pseudonym generation scheme is employed, which ensures that the non-repudiation of vehicles can be achieved by the *pseudonym issuing authority* and the *legal authority*. Even in a privacy-preserving authentication scheme, the generated pseudonyms are used as identifiers, and a *pseudonym change* process depends on the demands of vehicles. *Pseudonym issuing authority* periodically broadcasts the current public keys for pseudonym generation through RSUs. Vehicles can adopt the newly broadcasted keys to generate pseudonyms when necessary.

Based on a public key cryptographic system, PUCA [107] is a full anonymity scheme for honest vehicles, even against *pseudonym issuing authority* and *legal authority*. It authenticates with the *pseudonym issuing authority* and *legal authority* by using anonymous credentials, which not only has little impact on communication between vehicles and RSUs, but is also compatible with the existing standards. A privacy-friendly revocation mechanism is also leveraged to remove misbehaving vehicles from the system, without requiring resolution of pseudonyms. Similar to the process in Fig. 6, it is assumed that *pseudonym issuing authority* plays a role of issuer, while *legal authority* acts as a verifier. When a vehicle intends to obtain pseudonyms, it authenticates to *pseudonym issuing authority* by using a periodic n-show credential with full anonymity. Only up to n pseudonyms can be required during each time period. In traditional schemes, it is possible to construct a one-show credential, enabling verifiers to compute the vehicle's identity. In the *pseudonym issuance* phase of PUCA, each vehicle is issued by n one-show brand credentials [108], containing the current time and an invalidation token as attributes. In the *pseudonym change* phase, the vehicle can obtain a pseudonym certificate valid for the time encoded in the credential, and the attribute in the credential is updated to the next period.

Lesson 1: Pseudonym schemes are widely adopted in privacy-preserving schemes to hidden the real-identity information of vehicles. In order to realize the unlinkability of vehicles, a proper pseudonym changing process can be proceeded to keep the vehicle anonymous. The aforementioned studies mainly focus on four aspects of pseudonym management: executing an indistinguishable pseudonym changing process, pseudonym diversity expanding, pseudonym pool management and the integration of a pseudonym scheme with public key cryptography. Although some efficient privacy protection schemes have been provided in the system, some fields are ignored by the current studies and desired to be investigated further. First, the scalability of pseudonym schemes should be enhanced, since the current pseudonym schemes may be suitable for some special scenarios only. Second, the communication overhead of a pseudonym changing process should be controlled further in VSNs, because the number of vehicles is increasing rapidly and the communication among vehicles consumes large volumes of wireless communication resources. At last, pseudonym change strategies should be adjustable for different privacy-level requirements of applications.

B. Cryptographic Solutions

Modern cryptography offers many security technologies to developers, such as encryption/decryption algorithms, key generation and hash functions. The requirements for different cryptographic primitives can be classified as follows [109]:

- *Confidentiality:* It requires that messages transmitted in the network can only be read by the authorized users.
- *Authentication:* It allows a receiver to verify the received messages.
- *Integrity*: It means that the messages received by the destination are complete, and have not been altered in transmission.
- *Non-repudiation:* It ensures that a node cannot deny what it has done.

In a VSN, the above requirements illustrate that: the messages exchanged in the network should be kept in secret for the consideration of individual privacy; the vehicles should be able to prove their identity and mutually authenticate each other; an attacker should not be able to modify messages; at last, a vehicle should not be able to deny its selfish or malicious behaviors, e.g., sending a false warning message.

Cryptographic solutions for keeping privacy and resisting attacks can be generally classified into two categories, i.e., symmetric and asymmetric cryptography schemes [110]. In the former, a signer uses a secret key to encrypt a message, and the key is always utilized to verify the message by the verifier. As a result, its drawback is that all the involved entities must have access to the secret key, where non-repudiation may be violated. In the latter, each user has a private key and a public key. The private key must be kept in secret, while the public key is always broadcasted to the public [85]. Currently, one of the most frequently used technology based on asymmetric-based schemes in VSNs is identity/attribute-based cryptography, which requires TTA to generate private keys from the attributes or identifiers of vehicles instead of generating keys by vehicles. Most of the identity/attribute-based schemes are based on bilinear maps, generally called pairings. Obviously, schemes based on asymmetric cryptography are more complicated but more secure than the ones based on symmetric cryptography.

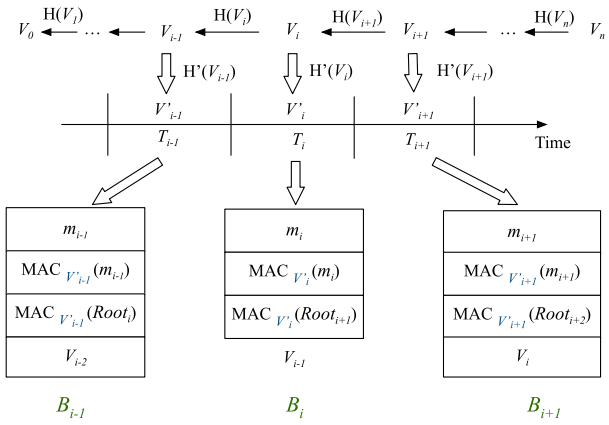


Fig. 7. Generation process of chained keys [111].

Based on symmetric cryptography, PBA [111] is an efficient broadcast authentication scheme, which not only defends against Denial of Service (DoS) attacks, but also resists package losses. It leverages source authentication by one-way hash chains. As shown in Fig. 7, considering a generated chain with *n* values, the algorithm in [112] randomly selects the last value V_n and repeatedly applies the one-way hash function *H*. Its objective is to obtain the previous values, where $V_i = H(V_{i+1})_{\forall i \in \{0,\ldots,n-1\}}$. The beginning value of the chain (V_0) is a commitment for the entire chain and enables the authentication of other values in the chain. Furthermore, a second hash function H' is leveraged to compute the key $V'_i = H'(V_i)$ for the generation of Message Authentication Codes (MACs) during each time period $T_{i,i\in\{0,\ldots,n-1\}}$. Beacon message m_i is broadcasted with the MACs computed by V'_i. When m_i arrives at a receiver, it can verify the beacon sent in the former interval. At the same time, the former beacon carries the prediction outcome for the current beacon message, which makes its verification become possible.

From the above description, we can conclude that though a key generation process for symmetric cryptography is feasible, the authentication process is more complex than that of asymmetric cryptography schemes. Currently, pairing-based cryptography is the most commonly used technology in asymmetric cryptographic-based schemes. It pairs elements in two cryptographic groups to a third group by a mapping method to develop cryptographic systems.

Generally, let G_0, G_1, and G_T be three additive cyclic groups of the primary order q. A bilinear map e is defined as $G_0 \times G_1 \rightarrow G_T$, which satisfies the following properties [113]:

- *Bilinearity:* $\forall a, b \in Z_q^*, \forall g_0 \in G_0, g_1 \in G_1 : e(a \cdot g_0, b \cdot g_1) = e(g_0, g_1)^{ab}$.
- *Computability:* an efficient algorithm is needed to compute *e*.
- *Non-degeneracy:* $e \neq 1$.

Then, the secret keys can be generated based on the above bilinear map. For example, a ciphertext-policy attribute-based encryption (CP-ABE) delegation scheme is studied, aiming at improving the decryption efficiency for vehicles with the help of RSUs in VANETs [114]. When a vehicle detects an event on roads, it can be reported to a traffic management center. Then the center can send encrypted messages to vehicles through RSUs. When receiving these messages, the RSU can dynamically decide whether to delegate the decryption process of messages or not. To achieve data privacy, this scheme encrypts the multimedia messages with an advanced encryption standard, while the message key is encrypted based on CP-ABE. Three keys are generated based on the pairing-based cryptography, i.e., master key, public key and privacy key. Specifically, the private key includes three parts: one is AK, i.e., the "attribute key" for the proxy (e.g., RSU); the second is SK, i.e., the private "security key" for vehicles; and the last is FK, i.e., the "full key" for vehicles.

An Identity-based Batch Verification (IBV) scheme leveraging paring-based cryptography is proposed to guarantee the security and efficiency of VANETs [115]. However, the current IBV schemes exhibit many security risks, e.g., wrong messages and conflicts between privacy and traceability. An improved scheme is investigated to satisfy the security and privacy requirements of vehicles, which only needs a small constant amount of pairing and point multiplication computation. In the system initialization phase, TTA generates the system parameters for all vehicles and RSUs. When each vehicle first registers to the system, a real identity and a password are assigned to it. Then, the vehicle can generate an anonymous identity and a signing key, based on which the messages can be signed. If an RSU receives messages from vehicles, the RSU can proceed a batch message verification process to improve the verification efficiency. Security analysis shows that this scheme can resist attacks, such as forgery, identity privacy violation and anti-traceability attacks. Performance results show that this scheme is efficient in reducing verification delay compared with existing schemes.

In order to ensure secure communication and individual privacy for users in vehicular networks, an innovative conditional privacy-preserving authentication scheme is proposed in [116]. This scheme provides secure authentication based on an elliptic curve cryptosystem for message transmission between vehicles and RSUs. Its advantages in comparison with other paring cryptography-based schemes include: a) any special one-way hash function is not required; and b) the use of pairing operations is not necessary. Only a general one-way hush function is necessary, which consumes less computing time than a special one. Since no pairing operation is utilized during the processes of signature generation and verification, this scheme can perform well on computational delay and efficiency. Meanwhile, security analysis shows that it is robust to the adaptive chosen message attack.

Lesson 2: We elaborate the cryptographic solutions mainly from two aspects: symmetric and asymmetric cryptography schemes. Both of them can provide secure V2V and V2I communications for users. The most dominant issue for cryptographic solutions is their high computational complexity and strict requirements for key update and revocation. Therefore, it is necessary to lower the algorithm complexity of cryptographic solutions, especially in VSNs with a high-dynamic topology where the communication duration of two vehicles can merely last for a few seconds. As we know, the complexity of different cryptographic algorithms is related to distinct security-level. Therefore, distinct complexity-level algorithms should be designed and leveraged to satisfy various application requirements.

C. Signature Schemes

The digital signature is an efficient authentication method for vehicles in the content dissemination process. The validity of the signature can be verified by anyone based on the public keys of the signer. The signature is mainly used for two purposes: one is to enable vehicles to create and prove their own pseudonyms without the help of TTA; while the other is utilized for message authentication [117], [118]. Generally, signature-based schemes are integrated with Public Key Infrastructure (PKI) cryptography technologies, and consists of the following phases.

Setup: TTA computes $P = k \cdot g_1$, where $k \in Z_p^*$ is a random secret, and g_1 is a generator. TTA publishes P as a shared key, and stores k as the secret key.

Extract: A signer requests the secret key from TTA. TTA computes the secret key by $K = kH(\cdot)$, and returns it to the signer through a secret channel.

Sign: A signer generates a signature based on the secret key K by using a suitable signature scheme.

Verify: A verifier employs the signature credentials, the public key of the signature generated by the signer and the public key $\mathbb{P}$ generated by TTA to verify the signature.

However, traditional signature schemes suffer from some problems, e.g., long computation delay in TTA, high computation cost and communication overhead. Currently, researchers devote themselves to finding ways to improve the performance of signature schemes while guaranteeing system security. A location-based authentication and billing scheme is proposed to resolve the security issues in mobile IPv6-enabled vehicular networks [119]. Lightweight hash functions and batch verification are designed for efficient authentication. Only a few signatures are required for a message to reduce computation overhead. In order to reduce the cost of network computation and resources, a novel approach using an ID-based cryptosystem and proxy blind signature over VANETs has been proposed [120]. Mambo *et al.* first propose the concept of proxy signature [121], which denotes that the original signer delegates a proxy signer to sign messages for users. Blind signature is firstly proposed by Chaum [122], which is important for ensuring the anonymity of users. In [120], a proxy blind signature scheme has been studied to protect individual privacy, in which the original signer allows the proxy one to generate a blind signature. The proposed scheme can guarantee message integrity and confidentiality, while lowing computational cost for networks.

An aggregate signature is useful in the case where many different users generate various different messages, and the

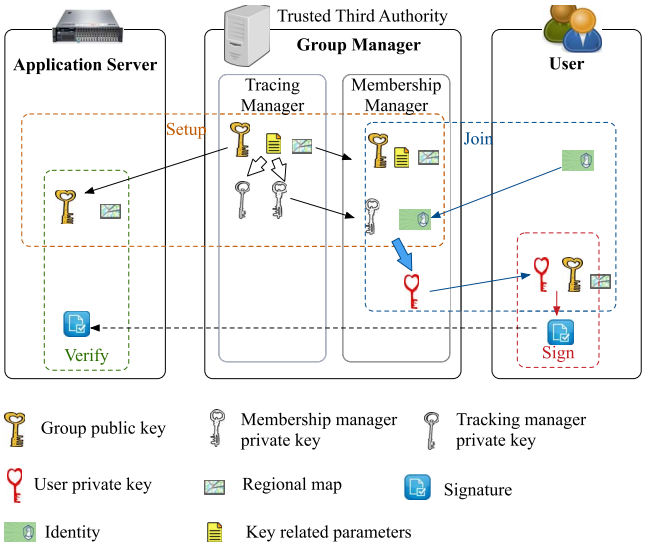


Fig. 8. Generation process of a group signature [124].

signatures on these messages need to be compressed. Its advantage is the saving of bandwidth and computation time in resource-constrained network environments. Recently, a novel certificateless aggregate signature scheme for V2I communication in VSNs has been presented [123]. In the phase of aggregation, an aggregate signature generator, such as an RSU, produces a collection of individual certificateless signatures. Then, the RSU aggregates them together to form a certificateless aggregate signature. Once an application server receives such a signature, it products a batch verification process. It is demonstrated that the proposed scheme can achieve conditional privacy preservation by mapping each message to a distinct pseudonym.

Group signature is commonly employed in VSNs to guarantee anonymous authentication. Messages can be signed by a group member on behalf of its group. As shown in Fig. 8, the generation process of a group signature mainly includes four steps [124]: a) Setup: the group manager generates the group public key and privacy key (including the membership manager private key and tracking manager private key in Fig. 8) based on input parameters; b) Join: when a user joins in the network, group manager can generate a privacy key for the user to sign messages; c) Sign: the valid member can use its private key and group public key to sign messages; d) Verify: a verifier can validate the signature by the group public key. However, long computation delay in signature verification and certificate revocation processes is the main obstacle for the existing schemes based on group signatures. In order to resolve this issue, an efficient privacy-preserving authentication scheme is proposed in [125]. In this scheme, the selected area is divided into several domains, such that RSUs can manage group private keys and vehicles locally. Furthermore, two methods are investigated to reduce time consumption: a) a hash message authentication code is designed to avoid time consumption for certificate revocation list checking; and b) a cooperative message authentication method is designed, requiring each vehicle to verify a fraction of messages only.

Ring signature is a special kind of group signatures, without group managers to setup groups or revoke the identities of signers. A group based on it is formed spontaneously even without the awareness of group members, and its members are allowed to sign messages anonymously on behalf of themselves. Linkable ring signature is introduced in [126], and allows network participants to determine whether two signatures are signed by the same signer. That is to say, if a group member signs only once by the ring signature, the anonymity can still be achieved the same as conventional ring signatures. Otherwise, the signatures signed by the same member can be linked. Then, escrowed linkability is proposed, where two ring signatures remain unlinkable to others except TTA [127]. The property of escrowed linkability enhances the application range of linkable ring signatures, such as spontaneous traceable signatures and anonymous verifiably encrypted signatures. The former allows TTA to track all signatures without revealing other users' identities, while the latter enables a signer to sign a message via an encrypted signature authorized by a TTA.

In VSNs, in order to detect malicious vehicles and exclude fake data, the collected information, including road conditions and traffic accidents, should be signed by vehicles before being delivered to a traffic management server. Ring signature is an efficient scheme to guarantee full anonymity. A road-to-vehicle communication system is established in [128] based on ring signature with relaxed anonymity by focusing on time-dependent linking properties. A vehicle cannot be linked unless it generates many signatures in a special period. In addition, a vehicle's certificates or secret keys do not need to update frequently, which are suitable for a mobile environment. A Sybil attack detection scheme based on linkable ring signatures is proposed for VSNs [129], which is based on vehicles' trajectories for identification while preserving their location privacy. When a vehicle moves into the wireless communication range of an RSU, it demands an authorized message signed by the RSU as its location proof for identification. Since the signed message is based on linkable ring signatures, any two authorized messages signed by the same RSU in the same period can be linked. Therefore, the identities of vehicles can be verified.

Threshold ring signature is first proposed in [130], which guarantees that a minimum number of vehicles in a group must be involved in producing a signature, while the privacy of remaining members can be hidden. A privacy preserving communication framework in VSNs is designed in [131] based on threshold ring signatures. It not only supports reliable announcements to be forwarded in the network, but also allows nondeterministic vehicles to generate signatures and send announcements anonymously in an untrusted environment. To reduce the complexity of threshold ring signature, an efficient threshold ring signature scheme is proposed for anonymous authentication [132]. This scheme generates a signature by solving a group of linear equations. The advantages compared with the scheme in [130] contain: a much lower computational complexity and the same length of the signature for the proposed scheme as that of regular ring signature.

Chameleon signature is generated without interacting with a message's intended receiver, which can resist attacks such as eavesdrop and linkability [133]. A privacy-preserving authentication protocol with authority traceability is proposed to ensure the anonymous message authentication among vehicles [134]. It is developed based on the elliptic curve-based chameleon hashing. However, its disadvantage is that if the public key is stolen by attackers, the unlinkability is no longer ensured. A redesigned chameleon hash signature is further designed to avoid using fixed public keys. The unique characteristic of chameleon signature is non-interactive, representing that a signature generation process can be proceeded without the interaction of receivers. Thus, it can largely improve the authentication performance. The algorithm mainly contains three processes: registration, authentication and tracking phases. The vehicles and RSUs register to TTA and get security-related information in the registration phase. When a vehicle prepares to communicate with an RSU, both of them should authenticate each other by using the security-related information. If an abnormal event happens, TTA can recover the vehicle's real identity by a tracking algorithm. Experimental results show that the proposed scheme can achieve fast verification and keep the system security simultaneously.

Lesson 3: The signature can be an efficient approach to authenticate vehicles and their messages. Many kinds of signatures have been introduced in the literature. We mainly describe several famous ones, including traditional signature, aggregate signature, group signature, ring signature and chameleon signature for different applications. The most commonly used schemes are group and ring signatures, since they have low communication overhead and can be linked when necessary. To reduce the long computation delay for authentication, these schemes are always integrated with batch verification processes. In order to improve the performance of signature schemes, the further work can be focused on: 1) reducing the signature length further to minimize the authentication delay for a wireless and mobile communication environment; 2) investigating whether the designed scheme is feasible for different systems and applicable for real-world devices.

D. Trust Establishment

In a VSN, it is possible to study the trustworthiness among vehicles to create a trusted communication environment. Currently, researches focusing on trust in VSNs mainly include three directions: entity-based trust, data-based trust and combined trust [135]. The entity-based trust schemes focus on the trustworthiness of users by measuring their behaviors, which can exclude the selfish or malicious nodes to ensure the reliable message delivery in vehicular networks [136]. The data-based trust methods always concentrate on the trustworthiness or quality of the transmitted data, in order to remove the fake messages. Entity trust is the prerequisite of data trust, and data trust can enhance entity trust in turn [137]. The combined trust models take advantage of the entity trust to evaluate data trustworthiness. The detailed descriptions of trustworthiness are as follows.

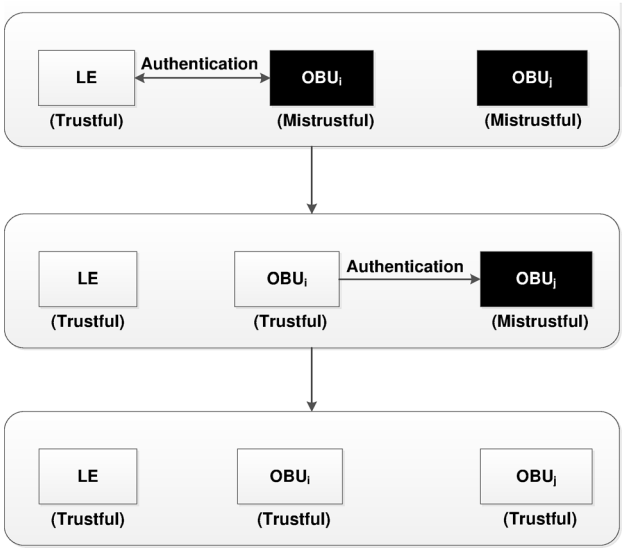


Fig. 9. Transitive trust relationships in TEAM [139].

1) Entity-Based Trust: The existing entity-based trust schemes usually compute trust value or reputation score from direct and indirect trusts. Generally, direct trust is estimated by direct connections in the past, while indirect trust is computed by recommendations from friends or neighbors [138].

TEAM [139] is a decentralized lightweight authentication scheme for V2V communications, which utilizes transitive trust relationships to improve the authentication performance. In this scheme, vehicles are classified into three categories: a Trustful Vehicle (TV), a Mistrustful Vehicle (MV) and a Law Executor (LE). LE is always trustful, and acts as a mobile authentication server. When a normal vehicle is successfully authenticated, it is regarded as a trustful one. In addition, a TV becomes an MV when the certificate expires. The transitive trust relationships in TEAM are illustrated in Fig. 9. Initially, only three vehicles exist in a VSN, i.e., LE and two MVs (OBU_i and OBU_j). After being authenticated by an LE, OBU_i becomes a TV and has the ability to authorize other MVs. When TV OBU_i encounters an MV OBU_j, it acts as an LE temporarily to authenticate OBU_j.

An approach aiming to solve the security problem for vehicles through plausibility and reputation checks is proposed in [140], which ensures security against several attacks, e.g., data aggregation and dropping, event modification and false event generation. When a node intends to forward data via some trusted nodes, it needs to broadcast a *Neighborreq* message and wait for *Neighborrep* messages. When a node receives a *Neighborreq* packet, it checks whether the particular node is in its trust node table. If the trust value of the particular node is 0, the received packet is discarded. Otherwise, the node accepts the message and updates its *Reqseentable*. A reputation-based trust management system is established according to a similarity-based bootstrapping method in VSNs [141]. It takes user behaviors and historic records (e.g., the total driving distance) into consideration to construct the reputation mechanism. A trust evaluation framework based on cloud computing is proposed to evaluate the

trustiness of vehicles in VSNs [142]. Neighbor trust, friend trust and history trust are considered to form an overall trust value of a vehicle.

2) Data-Based Trust: Due to the dynamic nature of the network topologies and message transmissions in VSNs, the existing data-based trust models are often established based on the context of events, and take location closeness, time closeness and event types into consideration.

A trust-based framework for information dissemination with the purpose of guaranteeing safety and reliability in vehicular networks is proposed in [143]. It includes two parts: one uses three security-based checks to ensure that the message is trustful; and the other looks for a safe path to forward messages. Trust is computed according to the service requirements of a certain application, such as anonymity, confidentiality, delay and reliability.

Different from the trust framework in [143], DTM^2 [144] is a distributed model based on the Spence's job market model in economics theory. In this model, a signal is transmitted with a message by the sender, and the signal represents the message trust for potential receivers. For each node, the optimization goal is to maximize the signal value. When a node first enters the network, it receives a specific amount of credit, which can be utilized to pay for the signal cost of sending and receiving messages. Initially, all the nodes have the same credit. If a message is approved by most of the receivers, the credit of its sender can be increased. If a message is regarded as false and refused to be received, the credit of its sender can be reduced. Simulation results show that this scheme can effectively detect and exclude malicious nodes.

3) Combined Trust: In the existing combined trust models, entity-based trust and data-based one always impact each other. The purpose of this kind of trust models is to establish reliable communication links among nodes in the situation that malicious nodes and messages coexist.

PTVC [145] is a privacy-preserving scheme based on trust establishment for cloud computing in vehicular networks. It not only selects the trustworthy vehicles to form a Vehicular Cloud (VC) with disclosure-minimizing privacy, but also checks the computation results from VC. When a vehicle intends to use a VC to offload its computation, it needs to locate the high-reputation vehicles nearby to form a VC. The selection process is as follows: first, the vehicle sets a threshold for trustiness and chooses a pseudonym to compute the requests; second, after receiving the request from the vehicle, a neighboring vehicle needs to check whether the request is sent by the registered vehicle, and determine whether the reputation value satisfies the trust level. If both conditions are satisfied, the neighboring vehicle provides the proof and replies to the original vehicle; At last, after receiving the response from the neighboring vehicle, the original vehicle checks whether the neighboring vehicle is suitable for transmission. In addition, with the purpose of keeping data trust, the vehicle needs to encrypt its data before outsourcing them to VC, and verify the received results. Security analyses show that PTVC is robust against attacks, including reputation spoofing attack, data analysis attack, arbitrary result attack and pseudosyms link attack.

An attack-resistant trust management scheme for VSNs is proposed for attack detection and defense by evaluating the trust values of both data and vehicles [146]. Data trust is computed based on the information sensed and collected by multiple vehicles. Node trust is derived from two dimensions: functional trust, indicating how likely a node can fulfill its functionality; and recommendation trust, showing how trustworthy the recommendation from a node for others is. A Dempster-Shafer theory of evidence is utilized to compute data and node trust. Then, the belief value of an event detected by a node can be obtained. Therefore, the data trust computed by combining reports from different nodes can also be calculated. The proposed combined trust scheme is applicable to multiple applications in VSNs, such as traffic safety improvement, environmental protection and mobility management based on enhanced trustworthiness.

Similar to ART, T-VNets [147] is a solution that focuses on traffic density estimation, trust computation among entities and the distribution of dishonest nodes in a network. Specifically, dishonest nodes can be excluded from the network by combining several trust metrics, including RSU-based, event-based, direct and indirect trusts. It computes a global trust on the basis of different pieces of collected information. In addition, RSUs can play as a TTA to evaluate the current and historical behavior of vehicles. The message format introduced by the ETSI standard is utilized to estimate the distribution of malicious nodes, traffic condition on roads and the credibility of the reported events. Then, the shortest, secure and reliable path can be chosen based on the measured features to deliver messages. Since this scheme is adaptable to environments, it is suitable for both highway and urban scenarios.

Lesson 4: In VSNs, constructing a trustworthy network environment is valuable to guarantee the benign development. The aforementioned studies mainly concern three aspects, i.e., entity-based trust, data-based trust and combined trust. These trust-based schemes can be further integrated with cryptographic and signature techniques to protect individual privacy while establishing available trust models. However, to realize trustworthy VSNs, there are still some issues to be deeply investigated in the further research. For example, in order to establish an efficient trust model, as much as possible information should be collected to analyze the individual behavior. The first question is how to classify and leverage the information to form an appropriate model to determine the trustworthiness of messages. Then, it is challenging to design a suitable algorithm for computing the trust value. The next question is how to extract the indirect trust based on the trust evaluation obtained from others. At last, how to keep individual privacy during the information exchanging and analysis processes is significant.

E. Game Theoretic Approaches

Game theory is a useful tool for multi-entity strategic decision making, and is suitable for modeling the interactions among entities in security issues [148]. The advantages of game-theoretic approaches are the fact that they provide the support for allocating limited resources, balancing potential

risks and considering incentive mechanisms. A tuple (*P*, *S*, *U*) generally represents a game *G*, where *P* is the set of players, *S* is the set of strategies, and *U* is the set of payoff functions. For a player *i*, its payoff is computed by $u_i(s) = b_i(s) - c_i(s)$. The symbol s is a strategy profile, $b_i(s)$ is the benefit, and $c_i(s)$ is the cost of player *i*.

In a complete information game, an *n*-triple strategy for all *n* players is expressed as the strategy $s = \{s_i\}_{i=1}^{n}$. The best bargain function of player *i* to the strategies of other players is denoted by $br_i(s_{-i})$, and is generally written as s_{-i}. The objective of each player is to maximize the utility of its strategy, i.e., $\max_{s_i} u_i(s_i, s_{-i})$.

Complete information games are utilized to model data privacy issues in VSNs [14], where a defender adopts privacy-preserving methods against attack strategies. The knowledge and attack strategies together with the different accuracy requirements on the performance of defense strategies are evaluated for individual privacy. A Nash Equilibrium (NE) is reached after the bargaining among players. That is, no player wants to continue bargaining on the given strategy, when $s_i = br_i(s_{-i})$ is satisfied for player *i*. A pure strategy is reached where an NE exists. For player *i*, the following expression should be satisfied:

$$u_i\left(s_i^*, s_{-i}^*\right) \geq u_i\left(s_i, s_{-i}^*\right), \forall s_i \in S_i. \tag{2}$$

Generally, a mixed strategy is always utilized in the actual schemes. Precisely, a mixed strategy x_i of player *i* is a probability distribution over his pure strategy set S_i. We assume that χ_i is a set of distributions over the pure strategy set S_i. Then an equivalent formula can be concluded:

$$\overline{u_i}\left(x_i^*, x_{-i}^*\right) \geq \overline{u_i}\left(x_i, x_{-i}^*\right), \forall x_i \in \chi_i, \tag{3}$$

where $\overline{u_i}$ is the expected payoff function. A Bayesian Nash Equilibrium (BNE) is adopted in [14]. If $S^* = (s_i^*(\theta_i), s_{-i}^*(\theta_{-i}))$ is a pure strategy BNE, the strategy for each player *i* satisfies:

$$s^* \in \max_{s_i \in S_i} \sum_{\theta_{-i}} p(\theta_{-i}) \cdot u_i\left(s_i, s_{-i}^*(\theta_{-i})\right), \forall \theta_i. \tag{4}$$

A non-cooperative game is utilized to study the characteristic of verifiable multilateration for the defender's strategy improvement in WSNs [149]. In this research, the interaction between independent malicious nodes and verifiers is modeled as a non-cooperative game. A tuple $\langle$ *Q*, *A*, *U* $\rangle$ represents a secure localization game, where *Q* is a pair of competitors and $Q = \{v, m\}$. Herein, *v* is a defender, while *m* is a malicious player. Set *A* contains the available actions to players, and set *U* embraces the players' utility functions. The corresponding objective is to maximize the value of the verifier player, which can be realized by minimizing the benefits of the maximum strategy for the malicious player.

An attack-defense game is utilized to balance attack and defense benefits in vehicular networks [150]. The attack-defense game is modeled as a static game, i.e., each player takes steps without knowing others' actions. The attack-defense tree describes the potential attack and defense strategies for an attacker and defender respectively. When two players respectively adopt the strategies s_{p_1} with probability $p_1 = (p_{c_1}, \ldots, p_{c_n})$ and s_{p_2} with $p_2 = (p_{a_1}, \ldots, p_{a_n})$, the mixed strategy $(s_{p_1^*}, s_{p_2^*})$ is an NE only if the mixed strategy for each participant satisfies Equation (3).

An intrusion detection and prevention scheme in vehicular networks has been designed with an ability to detect and predict the potential malicious behavior of an attacker via game theory [151]. The involved players are RSUs and their monitored vehicles, which are suspected as malicious ones. Each player performs a specific action to maximize its benefits. The strategies of an RSU are detecting and categorizing the monitored vehicles. The vehicle has two strategies: attack and wait. During each time slot, the game can take place as an interaction between an RSU and a vehicle located within the RSU's signal range.

An incomplete information game model is adopted for batch identification in wireless mobile networks, for the sake of selecting invalid signatures with the minimum delay in the situation where dynamic attacks exist [152]. There are generally two kinds of attackers in the network: one is hot-headed attackers and they do not take the possibility of a verifier's traceback into consideration; the other kind of attackers acts more cautiously compared to the hot-headed attackers, and has the ability to protect their identity by confusing the verifier. Each attacker owns a couple of attack strategies, and the verifier does not know the strategies taken by the attackers beforehand. The cost for anti-tracing is related to attack frequency, and grows when the amount of false messages rises.

Lesson 5: The aforementioned researches related to security games generally study the interaction between defenders and attackers, which can provide a fundamental decision for vehicles to adjust their behaviors. The security games formed in most of the studies are merely between one defender and one attacker, where a possible equilibrium is reached by rounds of bargains. However, the players in VSNs may only have a few seconds for communication due to the high mobility, making the bargains only available in a limited number of rounds. Moreover, the Nash equilibrium is difficult for computation and its complexity is even beyond the terminals' capability. Therefore, some important issues need further studies: 1) efficient mechanism design is necessary to make players change possible parameters to reach a desirable equilibrium; 2) extension security game requires to be designed for cooperative players to maximize their utilities; 3) security games under incomplete information are challenging, since some vehicles in VSNs may not have tight social relationships.

F. Location-Based Solutions

Location-based solutions are viewed as promising strategies for communications in VSNs, since vehicles can obtain location information from a Global Position System (GPS), and acquire the global map information from a digital map. In a location-based solution, the location is fundamentally important in developing an effective method.

Recently, the number of location-based services has increased dramatically. Location proofs enable users to be verified about their locations. It is essential that the proof

collection and validation should not violate individual privacy. VeriPlace [164] is a location proof architecture, which can not only detect cheating users lying their locations, but also preserve individual privacy. In VeriPlace, an Access Point (AP) issues an intermediate location proof for the nearby users, which certifies the user's presence. Later, when users want to access a service with a location proof, they must obtain a final proof by presenting their intermediate proofs to TTA.

Similar to VeriPlace, VProof [153] is also a location proof scheme in vehicular networks, which allows a vehicle to certify whether the current location matches its historical locations. The location proof is constructed by extracting relevant content from the messages received from RSUs. It is observed that the Received Signal Strength (RSS) of the packets received by the same vehicle exhibits similar patterns over time, when the vehicle passes an RSU and fixes its transmission power for these packets. Consequently, users need to show the correct RSS pattern of the packets sent by a nearby RSU, if they claim that their data have been collected at a certain place. When receiving a packet, a vehicle needs to create a location proof as $LP = (U_i, VAM, t, RSS, C_p, LOC)$, where a) U_i is the ID of an RSU that sends the packet to the vehicle, b) *VAM* is the authentication message, c) t is the generation time of the packet, d) *RSS* is the RSS value of the packet, e) C_p is the ciphertext of the transmission power p, and f) *LOC* is the GPS location of the vehicle when it receives the packet.

Location information can also be useful for detecting the vehicular rogue APs in VSNs [154]. In this scheme, users can distinguish a rogue AP from a normal one based on the RSS value of the received messages. Each AP needs to broadcast its GPS location, which leads to location forgery for vehicular rogue APs to avoid detection. A detection algorithm is also designed to validate the reported locations by employing RSS values. The inputs of the algorithm contain the reported locations of APs, the RSS of the beacon and the location of the vehicle. Based on the reported locations of APs and the vehicle's own location, the distance between the AP and vehicle can be inferred by the RSS value. The relationship between RSS and the distance can be characterized by a log-distance propagation algorithm. The propagation algorithm is computed by the parameters, including the RSS value based on a distance, the transmit power of the sender and the rate of attenuation. If there is a large gap between the distances computed from the GPS locations and those deduced from RSS values, the AP is likely to cheat users.

In location-based services, a location cloaking method can be utilized to cloak the exact locations to resist location-based attacks [157]. Location cloaking can hide vehicles' exact locations by generalization (e.g., k-anonymity), spatial transformation and dummy locations. To achieve k-anonymity, a big area at least covering $k-1$ other users should be found, so that the malicious nodes can be disabled to distinguish a user's exact location from the other $k-1$ locations. However, the traditional k-anonymity has some drawbacks: first, the location anonymizer is the unique manager in the system. If it suffers from an attack from an adversary, all users' privacy can be leaked; second, it is challenging to select the $k-1$ dummy locations to effectively protect the location privacy. To overcome the above disadvantages, a dummy-location selection algorithm is proposed to achieve k-anonymity in [165]. Its basic idea is to select the dummy locations by considering that some side information may be exploited by the adversary. Therefore, dummy locations with similar query probabilities can always be selected. Similar to [165], a k-anonymity based privacy preservation scheme is proposed to defend location injection attacks, which enables an attacker to inject fake locations to the anonymizier [166]. Its main focus is to explore the mobility patterns of users and find their similarity between fake and high-risk users such that the fake locations can be discovered.

Location cloaking can be integrated with clustering anonymization. Ying and Makrakis [155] propose a concept of an edge-cluster graph, and then transform a real road map into such a graph. A metric called hiding information strength is used to measure the information related to the edge-cluster graph and its corresponding real road map. Cloaking cycle and simple loop are defined in their proposed location cloaking algorithm. Then, the principles for determining the optimal cloaking cycle are defined to control the size of a final cloaking region.

The most important application for location cloaking is to protect the location privacy for an LBS query. For example, to resist the location-dependent attack in an LBS query, a privacy-preserving algorithm based on location cloaking is proposed in [156]. For a requesting user preparing to query for LBS, this scheme focuses on generating a cloaked region, which contains many other users to meet the privacy requirements. It contains four steps: first, it identifies as many candidate user sets as possible; second, the smallest circle is found among these candidate user sets; third, a safe cloaking region is generated by finding the largest candidate user set satisfying the smallest circle bound; at last, update the sub-candidate user set in a timely fashion. Similar to [156], a privacy preserving scheme is proposed to protect location privacy for LBS in vehicular transportation systems [157]. Point of interest is provided for drivers' queries by making use of transportation information on roads. However, the location cloaking approach may not prevent the continuous exposure of location information, resulting in the violation of location privacy [18].

An alternative approach for location cloaking to protect location privacy is mix-zones, which can break the continuous exposure of the location information. For example, the locations of mix-zones provide help for a pseudonym changing process in [57]. A mix-zone can be dynamically formed in the network by vehicles, at the time when their pseudonyms are expiring. After implementing a pseudonym change, vehicles can also increase their reputation values. The process is as follows: a) when the lifetime of a vehicle's pseudonym is close to 0, it sends a Request for Mix-zone Establishment (RME) message to the control server, containing location, pseudonym and average speed; b) the control server computes the mix-zone for the vehicle, and broadcasts a Request for Changing Pseudonym (RCP) message to other vehicles; c) upon receiving the RCP messages, vehicles check if they are located in the mix-zone and whether their pseudonyms are about to expire; if yes, they will send RME messages to a Control Server (CS); d) CS confirms whether the vehicles are located in the

mix-zone after receiving the RCP messages; if so, CS will not respond to these RCP messages.

Lesson 6: From the aforementioned studies, we can learn that location information can be mainly leveraged for two purposes: one is for location proof, and the other is utilized to cloak the exact location of vehicles to protect the location privacy. The advantage of using location-based information is the low computational complexity without requiring additional processing in mobile terminals. To protect location privacy, location cloaking and mix zones are promising to effectively hide users' exact locations. However, the performance for keeping individual privacy is largely reduced in low-density areas compared to that in high-density ones, since there are not enough anonymous samples to guarantee the unlinkability of vehicles. These drawbacks lead to new research directions for location-based solutions: 1) novel metrics for location-relevant operations to avoid the tracking by attackers. For example, the time-to-confusion metric is proposed in [167] to ensure the unlinkability of vehicles by defining a time-to-confusion value in a location cloaking algorithm; 2) the trade-off between location privacy and proof to satisfy different application requirements; and 3) the combination of location-based solutions with other privacy-preserving schemes to provide a high-level security while keeping low computational complexity.

G. Physical Layer Security Techniques

With the development of intelligent vehicles and the dynamic nature of VSN topology, various attacks can be launched without the awareness of participants, threating their privacy. Cryptography-based schemes are commonly utilized to protect individual privacy in VSNs. Nevertheless, the rapid evolution of wireless and mobility-aware technologies makes those attacks rather complicated. Since cryptographic algorithms alone are insufficient to resist potential attacks, other kinds of technologies need to be leveraged in VSNs as supplemental methods for privacy preservation. As a promising paradigm, Physical Layer Security (PLS) can be an alternative to complement cryptography-based methods in wireless networks [168], and protect individual privacy in the data transmission and content dissemination processes of VSNs from the perspective of physical layer. Generally, it allows developers to leverage the characteristics of wireless channels, i.e., interference, diversity, dispersion and noise, to guarantee the normal network operation and prevent eavesdroppers simultaneously [169]. It is important for PLS to design suitable transmission schemes to increase the gap between the performance of a receiver's link and that of the eavesdropper. Therefore, many PLS technologies and performance metrics are developed to enhance the security of a wireless communication environment [170]. Assume that a transmitter, who prepares to communicate with a legitimate receiver via a secret channel, is called Alice, and the legitimate receiver is named Bob. The eavesdropper who monitors the channel and wants to obtain private information is called Carl. According to the characteristics of signals, the methods for PLS can be classified into three categories: frequency, time and space domain security.

Orthogonal Frequency Division Multiplexing (OFDM) is a commonly used technology to improve network transmission efficiency. It enables the signal to be transmitted and received via many different sub-carrier frequencies merely by one antenna in a time slot. Many researches have paid attention to the design of secure OFDM schemes for frequency domain security [171]–[173]. The technology based on time domain security is well-investigated for PLS to prevent eavesdropping attack. This kind of technology allows transmitting and receiving the information-carrying signal over one carrier frequency and merely by one antenna in the time domain. A secure Orthogonal Transform Division Multiplexing (OTDM) waveform scheme is proposed in [174] for 5 G wireless systems. The orthogonal transform basis functions from the channel are extracted to keep the security of data symbols in the modulation and demodulation processes. Channel shorting technology is utilized in [175] to construct secure OFDM communication systems. The time domain scrambling technology is employed in OFDM systems for PLS [176]. The space domain security technology generates secret keys by exploiting multiple antennas and relays, not only including localized and trusted ones, but also embracing distributed and untrusted ones. In order to provide a secure communication environment, a power-efficient technique is designed based on an untrusted decode-and-forward mode [177]. A resource allocation scheme is studied in [178] for secure and energy-efficient communication in orthogonal frequency-division multiple-access downlink networks.

Though cryptography-based technologies are commonly utilized in VSNs, PLS technologies are more suitable to resist eavesdropping attacks in some circumstances. On one hand, the former always require TTA to guarantee system fairness, which is vulnerable to network failure. On the other hand, the timely communication between vehicles and TTA cannot be guaranteed in some rural areas, making the update of their keys delayed. Consequently, PLS technologies can be alternatives to the former to overcome its drawbacks [179]. A study on physical layer attacks is presented in [158], mainly focusing on jamming attacks. System-level simulations and real-world experiments demonstrate that jamming attack can be harmful to both internal and external vehicular communication, which threatens the security of VSNs. Two PLS technologies are proposed to establish secure communication links for millimeter wave vehicular communication systems in [159]. Multiple antennas with one and multiple Radio Frequency (RF) chains are studied for transmitting information to a vehicle.

In addition, some physical characteristics of a wireless channel can be exploited to generate secret keys for communications in VSNs. Generally, a channel-based key generation process requires the following stages [160]:

Channel probing: it helps vehicles obtain the physical information of channel status and make suitable decisions on channel utilization. A trade-off needs to be made between channel information collection and resource consumption for channel measurement. For example, Alice sends a sequence A to Bob in the first timeslot. Bob records the physical characteristics of A by some measurement strategies after receiving A. After that, Bob transmits a sequence B to Alice, and Alice

records the physical characteristics of B in the second timeslot. There can be several rounds of channel probings.

Measurement quantization: it transfers the measured characteristics into real numbers with the finite-wordlength representation. That is, both Alice and Bob convert their channel-based physical characteristics into random key bits by using a quantization approach.

Error correction: it corrects the unmatched information because of random noise and imperfect reciprocity in the channel. That is, the bit discrepancies are identified and reconciled by Alice and Bob. Privacy amplification techniques and key reconciliation are two common solutions.

Secret key generation techniques based on RSS of a radio channel for VSNs are proposed in [161] and [162]. RSS can be measured by different values at distinct locations, making legitimate vehicles and attackers acquire different measurements from the channel. Similar to [161] and [162], a secret key establishment scheme for VSNs is proposed in [163] to allow each pair of communicating vehicles to extract a shared secret key from the values of Received Signal Strength Indicator (RSSI). In addition, temporal variability attributes, including 3-D scattering and the mobility of these scatterers, are incorporated into the secret-key generation process for VSNs in [110]. Nonreciprocity compensation is combined with turbo codes to generate keys.

Lesson 7: The aforementioned PLS studies related to frequency, space and time domains mainly concentrate on transmission parameter optimization at the physical layer based on the characteristics of wireless communication channels. These schemes can keep system security by resisting eavesdropping attacks without the need of high-complexity computational resources. However, the drawback is that they merely take consideration of physical layer design without the parameter adjustment in upper layers. The disadvantage makes the application scope of PLS techniques narrow, especially in VSNs where multiple kinds of attacks may coexist. Therefore, the cross-layer security design by considering the interaction among different layers should be deeply studied from the perspective of PLS. For example, the joint physical-application layer security design and joint physical-network layer security design can be two promising research directions in the future PLS study. In addition, there are many other kinds of attacks besides an eavesdropping attack in VSNs, such as attacks aiming at revealing the information stored in RSUs and servers, resulting in high network environment complexity. Thus, the design of PLS should not only focus on V2V communications, but also take the design of V2I and Infrastructure-to-Infrastructure (I2I) communications into consideration.

Generally, the solutions are not utilized alone in each research but mostly integrated to handle privacy issues. We summarize the characteristics of aforementioned privacy-preserving solutions in VSNs in Tables VI and VII.

V. Research Challenges and Future Directions

In previous sections, we have reviewed the state-of-art of solutions for privacy issues in VSNs, and comprehensively analyzed the characteristics of existing schemes. However, there are several research challenges and open issues, which are left without mature answers. In this section, we discuss some possible future research directions to bring new visions into the horizon of security and privacy issues for the research community of VSNs.

A. Location-Aware Routing

The location-aware routing has received intensive attention from the research community of VSNs. Location and distance information can be served as supplemental conditions for node authentication. Though it is useful to utilize the location information to solve problems as described in Section IV-F, there are still some challenges for the location-aware routing schemes.

1) Location-Based Metrics: The locations obtained by the GPS equipment are utilized for the location proof in an authentication process. Although GPS provides a high localization accuracy in urban areas, the full dependence on GPS information is problematic [180]. If the communication failures happen, the inaccurate GPS information can substantially lower the accuracy of a vehicle's location information.

Recently, some researches have focused on exploiting metrics to improve the localization services (e.g., [181] and [182]). Besides these methods, efficient algorithms need to be designed to support localization services. For example, the fingerprint information of the surrounding Wi-Fi can be used as a supplemental method to get the accurate location of vehicles. In addition, the relative positions with other vehicles or RSUs can also be applied in localization algorithms. With these metrics, the location proof in security routing schemes can be enhanced. Although malicious nodes can pretend to be at a location, they can not fake a fingerprint of Wi-Fi.

2) Trade-Off Between Location Proof and Location Privacy: Privacy is a major concern in VSNs. Users are becoming increasingly concerned about the risks of compromising their personal information, since the privacy in VSNs can be undermined without awareness. Generally, researchers have understood the necessity of privacy protection for a long time. They generally focus on the data, identity and location privacy in the VSNs, and commonly utilize PKI-based cryptographic algorithms [183], [184].

As we know, location privacy is one of the fundamental concerns in VSNs. If the location of a vehicle is leaked and tracked by a malicious node, the personal information of the driver may be under threat. Vehicles are required to periodically broadcast authenticated safety messages, containing their real-time location and speed. These messages make the surrounding vehicles be aware of dangerous situations and warnings, and also threaten the location privacy of vehicles. Therefore, a trade-off has to be made between the location proof and location privacy.

In addition, in online or mobile networks, users establish social connections mainly from their online friends or family members. Nevertheless, a social connection among vehicles is based on their common interests or preferences in VSNs, and the high mobility makes vehicles hard to keep a long-term relationship. Therefore, location and interest-based privacy deserves to be protected. Though various studies either

TABLE VI
SUMMARY OF SECURITY AND PRIVACY SOLUTIONS IN VSNs

Ref.	Description	Scenario	Privacy issues				Attacks			Solutions						
			Community privacy	Location privacy	Interest privacy	Other privacy	Server attack	RSU attack	OBU attack	Pseudonym	Cryptography	Signature	Trust	Game theory	Location	PLS
[79]	A privacy-preserving social-based content dissemination scheme	Urban area	×	×	√	×	×	×	√	×	×	√	×	×	×	×
[80]	Transaction privacy protection for vehicles	Urban area	×	×	√	×	√	×	√	×	√	×	×	×	×	×
[81]	Quality optimization and reliability assurance for service access	Urban area	×	×	√	×	×	×	√	×	×	×	√	×	×	×
[82]	Community privacy investigation and protection mechanisms	Urban area	√	√	×	√	√	×	×	×	×	×	×	×	×	×
[103]	An effective pseudonym changing strategy at social spots	Urban area	×	√	×	√	×	×	√	√	√	×	×	√	×	×
[104]	A framework for providing anonymity to communicating cars	Highway	×	×	×	√	×	√	√	√	√	×	×	×	×	×
[105]	A hierarchical pseudonyms management scheme	Highway	×	√	×	√	×	×	√	√	√	×	×	×	×	×
[106]	A novel authentication framework	Highway	×	√	×	√	×	×	√	√	√	×	×	×	×	×
[111]	An efficient broadcast authentication scheme	Highway	×	×	×	√	×	×	√	×	√	√	×	×	×	×
[114]	A message forwarding scheme based on computational abilities of RSUs	Urban area	×	×	×	√	×	×	√	×	√	√	×	×	×	×
[115]	An identity-based batch verification scheme	Highway	×	×	×	√	×	√	√	×	√	√	×	×	×	×
[116]	A novel authentication scheme according to ID-based signature	Urban area	×	×	×	√	×	×	√	×	√	√	×	×	×	×
[119]	An incentive-aware multihop forwarding procedure	Urban area	×	√	×	√	×	√	√	×	√	√	×	×	√	×
[120]	Secure communication establishment for V2V	Highway	×	×	×	√	×	×	√	×	√	√	×	×	×	×
[123]	Secure communication establishment for V2I	Highway	×	×	×	√	√	√	√	×	√	√	×	×	×	×
[125]	An efficient authentication scheme	Urban area	×	×	×	√	×	√	√	×	√	√	×	×	×	×
[126]	A group signature scheme for ad hoc network	Suitable for all routers	√	×	×	√	×	×	√	×	√	√	×	×	×	×
[128]	A V2I communication system	Suitable for all routers	√	×	×	√	×	×	√	×	√	√	×	×	×	×
[129]	A Sybil attack detection mechanism	Urban area	×	√	×	×	×	×	√	×	√	√	×	×	×	×
[131]	A privacy-preserving incentive scheme	Urban area	×	√	×	√	×	×	√	×	√	√	×	×	×	×
[134]	A privacy-preserving authentication protocol	Suitable for all routers	×	×	×	√	×	×	√	×	√	√	×	×	×	×
[139]	An authentication scheme for V2V	Suitable for all routers	×	√	×	√	×	√	√	×	√	×	√	×	×	×
[140]	Vehicular security against various attacks	Highway	×	×	×	√	×	×	√	×	×	×	√	×	×	×
[143]	A safe and reliable information dissemination scheme	Urban area	×	×	×	√	×	×	√	×	×	×	√	×	×	×
[144]	A Distributed Trust Model	Urban area	×	×	×	×	×	×	√	×	×	×	√	×	×	×
[145]	A trust-based verifiable vehicular cloud computing scheme	Urban area	×	√	×	√	×	×	√	×	√	×	√	×	×	×
[146]	An attack-resistant trust management scheme	Urban area	×	×	×	×	×	×	√	×	×	×	√	×	×	×
[147]	A novel trust establishment architecture	Urban area	×	×	×	√	×	×	√	×	×	×	√	×	×	×
[149]	Attack resistance for node localization	Urban area	×	×	×	×	×	×	√	×	×	×	×	√	√	×
[150]	An attack-and-defense game for security assessment	Highway	×	√	×	√	×	×	√	×	×	×	×	√	×	×

("√" if the protocol satisfies the property, "×" if not)

consider location privacy or interest privacy, their corresponding relationships have not been fully investigated. If an attacker combines them to initiate some attacks, the real identity of a user can be disclosed.

3) Secure Routing in a Fully Distributed Manner: Many researches have addressed the routing schemes in distributed VSN structures (e.g., [185]–[187]). Unlike the conventional centralized systems, the infrastructures (e.g., RSUs) are

TABLE VII
SUMMARY OF SECURITY AND PRIVACY SOLUTIONS IN VSNS (CONT.)

Ref.	Description	Scenario	Privacy issues				Attacks			Solutions						
			Community privacy	Location privacy	Interest privacy	Other privacy	Server attack	RSU attack	OBU attack	Pseudonym	Cryptography	Signature	Trust	Game theory	Location	PLS
[151]	A novel intrusion detection and prevention scheme	Suitable for all routers	×	×	×	×	×	×	√	×	×	×	×	√	×	×
[152]	A batch identification model	Urban area	×	×	×	×	×	×	√	×	√	√	×	√	×	×
[153]	A vehicle location proof	Urban area	×	×	×	√	×	×	√	×	√	×	×	×	√	×
[154]	A practical user-side detection scheme to detect rogue APs	Suitable for all routers	×	×	×	×	×	√	√	×	×	×	×	×	√	×
[57]	Selfish vehicle protection for location privacy	Urban area	×	√	×	√	×	√	√	√	×	×	√	×	√	×
[155]	Location privacy protection for location-based services	Urban area	×	√	×	×	×	×	√	×	×	×	×	×	√	×
[156]	A location privacy preserving algorithm	Suitable for all routers	×	√	×	×	×	×	√	×	×	×	×	×	√	×
[157]	Private information retrieval	Urban area	×	√	×	×	×	×	√	×	√	×	×	×	√	×
[158]	A study on multiple attack strategies based on vehicular communication	Urban area	×	×	×	√	×	×	√	×	×	×	×	×	×	√
[159]	PLS techniques for vehicular communications	Suitable for all routers	×	×	×	√	×	×	√	×	×	×	×	×	×	√
[160]	A key generation technique for cyber-physical system	Urban area	×	×	×	√	×	×	√	×	×	×	×	×	×	√
[161]	Secret key establishment for vehicular communications	Highway	×	×	×	√	×	×	√	×	√	×	×	×	×	√
[162]	A key generation technique based on channel properties	Urban area	×	×	×	√	×	×	√	×	√	×	×	×	×	√
[163]	Secret key extraction for VSNs	Suitable for all routers	×	×	×	√	×	×	√	×	×	×	×	×	×	√

("√" if the protocol satisfies the property, "×" if not)

deployed in a highly distributed manner, and managed by different entities. For example, a shopping center may install an RSU to distribute the recent promotion information to the public. The distributed RSUs installed by different shopping centers and other businesses collectively form an infrastructure network. Nevertheless, secure routing under a distributed network structure is still in the initial stage. Though the attackers cannot obtain the total information in the network, yet they can control part of the network.

There also exist some challenges for designing secure routing schemes in distributed systems. For example, how to manage and process network resources in a distributed manner for both infrastructures and vehicles needs to be further investigated. In a distributed network, information is generated and managed by different entities. The attackers need to go extra mile to control the same amount of resources compared to a centralized network. If an attacker focuses on a specific piece of information only, it can target at the server that owns such information. This may lead to weak protection compared with a centralized server. In addition, how to securely transmit messages in distributed systems is another issue. Without the centralized server, vehicles need efficient authentication methods to verify each other among different subsystems, and establish a proper routing path for messages.

B. Secure Handover in Urban Areas

Different handover schemes have been studied in heterogeneous networks, where wireless and cellular networks coexist [37], [188]. In VSNs, handover management is carried out by constructing a new path towards the destination, which is called rerouting. In order to ensure handover performance, plenty of researches focus on mobility management and delay reduction for a transmission path. Either mobile IPv6 or proxy mobile IPv6 protocol is used to enable a handover scheme. However, there are some security issues to be investigated.

1) Packet Loss: To ensure the network connectivity for multiple mobile nodes (e.g., vehicles and intelligent devices) in ITSs, the network mobility basic support protocol [189] has been formalized as a standard protocol. Since the originally designed purpose of mobile IPv6 is only for a single mobile node, network mobility based on mobile IPv6 incurs a high tunneling burden on the link between the previous and current access routers. For example, the traffic of mobile nodes may block in the tunnel and be overloaded, when there are many mobile nodes. With high traffic density of mobile nodes, the tunnel may even suffer from a congestion, and packet loss may occur during the handover process. Therefore, effective mechanisms need to be developed to reduce the packet loss.

2) Authentication Delay: Handover based on mobile IPv6 is inevitable to cause network delay because of the movement detection, IP address configuration and location update. The total handover delay may be too large for real-time applications or multimedia services. The interactions and interworking between MAC and routing layers need to be addressed to solve the handover delay problem and provide seamless handover. In addition, a trade-off has to be made between the high security level and the desired QoS. Developers should design reasonable handover schemes based on different service requirements in the future.

3) Data Privacy: The handover process in VSNs is possible to occur between an access point and a vehicle by generating session keys based on the simultaneous key update function. Nevertheless, several issues exist in key management schemes. For example, the desynchronization attack may be launched to compromise the subsequent session keys. In addition, the semi-trusted third parties can obtain all the transmitted messages, and may expose to attackers with malicious purposes. In order to protect data privacy in message transmission processes, a handover key management algorithm is studied in [190]. A proxy re-encryption system is established by allowing the session key to be encrypted by the mobility management entity and a mobile relay node sequentially. A software defined network enabled security scheme is designed in [191] to achieve privacy protection and efficient authentication in handover processes.

C. Big Data Collection and Analysis

Huge volumes of data (e.g., beacon and warning messages) are generated every day in VSNs, and all participants in the network act as data generators [192], [193]. Most drivers or passengers intend to watch videos in cars or buses to kill time during their long journey. Consequently, how to exploit the big data in VSNs has drawn much attention [194]. Efforts have concentrated on the big data exploitation to improve some special performances in VSNs. For example, a social-based localization algorithm is proposed, which predicts location by big data analysis to assist global localization in VSNs [182].

However, the security and privacy issues of big data in VSNs are still open. One future trend is privacy-preserving big data mining and analysis in VSNs. Big data analysis in a secure manner is significant, because they are referred to a vehicle's daily trace and even activities. Mining and analyzing these data may reveal the identities of drivers and passengers, violating the privacy requirements of individuals. As a result, privacy-preserving big data mining and analysis are of great importance for the big data-based applications. To balance individual privacy concerns and social data utilization, a data processing approach is proposed in [195] to protect sensitive information while keeping data availability. To address the privacy issues of ride sharing for autonomous vehicles, a similarity measurement scheme is proposed for encrypted data to guarantee data privacy [196]. Each user encrypts the data locally and submits them to a server, and the server decides which user can share data with others by measuring the similarity of users' data.

With the increasingly generated big data in VSNs, technologies based on vehicular cloud computing are developed rapidly. Outsourcing data and computational burden for vehicles to the cloud side is promising. Nevertheless, this may raise new research problems that need further explorations. For example, how to ensure the security of these outsourced databases is significant, because some operations may easily access sensitive datasets. Du *et al.* [197] design a privacy-preserving method based on machine learning in the application of mobile edge computing. Differential privacy is achieved by adding Laplacian noise in the training data. A proximity model is established in [198] to enable the semantic proximity of sensitive values and attributes in cloud servers. In addition, a two-step clustering method is designed to solve the formulated proximity-aware clustering problem.

D. Attack Resistance

Attacks in wireless networks can be launched by different kinds of sources and may target at any vehicle. VSNs can be viewed as a special example of MSNs, and suffer from all the security weaknesses in MSNs. However, the security of VSNs is more challenging due to the high mobility of vehicles and the dynamic nature of the network topology. Therefore, attacks may always spring up to violate the network security and privacy rules, e.g., a long-range wireless attack can be launched by a malicious application installed in a smartphone or vehicles in a connected car environment [199].

1) Authentication Schemes: Authentication is a frequently used method to validate the identities and authorities of vehicles in VSNs. An identity is required for the authentication process, while no link can be established between the information that others obtain and its original owner for privacy protection. TTA is always utilized to meet the above contradictory requirements. However, multiple querying to remote TTA may cause network bottlenecks. Therefore, suitable authentication mechanisms should be designed to overcome the contradiction between authentication efficiency and privacy requirements.

In addition, with the booming attacks, long-term effective authentication methods do not exist. To resist these attacks, on one hand, efficient authentication methods should be designed to meet the security requirements. On the other hand, authentication methods should be updated in a timely manner. Therefore, how to develop the updated mechanisms of authentication methods, which are not only compatible with existing authentication schemes, but also require low update cost, should be investigated.

2) Trust-Based Schemes: Due to the advantages of wireless access technologies, vehicles in different places can be connected to form a VSN. Within such a network, trustworthiness between vehicles can be mined from their behaviors and interactions to support trustworthy information sharing among vehicles. Currently, various trust-based schemes (direct or indirect trust) have been introduced to model the trust of vehicles in VSNs [200]. Both topology-based and evidence-based methods have been deployed. Nevertheless, there still exist some open issues to be further investigated.

Establishing appropriate trust models among highly mobile vehicles is an important issue, especially for indirect trust models. This is because the network topology is time-varying, and the connections among vehicles are weak. Consequently, modeling trust propagation and computing the expected trustworthiness of a social connection are necessary. In addition, certain dynamic trust metrics should be considered in the trust models, e.g., location, time and tasks. For instance, if a received message containing an event is close to the place where the event happens, the trust value of the generated message should be high.

VI. Conclusion

In this article, we have presented a comprehensive literature review, focusing on the privacy preserving mechanisms for content dissemination in VSNs. First, we introduce the characteristics and features of content dissemination in VSNs. We then study and analyze the privacy issues deserving to be considered for the design of content dissemination approaches. After that, we discuss several kinds of privacy-preserving technologies to resist various attacks and protect individual privacy in VSNs. Finally, we outline some open issues and future research directions. Since privacy issues are becoming increasingly important in VSNs, we believe that this survey is timely and useful for the protocol and application developers, and help them design efficient and effective privacy-preserving solutions for content dissemination in VSNs as well as develop new applications related to VSNs in the big date era [201]–[204].

References

[1] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of VANET clustering techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 657–681, 1st Quart., 2017.

[2] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of Vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4568–4578, Oct. 2018.

[3] 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.

[4] X. Wang *et al.*, "A city-wide real-time traffic management system: Enabling crowdsensing in social Internet of Vehicles," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 19–25, Sep. 2018.

[5] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 49–55, May 2017.

[6] Z. Ning *et al.*, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.

[7] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFI protocol for medical privacy protection in IoT," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1656–1665, Jan. 2018.

[8] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.

[9] C. Lai, D. Zheng, Q. Zhao, and X. Jiang, "SEGM: A secure group management framework in integrated VANET-cellular networks," *Veh. Commun.*, vol. 11, pp. 33–45, Jan. 2018.

[10] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 42–47, Aug. 2015.

[11] 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.

[12] K. Ota, M. Dong, S. Chang, and H. Zhu, "MMCD: Cooperative downloading for highway VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 34–43, Mar. 2015.

[13] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[14] Y. He, L. Sun, W. Yang, and H. Li, "A game theory-based analysis of data privacy in vehicular sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 1, pp. 1–14, 2014.

[15] X. Hu *et al.*, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1557–1581, 3rd Quart., 2015.

[16] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social Internet of Vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[17] A. Rahim *et al.*, "Vehicular social networks: A survey," *Pervasive Mobile Comput.*, vol. 43, pp. 96–113, Jan. 2017.

[18] P. Asuquo *et al.*, "Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges and countermeasures," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2820039.

[19] D. Eckhoff and C. Sommer, "Driving for big data? Privacy concerns in vehicular networking," *IEEE Security Privacy*, vol. 12, no. 1, pp. 77–79, Jan./Feb. 2014.

[20] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2018.2818888.

[21] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[22] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.

[23] H. Jin, M. Khodaei, and P. Papadimitratos, "Security and privacy in vehicular social networks," in *Vehicular Social Networks*. Boca Raton, FL, USA: CRC Press, 2016, pp. 155–169.

[24] F. Cunha *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Netw.*, vol. 44, pp. 90–103, Jul. 2016.

[25] M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad hoc networks," *Veh. Commun.*, vol. 1, no. 4, pp. 214–225, 2014.

[26] F. Silva *et al.*, "Vehicular networks: A new challenge for content-delivery-based applications," *ACM Comput. Surveys*, vol. 49, no. 1, pp. 1–30, 2016.

[27] F. Mezghani, R. Dhaou, M. Nogueira, and A.-L. Beylot, "Content dissemination in vehicular social networks: Taxonomy and user satisfaction," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 34–40, Dec. 2014.

[28] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "RoadSpeak: Enabling voice chat on roadways using vehicular social networks," in *Proc. ACM SocialNets*, 2008, pp. 43–48.

[29] S. Dietzel, J. Petit, and F. Kargl, "In-network aggregation for vehicular ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1909–1932, 4th Quart., 2014.

[30] X. Wang *et al.*, "A privacy-preserving message forwarding framework for opportunistic cloud of things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2864782.

[31] M. A. Yaqub, S. H. Ahmed, S. H. Bouk, and D. Kim, "FBR: Fleet based video retrieval in 3G and 4G enabled vehicular ad hoc networks," in *Proc. IEEE ICC*, Kuala Lumpur, Malaysia, 2016, pp. 1–6.

[32] Z. Zhou *et al.*, "Social big data based content dissemination in Internet of Vehicles," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 768–777, Feb. 2018.

[33] J. Joy and M. Gerla, "Internet of Vehicles and autonomous connected car—Privacy and security issues," in *Proc. IEEE ICCCN*, Vancouver, BC, Canada, 2017, pp. 1–9.

[34] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic Internet of smartphones," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 810–820, Apr. 2017.

[35] B. Jedari, F. Xia, and Z. Ning, "A survey on human-centric communications in non-cooperative wireless relay networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 914–944, 2nd Quart., 2018.

[36] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.

[37] Y. Bi, H. Zhou, W. Xu, X. S. Shen, and H. Zhao, "An efficient PMIPv6-based handoff scheme for urban vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 12, pp. 3613–3628, Dec. 2016.

[38] F. Zhang, H. Liu, Y.-W. Leung, X. Chu, and B. Jin, "CBS: Community-based bus system as routing backbone for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2132–2146, Aug. 2017.

[39] K. Y. Bae and H. W. Lee, "End to end model and delay performance for V2X in 5G," *J. Intell. Inf. Syst.*, vol. 22, no. 1, pp. 107–118, 2016.

[40] T. H. Luan, X. S. Shen, and F. Bai, "Integrity-oriented content transmission in highway vehicular ad hoc networks," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2562–2570.

[41] F. M. Al-Turjman, A. E. Al-Fagih, W. M. Alsalih, and H. S. Hassanein, "A delay-tolerant framework for integrated RSNs in IoT," *Comput. Commun.*, vol. 36, no. 9, pp. 998–1010, 2013.

[42] F. Al-Turjman, "Price-based data delivery framework for dynamic and pervasive IoT," *Pervasive Mobile Comput.*, vol. 42, pp. 299–316, Dec. 2017.

[43] J. J. Cheng *et al.*, "Routing in Internet of Vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[44] F. Al-Turjman, "Cognitive routing protocol for disaster-inspired Internet of Things," *Future Gener. Comput. Syst.*, Mar. 2017. [Online]. Available: https://doi.org/10.1016/j.future.2017.03.014

[45] M. Z. Hasan, F. Al-Turjman, and H. Al-Rizzo, "Optimized multi-constrained quality-of-service multipath routing approach for multimedia sensor networks," *IEEE Sensors J.*, vol. 17, no. 7, pp. 2298–2309, Apr. 2017.

[46] M. Z. Hasan, H. Al-Rizzo, and F. Al-Turjman, "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1424–1456, 3rd Quart., 2017.

[47] J. Zhang *et al.*, "Joint resource allocation for latency-sensitive services over mobile edge computing networks with caching," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2875917.

[48] Z. Ning, P. Dong, X. Kong, and F. Xia, "A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of Things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2868616.

[49] G. T. Singh and F. M. Al-Turjman, "Learning data delivery paths in QoI-aware information-centric sensor networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 572–580, Aug. 2016.

[50] F. Al-Turjman, "Cognitive caching for the future sensors in fog networking," *Pervasive Mobile Comput.*, vol. 42, pp. 317–334, Dec. 2017.

[51] Z. Chu *et al.*, "Game theory based secure wireless powered D2D communications with cooperative jamming," in *Proc. IEEE Wireless Days*, 2017, pp. 95–98.

[52] S. A. Alabady, M. F. M. Salleh, and F. Al-Turjman, "LCPC error correction code for IoT applications," *Sustain. Cities Soc.*, vol. 42, pp. 663–673, Oct. 2018.

[53] F. Al-Turjman, Y. K. Ever, E. Ever, H. X. Nguyen, and D. B. David, "Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks," *IEEE Access*, vol. 5, pp. 24617–24631, 2017.

[54] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.

[55] F. Al-Turjman, "5G-enabled devices and smart-spaces in social-IoT: An overview," *Future Gener. Comput. Syst.*, Dec. 2017. [Online]. Available: https://doi.org/10.1016/j.future.2017.11.035

[56] D. He, S. Chan, Y. Qiao, and N. Guizani, "Imminent communication security for smart communities," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 99–103, Jan. 2018.

[57] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5631–5641, Dec. 2015.

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

[59] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[60] R. Hussain *et al.*, "Secure and privacy-aware incentives-based witness service in social Internet of Vehicles clouds," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2441–2448, Aug. 2018, doi: 10.1109/JIOT.2018.2847249.

[61] J. Ni, X. Lin, and X. Shen, "Privacy-preserving data forwarding in VANETs: A personal-social behavior based approach," in *Proc. IEEE GLOBECOM*, Singapore, 2018, pp. 1–6.

[62] M. Katsomallos, S. Lalis, T. Papaioannou, and G. Theodorakopoulos, "An open framework for flexible plug-in privacy mechanisms in crowdsensing applications," in *Proc. IEEE PerCom*, 2017, pp. 237–242.

[63] R. Xu, H. Saïdi, and R. J. Anderson, "Aurasium: Practical policy enforcement for Android applications," in *Proc. USENIX Security Symp.*, 2012, p. 27.

[64] Y. Shi, H. D. Tuan, A. V. Savkin, T. Q. Duong, and H. V. Poor, "Model predictive control for smart grids with multiple electric-vehicle charging stations," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2017.2789333.

[65] H. Li, G. Dán, and K. Nahrstedt, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2305–2313, Sep. 2017.

[66] Y. Cao, N. Wang, G. Kamel, and Y.-J. Kim, "An electric vehicle charging management scheme based on publish/subscribe communication framework," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1822–1835, Sep. 2017.

[67] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, Jan. 2018, doi: 10.1016/j.future.2017.12.041.

[68] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[69] K. M. A. Alheeti, A. Gruebler, K. D. Mcdonald-Maier, and A. Fernando, "Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy Petri net model," in *Proc. IEEE ICCE*, Las Vegas, NV, USA, 2016, pp. 502–503.

[70] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[71] S. Aoki and K. Sezaki, "Privacy-preserving community sensing for medical research with duplicated perturbation," in *Proc. IEEE ICC*, Sydney, NSW, Australia, 2014, pp. 4252–4257.

[72] R. Jardí-Cedó *et al.*, "Time-based low emission zones preserving drivers' privacy," *Future Gener. Comput. Syst.*, vol. 80, pp. 558–571, Mar. 2018.

[73] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Comput. Netw.*, vol. 134, no. 7, pp. 78–92, 2018.

[74] S. Allal and S. Boudjit, "Geocast routing protocols for VANETs: Survey and geometry-driven scheme proposal," *J. Internet Services Inf. Security*, vol. 3, nos. 1–2, pp. 20–36, 2013.

[75] X. He, R. Jin, and H. Dai, "Leveraging spatial diversity for privacy-aware location based services in mobile networks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1524–1534, Jun. 2018.

[76] K. Emara, "Safety-aware location privacy in VANET: Evaluation and comparison," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10718–10731, 2017.

[77] K. Rabieh, M. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 1–11, Mar. 2017.

[78] R. Lu, X. Lin, X. Liang, and X. Shen, "FLIP: An efficient privacy-preserving protocol for finding like-minded vehicles on the road," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

[79] L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving social-assisted mobile content dissemination scheme in DTNs," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2301–2309.

[80] J. Kang *et al.*, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[81] Z. Ning *et al.*, "A cooperative quality-aware service access system for social Internet of Vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506–2517, Aug. 2017.

[82] J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "Privacy of community pseudonyms in wireless peer-to-peer networks," *Mobile Netw. Appl.*, vol. 18, no. 3, pp. 413–428, 2013.

[83] J. Du, C. Jiang, K.-C. Chen, Y. Ren, and H. V. Poor, "Community-structured evolutionary game for privacy protection in social networks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 574–589, Mar. 2018.

[84] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[85] L. Guo *et al.*, "A secure mechanism for big data collection in large scale Internet of Vehicles," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 601–610, Mar. 2017.

[86] R. Neha and J. Y. Bevish, "A survey on security challenges and malicious vehicle detection in vehicular ad hoc networks," *Contemp. Eng. Sci.*, vol. 8, no. 5, pp. 235–240, 2015.

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

[88] L. Zhang, X. Men, K.-K. R. Choo, Y. Zhang, and F. Dai, "Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2797190.

[89] D. Jiang, L. Huo, Z. Lv, H. Song, and W. Qin, "A joint multi-criteria utility-based network selection approach for vehicle-to-infrastructure networking," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 10, pp. 3305–3319, Jan. 2018, doi: 10.1109/TITS.2017.2778939.

[90] S. Chang *et al.*, "Private and flexible urban message delivery," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 4900–4910, Jul. 2016.

[91] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594–605, Jan. 2016.

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

[93] H. Chen, W. Lou, Z. Wang, and Q. Wang, "A secure credit-based incentive mechanism for message forwarding in noncooperative DTNs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6377–6388, Aug. 2016.

[94] J. Shao, R. Lu, and X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, 2014, pp. 244–252.

[95] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6475–6488, Jul. 2017.

[96] M. H. 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.

[97] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A two level privacy preserving pseudonymous authentication protocol for VANET," in *Proc. IEEE WiMob*, 2015, pp. 643–650.

[98] H. Li, G. Dán, and K. Nahrstedt, "Proactive key dissemination-based fast authentication for in-motion inductive EV charging," in *Proc. IEEE ICC*, London, U.K., 2015, pp. 795–801.

[99] D.-Y. Yu, A. Ranganathan, R. J. Masti, C. Soriente, and S. Capkun, "SALVE: Server authentication with location verification," in *Proc. ACM MobiCom*, 2016, pp. 401–414.

[100] Y. Michalevsky, S. Nath, and J. Liu, "MASHaBLE: Mobile applications of secret handshakes over Bluetooth LE," in *Proc. ACM MobiCom*, 2016, pp. 387–400.

[101] R. Yu *et al.*, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 1, pp. 93–105, Jan./Feb. 2016.

[102] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[103] 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.

[104] H. Artail and N. Abbani, "A pseudonym management system to achieve anonymity in vehicular ad hoc networks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 1, pp. 106–119, Jan./Feb. 2016.

[105] X. Huang, J. Kang, and R. Yu, "A hierarchical pseudonyms management approach for software-defined vehicular networks," in *Proc. IEEE VTC*, 2016, pp. 1–5.

[106] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.

[107] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 37, pp. 122–132, Feb. 2016.

[108] S. A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA, USA: MIT Press, 2000.

[109] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken, NJ, USA: Wiley, 2007.

[110] G. Epiphaniou *et al.*, "Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2496–2505, Aug. 2018, doi: 10.1109/JIOT.2017.2764384.

[111] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 1, pp. 71–83, Jan./Feb. 2016.

[112] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA Cryptobytes*, vol. 5, no. 2, pp. 1–35, 2005.

[113] E.-J. Goh, *Encryption Schemes From Bilinear Maps*. Stanford, CA, USA: Stanford Univ., 2007.

[114] Y. Xia *et al.*, "Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2629–2641, Oct. 2017.

[115] S.-F. Tzeng *et al.*, "Enhancing security and privacy for identity-based batch verification scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[116] 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.

[117] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proc. IEEE ChinaCom*, 2006, pp. 1–8.

[118] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. ACM VANET*, 2007, pp. 19–28.

[119] L.-Y. Yeh and Y.-C. Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1607–1621, Aug. 2014.

[120] S. Prabhadevi and A. M. Natarajan, "Utilization of ID-based proxy blind signature based on ECDLP in secure vehicular communications," *Int. J. Eng. Innov. Technol.*, vol. 3, no. 5, pp. 55–60, 2013.

[121] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 79, no. 9, pp. 1338–1354, 1996.

[122] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Boston, MA, USA: Springer, 1983, pp. 199–203.

[123] S.-J. Horng *et al.*, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015.

[124] Y.-C. Li and S.-M. Cheng, "Privacy preserved mobile sensing using region-based group signature," *IEEE Access*, vol. 6, pp. 61556–61568, 2018, doi: 10.1109/ACCESS.2018.2868502.

[125] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 907–919, Feb. 2014.

[126] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Proc. Australasian Conf. Inf. Security Privacy*, 2004, pp. 325–335.

[127] S. S. M. Chow, W. Susilo, and T. H. Yuen, "Escrowed linkability of ring signatures and its applications," in *Proc. VIETCRYPT*, 2006, pp. 175–192.

[128] K. Emura and T. Hayashi, "Road-to-vehicle communications with time-dependent anonymity: A lightweight construction and its experimental results," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1582–1597, Feb. 2018.

[129] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil attacks in urban vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[130] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Proc. CRYPTO*, 2002, pp. 465–480.

[131] L. Li *et al.*, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[132] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1018–1025, Mar. 2013.

[133] H. M. Krawczyk and T. D. Rabin, "Chameleon hashing and signatures," U.S. Patent 6,108,783, Aug. 22, 2000.

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

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

[136] J. Zhang, "A survey on trust management for VANETs," in *Proc. IEEE AINA*, 2011, pp. 105–112.

[137] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Front. Comput. Sci.*, vol. 9, no. 2, pp. 280–296, 2015.

[138] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2167–2178, Sep. 2018.

[139] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Syst. J.*, vol. 8, no. 3, pp. 749–758, Sep. 2014.

[140] 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.

[141] D. Alishev, R. Hussain, W. Nawaz, and J. Y. Lee, "Social-aware bootstrapping and trust establishing mechanism for vehicular social networks," in *Proc. IEEE VTC*, 2017, pp. 1–5.

[142] X. Chen and L. Wang, "A trust evaluation framework using in a vehicular social environment," in *Proc. IEEE INFOCOM WKSHPS*, 2017, pp. 1004–1005.

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

[144] N. Haddadou and A. Rachedi, "DTM2: Adapting job market signaling for distributed trust management in vehicular ad hoc networks," in *Proc. IEEE ICC*, 2013, pp. 1827–1832.

[145] C. Huang, R. Lu, H. Zhu, H. Hu, and X. Lin, "PTVC: Achieving privacy-preserving trust-based verifiable vehicular cloud computing," in *Proc. IEEE GLOBECOM*, 2016, pp. 1–6.

[146] 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.

[147] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS," *Comput. Commun.*, vol. 93, pp. 68–83, Nov. 2016.

[148] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," *Future Gener. Comput. Syst.*, vol. 82, pp. 12–28, May 2018.

[149] N. Basilico, N. Gatti, M. Monga, and S. Sicari, "Security games for node localization through verifiable multilateration," *IEEE Trans. Depend. Secure Comput.*, vol. 11, no. 1, pp. 72–85, Jan./Feb. 2014.

[150] S. Du, X. Li, J. Du, and H. Zhu, "An attack-and-defence game for security assessment in vehicular ad hoc networks," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 215–228, 2014.

[151] H. Sedjelmaci, T. Bouali, and S. M. Senouci, "Detection and prevention from misbehaving intruders in vehicular networks," in *Proc. IEEE GLOBECOM*, Austin, TX, USA, 2014, pp. 39–44.

[152] J. Chen, Q. Yuan, G. Xue, and R. Du, "Game-theory-based batch identification of invalid signatures in wireless mobile networks," in *Proc. IEEE INFOCOM*, 2015, pp. 262–270.

[153] Y. Zhang, C. C. Tan, F. Xu, H. Han, and Q. Li, "VProof: Lightweight privacy-preserving vehicle location proofs," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 378–385, Jan. 2015.

[154] H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li, "VR-Defender: Self-defense against vehicular rogue APs for drive-thru Internet," *IEEE Trans. Veh. Technol.*, vol. 63, no. 8, pp. 3927–3934, Oct. 2014.

[155] B. Ying and D. Makrakis, "Protecting location privacy with clustering anonymization in vehicular networks," in *Proc. IEEE INFOCOM WKSHPS*, Toronto, ON, Canada, 2014, pp. 305–310.

[156] H. Jiang, P. Zhao, and C. Wang, "RobLoP: Towards robust privacy preserving against location dependent attacks in continuous LBS queries," *IEEE/ACM Trans. Netw.*, vol. 26, no. 2, pp. 1018–1032, Apr. 2018.

[157] Z. Tan, C. Wang, M. Zhou, and L. Zhang, "Private information retrieval in vehicular location-based services," in *Proc. IEEE WF-IoT*, 2018, pp. 56–61.

[158] Y. O. Basciftci, F. Chen, J. Weston, R. Burton, and C. E. Koksal, "How vulnerable is vehicular communication to physical layer jamming attacks?" in *Proc. IEEE VTC Fall*, Boston, MA, USA, 2015, pp. 1–5.

[159] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.

[160] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[161] A. M. S. Abdelgader, S. Feng, and L. Wu, "Exploiting the randomness inherent of the channel for secret key sharing in vehicular communications," *Int. J. Intell. Transport. Syst. Res.*, vol. 16, no. 1, pp. 39–50, 2018.

[162] J. Wan, A. B. Lopez, and M. A. Al Faruque, "Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security," in *Proc. 7th Int. Conf. Cyber Phys. Syst.*, 2016, p. 13.

[163] X. Zhu *et al.*, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, Jul. 2017.

[164] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in *Proc. ACM GIS*, 2010, pp. 23–32.

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

[166] P. Zhao *et al.*, "ILLIA: Enabling k-anonymity-based privacy preserving against location injection attacks in continuous LBS queries," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1033–1042, Apr. 2018.

[167] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1089–1107, Aug. 2010.

[168] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, to be published.

[169] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6190–6204, Sep. 2018.

[170] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017.

[171] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *Proc. IEEE IWCMC*, 2017, pp. 1338–1343.

[172] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.

[173] A. A. E. Hajomer, X. Yang, and W. Hu, "Secure OFDM transmission precoded by chaotic discrete Hartley transform," *IEEE Photon. J.*, vol. 10, no. 2, pp. 1–9, Apr. 2018.

[174] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017.

[175] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *Proc. IEEE PIMRC*, Montreal, QC, Canada, 2017, pp. 1–5.

[176] H. Li, X. Wang, and W. Hou, "Secure transmission in OFDM systems by using time domain scrambling," in *Proc. IEEE VTC Spring*, Dresden, Germany, 2013, pp. 1–5.

[177] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secure communication via untrusted switchable decode-and-forward relay," in *Proc. IEEE IWCMC*, 2017, pp. 1333–1337.

[178] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.

[179] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, 2015.

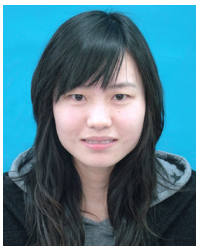
[180] S. Zakhary and A. Benslimane, "On location-privacy in opportunistic mobile networks, a survey," *J. Netw. Comput. Appl.*, vol. 103, pp. 157–170, Feb. 2018.

[181] D. Wu, Y. Zhang, L. Bao, and A. C. Regan, "Location-based crowdsourcing for vehicular communication in hybrid networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 837–846, Jun. 2013.

[182] K. Lin, J. Luo, L. Hu, M. S. Hossain, and A. Ghoneim, "Localization based on social big data analysis in the vehicular networks," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1932–1940, Aug. 2017.

[183] 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 Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[184] G. Yan, S. Olariu, J. Wang, and S. Arif, "Towards providing scalable and robust privacy in vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1896–1906, Jul. 2014.
[185] C. Liu, J. Luo, and Q. Pan, "A distributed location-based service discovery protocol for vehicular ad-hoc networks," in *Proc. Springer ICA3PP*, 2015, pp. 50–63.
[186] T. H. Luan, L. X. Cai, J. Chen, X. S. Shen, and F. Bai, "Engineering a distributed infrastructure for large-scale cost-effective content dissemination over urban vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1419–1435, Mar. 2014.
[187] T. H. Luan, X. S. Shen, F. Bai, and L. Sun, "Feel bored? Join verse! Engineering vehicular proximity social networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 3, pp. 1120–1131, Mar. 2015.
[188] N. Cheng *et al.*, "Opportunistic WiFi offloading in vehicular environment: A game-theory approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 7, pp. 1944–1955, Jul. 2016.
[189] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (NEMO) basic support protocol," Internet Eng. Task Force, Fremont, CA, USA, Rep. 3963, 2004, doi: 10.17487/RFC3963.
[190] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in LTE-advanced networks," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 29–39, Feb. 2017.
[191] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G HetNets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, Apr. 2015.
[192] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.
[193] C. Gosman, T. Cornea, C. Dobre, F. Pop, and A. Castiglione, "Controlling and filtering users data in intelligent transportation system," *Future Gener. Comput. Syst.*, vol. 78, pp. 807–816, Jan. 2018.
[194] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.
[195] Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 665–673, Jan. 2018.
[196] A. B. Sherif, K. Rabieh, M. M. E. A. Mahmoud, and X. Liang, "Privacy-preserving ride sharing scheme for autonomous vehicles in big data era," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 611–618, Apr. 2017.
[197] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.
[198] X. Zhang *et al.*, "Proximity-aware local-recoding anonymization with mapreduce for scalable big data privacy preservation in cloud," *IEEE Trans. Comput.*, vol. 64, no. 8, pp. 2293–2307, Aug. 2015.
[199] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.
[200] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, Nov. 2018.
[201] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 1, pp. 27–40, Jan. 2017.
[202] W. Xu *et al.*, "Internet of Vehicles in big data era," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 19–35, Jan. 2018.
[203] F.-Y. Wang *et al.*, "Parallel driving in CPSS: A unified approach for transport automation and vehicle intelligence," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 4, pp. 577–587, Sep. 2017.
[204] Y. Lv, Y. Chen, X. Zhang, Y. Duan, and N. L. Li, "Social media based transportation research: The state of the work and the networking," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 1, pp. 19–26, Jan. 2017.



Xiaojie Wang received the M.S. degree from Northeastern University, China, in 2011. She is currently pursuing the Ph.D. degree with the School of Software, Dalian University of Technology, Dalian, China. From 2011 to 2015, she was a Software Engineer with NeuSoft Corporation, China. Her research interests are vehicular social networks and network security.

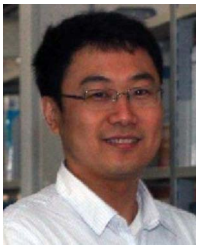
Zhaolong Ning received the M.S. and Ph.D. degrees from Northeastern University, Shenyang, China, in 2011 and 2014, respectively. He was a Research Fellow with Kyushu University, Japan, from 2013 to 2014. He is an Associate Professor with the School of Software, Dalian University of Technology, China. His research interests include social computing, vehicular social network, and network optimization. He has been serving as an Associate Editor for the *International Journal of Communication Systems* and IEEE ACCESS and the lead guest editors of *Computer Journal*, IEEE ACCESS, and *China Communications*.

MengChu Zhou (S'88–M'90–SM'93–F'03) received the B.S. degree in control engineering from the Nanjing University of Science and Technology, Nanjing, China, in 1983, the M.S. degree in automatic control from the Beijing Institute of Technology, Beijing, China, in 1986, and the Ph.D. degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1990. He joined the New Jersey Institute of Technology, Newark, NJ, USA, in 1990, where he is currently a Distinguished Professor of electrical and computer engineering. He has over 800 publications, including 12 books, over 460 journal papers (over 360 in IEEE TRANSACTIONS), and 28 book-chapters. His research interests are in Petri nets, intelligent automation, Internet of Things, big data, and intelligent transportation.

He has led or participated in over 50 research and education projects with total budget over $12M, funded by National Science Foundation, Department of Defense, NIST, New Jersey Science and Technology Commission, and industry. He was invited to lecture in Australia, Canada, China, France, Germany, Hong Kong, Italy, Japan, South Korea, Mexico, Saudi Arabia, Singapore, Taiwan, and USA, and served as a plenary/keynote speaker for many conferences. He is the Founding Editor of IEEE Press Book Series on Systems Science and Engineering, the Editor-in-Chief of the *IEEE/CAA Journal of Automatica Sinica*, and an Associate Editor of the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE INTERNET OF THINGS JOURNAL, and the *Frontiers of Information Technology & Electronic Engineering*. He served as an Associate Editor of the IEEE TRANSACTIONS ON ROBOTICS AND AUTOMATION, the IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, the IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS, the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, PART B: CYBERNETICS, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and the *IEEE/CAA Journal of Automatica Sinica*, the Managing Editor of the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, PART C: REVIEW AND APPLICATIONS, and an Editor of the IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING. He served as a Guest-Editor for many journals, including the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, and the IEEE TRANSACTIONS ON SEMICONDUCTOR MANUFACTURING. He was the General Chair of IEEE Conference on Automation Science and Engineering, Washington, DC, USA, in 2008, the General Co-Chair of 2003 IEEE International Conference on System, Man and Cybernetics (SMC), Washington, DC, USA, in 2003, the Founding General Co-Chair of 2004 IEEE International Conferecne on Networking, Sensing and Control, Taipei, in 2004, and the General Chair of 2006 IEEE International Conference on Networking, Sensing and Control, Ft. Lauderdale, FL, USA, in 2006. He was the Program Chair of 2010 IEEE International Conference on Mechatronics and Automation XiŠan, China, in 2010, the 1998 and 2001 IEEE International Conference on SMC, and the 1997 IEEE International Conference on Emerging Technologies and Factory Automation. He organized and chaired over 100 technical sessions and served on program committees for many conferences.

Dr. Zhou was a recipient of the Humboldt Research Award for U.S. Senior Scientists, the Franklin V. Taylor Memorial Award, and the Norbert Wiener Award from IEEE Systems, Man and Cybernetics Society. He is the Founding Editor of IEEE Press Book Series on Systems Science and Engineering. He is serving as the Vice President for Conferences and Meetings for IEEE Systems, Man and Cybernetics Society. He is a Life Member of the Chinese Association for Science and Technology—USA and served as its President in 1999. He is a fellow of International Federation of Automatic Control and American Association for the Advancement of Science.

Xiping Hu received the Ph.D. degree from the University of British Columbia, Vancouver, Canada. He is currently a Professor with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China. He is also the Co-Founder and the Chief Scientist of Erudite Education Group Ltd., Hong Kong, a leading language learning mobile application company with over 100 million users, and listed as top two language education platform globally. He has over 70 papers published and presented in prestigious conferences and journals, such as IEEE TETC/TVT/TII/IoT journal, ACM TOMM, IEEE COMST, *IEEE Communications Magazine*, IEEE NETWORK, HICSS, ACM MobiCom, and WWW. His research areas consist of mobile cyber-physical systems, crowdsensing, social networks, and cloud computing. He has been serving as the lead guest editors for the IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING and WCMC.



Lei Wang received the B.S., M.S., and Ph.D. degrees from Tianjin University, China, in 1995, 1998, and 2001, respectively. He is currently a Full Professor with the School of Software, Dalian University of Technology, China. He was a Member of Technical Staff with Bell Labs Research China from 2001 to 2004, a Senior Researcher with Samsung, South Korea, from 2004 to 2006, a Research Scientist with Seoul National University from 2006 to 2007, and a Research Associate with Washington State University, Vancouver, WA, USA, from 2007 to 2008. His research interests involve wireless ad hoc network, sensor network, social network, and network security. He has published over 90 papers in the above areas.

Yan Zhang (M'05–SM'10) received the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. He is currently a Full Professor with the Department of Informatics, University of Oslo, Norway. His current research interests include next-generation wireless networks leading to 5G, green and secure cyber-physical systems, such as smart grid, healthcare, and transport. He is an Associate Technical Editor of the *IEEE Communications Magazine*, an Editor of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, an Editor of the IEEE COMMUNICATIONS SURVEY & TUTORIALS, an Editor of the IEEE INTERNET OF THINGS JOURNAL, and an Associate Editor of IEEE ACCESS. He serves as the chair positions in a number of conferences, including the IEEE GLOBECOM 2017, the IEEE VTC-Spring 2017, the IEEE PIMRC 2016, the IEEE CloudCom 2016, the IEEE ICCC 2016, the IEEE CCNC 2016, the IEEE SmartGridComm 2015, and the IEEE CloudCom 2015. He serves as a TPC Member for numerous international conferences, including the IEEE INFOCOM, the IEEE ICC, the IEEE GLOBECOM, and the IEEE WCNC. He is the IEEE Vehicular Technology Society (VTS) Distinguished Lecturer. He is also a Senior Member of the IEEE ComSoc, the IEEE CS, the IEEE PES, and the IEEE VTS. He is a fellow of IET.

Fei Richard Yu (S'00–M'04–SM'08–F'18) received the Ph.D. degree in electrical engineering from the University of British Columbia in 2003. From 2002 to 2006, he was with Ericsson, Lund, Sweden, and a start-up in California, USA. He joined Carleton University in 2007, where he is currently a Professor. His research interests include wireless cyber-physical systems, connected/autonomous vehicles, security, distributed ledger technology, and deep learning. He was a recipient of the IEEE Outstanding Service Award in 2016, IEEE Outstanding Leadership Award in 2013, the Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly, Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at IEEE ICNC 2018, VTC 2017 Spring, ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009, and International Conference on Networking 2005.

He serves on the editorial boards of several journals, including the Co-Editor-in-Chief for *Ad Hoc & Sensor Wireless Networks*, an Area Editor for the IEEE COMMUNICATIONS SURVEYS & TUTORIALS, a Lead Series Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING. He has served as the technical program committee co-chair of numerous conferences. He is a registered Professional Engineer in the province of Ontario, Canada and a fellow of the Institution of Engineering and Technology. He is a Distinguished Lecturer, the Vice President (Membership), and an Elected Member of the Board of Governors of the IEEE Vehicular Technology Society.

Bin Hu (M'05–SM'10) is currently a Professor and the Dean of the School of Information Science and Engineering, Lanzhou University, an Adjunct Professor with Tsinghua University, China, and a Guest Professor with ETH Zurich, Switzerland. His work has been funded as a PI by the Ministry of Science and Technology, National Science Foundation China, European Framework Programme 7, EPSRC, and HEFCE, U.K. He has published over 100 papers in peer reviewed journals, conferences, and book chapters, including *Science*, the *Journal of Alzheimer's Disease*, *PLoS Computational Biology*, IEEE TRANSACTIONS, IEEE Intelligent Systems, AAAI, BIBM, EMBS, CIKM, and ACM SIGIR. He has served as the chair/co-chair in many IEEE international conferences/workshops, and an Associate Editor in peer reviewed journals on *Cognitive Science and Pervasive Computing*, such as the IEEE TRANSACTIONS ON AFFECTIVE COMPUTING, *Brain Informatics*, *IET Communications*, *Cluster Computing*, *Wireless Communications and Mobile Computing*, the *Journal of Internet Technology*, and Wiley's *Security and Communication Networks*. He is also IET Fellow, co-chairs of IEEE SMC TC on Cognitive Computing, a Member-at-Large of ACM China, and the Vice President of International Society for Social Neuroscience (China Committee).