INVITED PAPER

5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy

This article reviews the architecture and the use cases of 5G V2X; studies a series of trust, security, and privacy issues in 5G V2X services; and discusses the potential attacks on trust, security, and privacy in 5G V2X.

By Rongxing Lu, *Senior Member IEEE*, Lan Zhang, *Student Member IEEE*, Jianbing Ni, *Member IEEE*, and Yuguang Fang, *Fellow IEEE*

ABSTRACT | 5G is emerging to serve as a platform to support networking connections for sensors and vehicles on roads and provide vehicle-to-everything (V2X) services to drivers and pedestrians. 5G V2X communication brings tremendous benefits to us, including improved safety, high reliability, large communication coverage, and low service latency. On the other hand, due to ubiquitous network connectivity, it also presents serious trust, security, and privacy issues toward vehicles, which may impede the success of 5G V2X. In this article, we present a comprehensive survey on the security of 5G V2X services. Specifically, we first review the architecture and the use cases of 5G V2X. We also study a series of trust, security, and privacy issues in 5G V2X services and discuss the potential attacks on trust, security, and privacy in 5G V2X. Then, we offer an in-depth analysis of the state-of-the-art strategies for securing 5G V2X services and elaborate on how to achieve the trust, security, or privacy protection in each strategy. Finally, by pointing out several future research directions, it is expected to draw more attention and efforts into the emerging 5G V2X services.

KEYWORDS | 5G vehicle-to-everything (V2X) services; challenges; privacy; security; solutions; trust.

I. INTRODUCTION

Vehicle-to-everything (V2X) communication [1] is the key enabler for connected vehicles that have great potential to prevent traffic accidents and save lives by allowing the vehicles to "hear" the broadcasting messages from the surrounding environment. To gear toward safety, many critical information is conveyed to the vehicles, regarding inclement weather, road conditions, traffic accidents, approaching pedestrians, and the dangerous activities of nearby vehicles [2]. This technique also can improve the comfort of passengers and the energy efficiency of road travel and provide convenience to drivers with the connectivity to the Internet and the driving-through systems.

To build the connectivity of vehicles, LTE and LTE-advanced, augmented with multiaccess edge computing, provide flexible and cost-effective solutions for accelerating the adoption of V2X communications on the way to 5G [3]. Due to the advantages of high data rate, massive device connectivity, and low service latency, 5G has been widely adopted to support a large variety of V2X use cases, including vehicle platooning, remote driving, video and map sharing, and cooperative collision avoidance, which bring significant convenience and safety improvement for passengers. In 5G V2X systems, several advanced techniques, e.g., software-defined network (SDN), network function virtualization (NFV), network slicing, and mobile edge computing (MEC), have been used to extend the 4G LTE or LTE-advanced. 5G new radio (NR) [4] has also been developed to provide observed enhancements on flexibility, scalability, and efficiency of power usage and spectrum.

The connectivity of vehicles to everything on roads does offer diverse benefits [5], but it also creates a variety of

Manuscript received July 10, 2019; revised September 23, 2019; accepted October 10, 2019. Date of publication November 13, 2019; date of current version January 22, 2020. *(Corresponding author: Jianbing Ni.)*

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rlu1@unb.ca).

L. Zhang and **Y. Fang** are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: lanzhang@ufl.edu; fang@ece.ufl.edu).

J. Ni is with the Department of Electrical and Computer Engineering, Queen's University, Kingston, ON K7L 3N6, Canada (e-mail: jianbing.ni@queensu.ca).

Digital Object Identifier 10.1109/JPROC.2019.2948302

serious security and privacy concerns. Wireless interfaces on vehicles create the possibility for hackers to remotely access vehicles. The success of killing a jeep on the highway in 2015 witnessed the potential security risks of smart vehicles, which results in serious injury or even death [6]. The vulnerability of remote control function on smart vehicles has already raised huge concerns to drivers. The security issues of vehicles become more serious when they are smart and connected, which would have the same story with smartphones that are facing huge security challenges. Even worse, the network infrastructure in 5G suffers from different kinds of cyberattacks, which may result in data exposure and corruption [7]. Vehicles become data centers on wheels nowadays; the carried data, such as the GPS data and V2X service data, are sensitive from the perspectives of drivers. As the connected vehicles become a central part of our digital life, it is of importance to address the security and privacy issues, thereby makes drivers feel safe to enjoy various V2X services via 5G systems.

In this article, we start with the architecture and use cases of 5G V2X services. 5G V2X is a new layered paradigm with extended connectivity via deployed sensors in vehicles and on the roads and the remote V2X servers. We then exam the trust, security, and privacy issues in each layer of the 5G V2X architecture, which are exposed to a variety of cyberattacks, ranging from well-studied attacks, such as denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, and eavesdropping attacks, to special attacks aiming to corrupt a property of V2X communications, such as the inference attack and identity revealing attack that compromise the privacy of vehicles. To address these trust, security, and privacy issues, the extensive and comprehensive analyses of potential strategies are presented in a top–down approach. Finally, we present several future research directions to stimulate more efforts on trust, security, and privacy in 5G V2X services. This article focuses on the trust, security, and privacy threats in 5G V2X and explores the potential strategies to enhance the reliability of V2X communications on 5G network, which differentiate this article from the existing surveys that either review the communication techniques in 5G V2X [8], [9] or overview the authentication or privacy preservation mechanisms in 5G V2X [7], [10], [11].

II. 5G V2X: AN OVERVIEW

In this section, in order to deal with the security-related issues, we overview the 5G V2X architecture, identify the types of 5G V2X communications, and discuss some potential use cases of 5G V2X.

A. 5G V2X Architecture

According to 3GPP TS 23.501 [12], 3GPP TR 23.886 [13], and 3GPP TS 23.287 [14], 5G V2X architecture consists of four network layers, i.e., 5G access network, network edge, 5G core network, and data network, as shown in Fig. 1. The 5G access network is comprised of a next-generation radio access network (NG-RAN) or/and non-3GPP access network connecting 5G core network and user equipment (UE), such as vehicles, infrastructure and sensors on roads, and mobile phones carried by pedestrians. 5G V2X communications include two operation modes, PC5 and LTE-Uu. Proximity-based service discovery is used by V2X for supporting UE. For PC5 and LTE-Uu, each vehicle is equipped with the radio resources and the USIM card. 5G NR is a key supplementary of LTE V2X.

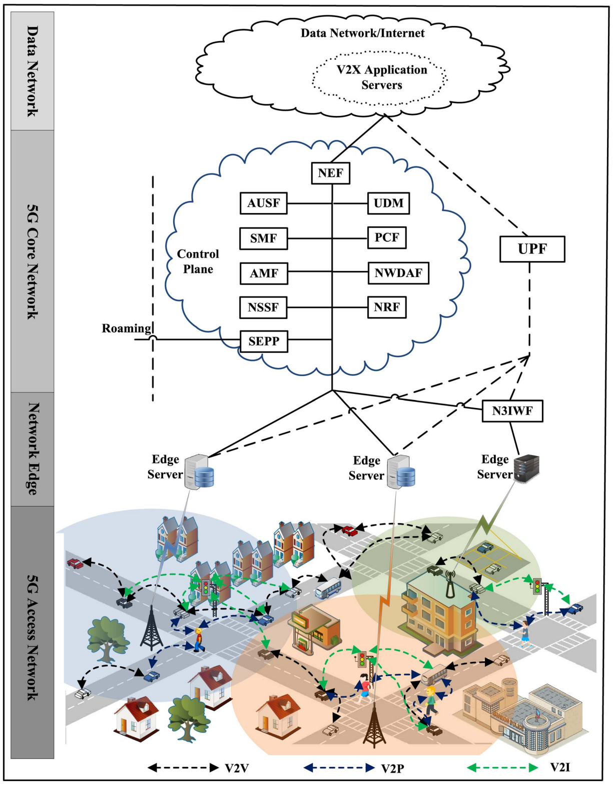


Fig. 1. ***Architecture of 5G V2X services.***

Edge servers are located on the top of NG-RAN and non-3GPP access network, i.e., the network edge. The computing and storage resources and virtual network functions are deployed at the edge of the access network to support delay-sensitive or location-aware V2X services, such as road surface ice detection, video and map sharing, and vehicle platooning. These resources are usually virtualized to be isolated virtual machines (VMs) by a local controller, such that the whole access network is divided into several slices for different V2X services. Specifically, multiple network slices can be deployed to deliver the same features for different UEs or different V2X services for the same set of UEs, with different service/slice types. Non-3GPP access networks shall be connected to the 5G core network through a non-3GPP interworking function (N3IWF). To secure the communication between N3IWF and UE, IPSec tunnels are built over the untrusted non-3GPP network.

The 5G core network is innovated to enable mobile data connectivity and services based on emerging technologies, such as SDN and NFV. By separating the user plane function (UPF) from the control plane function (CPF), the 5G core becomes independent, scalable, and flexible. UPF includes traffic usage reporting, data forwarding, and transport-level packet marking. CPF manages the packet processing in UPF by provisioning a set of rules in sessions, i.e., routing rules, packet detection rules, policy control, and charging rules. These functionalities are virtualized into several individual functions, including authentication server function (AUSF), access and mobility management function (AMF), session management function (SMF), network slice selection function (NSSF), unified data management (UDM), network data analytics function (NWDAF), and security edge protection proxy (SEPP). Most of these functions are responsible for the authorization and authentication of network access for UEs. Specifically, AMF manages UE registration, access authentication, and authorization; SMF includes session management, IP address management, selection and control of UP; UDM generates primary authentication credentials and manages user identification and subscription; AUSF supports authentication for 3GPP access and untrusted non-3GPP access; and SEPP is a nontransparent proxy that supports message filtering and policing for inter-PLMN and provides key management, mutual authentication, and cipher suites negotiation for roaming UEs. NWDAF provides slice-specific network data analytics for service providers, and NSSF selects the set of network slice instances serving users and determines the Network Slice Selection Association Information (NSSAI) corresponding to applicable network slice instances and the set of AMF to be used to serve UEs. Several security solutions are offered to guarantee authentication, discovery, authorization, integrity, and privacy [15]. Primary authentication and key agreement based on the EAP-AKA protocol enable mutual authentication between the UE and the serving network and offer key materials in subsequent security procedures. According to the key hierarchy generation framework, 11 secret keys are derived and distributed to the UE, and each key is used to secure a network function, including AMF in the serving network, AUSF for the home network, and the UP traffic. The Internet Key Exchange (IKE) protocol is leveraged to secure non-3GPP access to the 5G core network. IPsec Encapsulating Security Payload (ESP) and IKE certificates-based authentication are adapted to protect the nonservice-based interfaces, and the TLS protocol is suggested to guarantee secure communications through the service-based interfaces.

The 5G core network connects to the external data network, i.e., the Internet, to offer a variety of appealing V2X services to UEs, including remote driving, autonomous driving, and dynamic ride sharing. To reduce the latency of V2X services, V2X servers leverage the computing and storage resources at the network edge for computation offloading and data caching.

B. Types of 5G V2X Communications

5G V2X communications can be roughly divided into two types: 1) device-to-device communications, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) and 2) device-to-network communications, i.e., vehicle-to-network (V2N).

1) *V2V:* When two vehicles are in close proximity, they can directly communicate with each other. V2V mainly aims for improving road safety, e.g., collision avoidance; thus, low latency and high reliability are necessary for such V2V communications.
2) *V2I:* When a vehicle gets into the radio range of a roadside unit (RSU), they can exchange and share some delay-insensitive information, e.g., collected traffic data for large-scale traffic monitoring in the uplink and possible infotainment data in the downlink. Since a vehicle usually does not stop within the radio range of RSU for a long time, short-lived and high data rate connections are featured in V2I communications.
3) *V2P:* When a vehicle approaches pedestrians crossing a road or an intersection, V2P direct communication will be used to exchange position, speed, and direction information, which will be used for predicting the possibility of collision and alerting both drivers and pedestrians to avoid potential traffic accidents.
4) *V2N:* As one type of device-to-network communications, V2N allows vehicles to communicate with remote servers for various services, e.g., real-time traffic, weather, and customized navigation.

C. Use Cases of 5G V2X

Due to rich information exchange/sharing between vehicles and vehicles and between vehicles and pedestrians, infrastructure, and/or remote servers, 5G V2X significantly transforms the future mobility on the road and can greatly improve the road safety and traffic efficiency, provide infotainment services, and maximize efficient use of road and other transportation infrastructure. According to [2], use cases of 5G V2X can be divided into the following few categories: cooperative awareness, cooperative sensing, cooperative maneuvering, awareness of vulnerable road users (VRUs), improving traffic efficiency, and teleoperated driving.

1) *Cooperative Awareness:* As one use case of 5G V2X, cooperative awareness aims to support vehicles on the road by providing knowledge about the surroundings and relies on the information exchange enabled by V2V/V2I communications [16]. Cooperative awareness is crucial for improving the road safety, and typical examples include emergency vehicle warning, emergency electronic brake light, forward collision warning, wrong driving warning, and precrash sensing warning.
2) *Cooperative Sensing:* To improve the quality and reliability of individual detections and increase vehicles'

environmental perception, sensor data and objective information from radars, cameras, and other sensors will be exchanged among neighbor vehicles. Cooperative sensing is also based on V2V/V2I communications, which is the one essential feature in cooperative autonomous driving [17].

3) *Cooperative Maneuvering:* In many use cases of 5G V2X, including cooperative collision avoidance, cooperative lane change, vehicle platooning, and autonomous driving [2], V2V-/V2I-based cooperative maneuvering enables a group of autonomous vehicles to drive coordinately according to a common centralized or decentralized decision-making strategy [17].
4) *Awareness of VRUs:* VRUs are referred to road users who have a high casualty rate and should be paid special attention to the road. The awareness of VRUs, as another use case of 5G V2X, relies on the V2P communications, which provides the ability to detect possible safety conditions due to the presence of VRUs [18], [19].
5) *Improving Traffic Efficiency:* Improving traffic efficiency is also a use case of 5G V2X, which is supported by both V2I and V2N communications. In general, the information shared between vehicles and infrastructure or remote servers is not delay-sensitive, but this information is helpful for traffic efficiency. For example, in a customized navigation scenario, each vehicle can update its location, status, and road condition to the traffic management server every few seconds, and then, the server will respond with the updated digital map back to the vehicle [2].
6) *Teleoperated Driving:* As a use case of 5G V2X, teleoperated driving uses the V2N communications to remotely control a vehicle in normal traffic. Provided with information about a vehicle's environment, including a video feed, a GPS position on a map, and current weather conditions, a driver can remotely control a car from the control center [2]. Note that the development of a fully autonomous vehicle is on the way, but it is still in the early testing stage, and thus, teleoperated driving can be regarded as a solution in the transition phase.

III. KEY CHALLENGES IN SECURE 5G V2X SERVICES

In this section, we are ready to discuss the key challenges on trust, security, and privacy in 5G V2X services.

A. Trust Issues in 5G V2X Services: Issues and Attacks

The ubiquitous network connectivity on vehicles creates new possibility and enlarges attack surface for hackers to compromise network devices in the 5G V2X architecture, which brings huge concerns to the entities that connect to 5G networks. Moreover, the design flows, misconfiguration, and implementation bugs may cause system failures. The reliability of 5G systems and V2X services is in high risks. Even worse, with personal incentives, it is difficult to guarantee that all the entities in 5G V2X behave honestly and follow the regulations. Facebook's troubles [20] and Snowden's revelations [21] have decreased human's trust in a single institution or government. The trust of 5G V2X systems become a vital issue, while the success of 5G V2X heavily depends on the users' perception [22]. Trust management, which is typically used to gauge the security level of the whole system as well as the effectiveness of security policies, is deeply explored to develop secure V2X services [23], [24]. To ensure trust management, all system entities in 5G V2X architecture should register their real identities through a trust authority (TA), where the certificates (e.g., certified public keys) are managed, i.e., issued, stored, and revoked, by TA [25], [26]. However, it is worth noting that a certificate can only verify that a public key is owned by a registered entity, while the trustworthiness of that entity can be hardly guaranteed. Thus, in addition to certificate-based trust strategies, other strategies, such as the recommendation/reputation-based trust strategies, should also be jointly considered. Moreover, due to the various V2X services, the relative static roles found in conventional cellular systems are much more fluid in 5G V2X systems. For example, a vehicle enjoying the V2N service can also be a server to another vehicle and pedestrian for providing V2V and V2P services, respectively. Thus, V2X trust management becomes much more challenging, which should recognize a set of roles and the corresponding responsibilities that each system entity might take. In the following, we identify the representative trust attacks in 5G V2X systems.

1) *Bad Mouth Attacks:* A bad mouth attack compromises normal system entities and provides dishonest recommendations to frame up good entities and/or boost the trustworthiness of malicious entities [27]. For example, a malicious vehicle may defame surrounding legitimate vehicles, which might force those innocent vehicles to be expelled from the system [23].
2) *Conflicting Behavior Attacks:* Given the fact that a trust is a dynamic event, a malicious entity may have conflicting behaviors, i.e., performing well or badly alternatively, to cover its identity while causing damages [24]. Specifically, an attacker may have time-domain inconsistent behaviors, e.g., an attacker may utilize the fact of V2X channel changing to cover its bad behaviors intentionally, which is also named as ON–OFF attack. In addition, the conflicting behaviors of an attacker may happen toward two different entity groups, where two groups may have conflicting opinions about the attacker, which can lower the trustworthiness between these two groups. The conflicting attacks subvert trust management by adapting to the dynamic properties of trust in V2X systems.
3) *Blackhole Attacks:* A blackhole attack, also known as packet drop attack, is a type of DoS attack, where a malicious entity discards the packets that should

be relayed [24]. In multihop routing-based V2X services, a malicious entity publicizes its availability of fresh routes regardless of checking its routing table. Moreover, the malicious entity will immediately reply to any request before the response from legitimate system entities [27].

4) *Sybil Attacks:* If a malicious entity can forge several fake identities, the Sybil attack occurs [7]. The faked identities can be used to take the blame of bad behaviors, while the real identity can be automatically protected.

B. Security Issues in 5G V2X Services: Issues and Attacks

In this section, we present a systematic view of various security issues in 5G V2X services and particularly identify some possible existing attacks.

1) Security Issues in 5G V2X: 5G V2X services seamlessly connect V2X and 5G communications, which, thus, greatly increase the attack surfaces. In general, the following basic security requirements should be satisfied.

1) *Confidentiality:* The confidentiality is to prevent the disclosure of information to unauthorized entities so that only intended authorized users can access the data.
2) *Authenticity:* The authenticity is to confirm the true identity of an entity to distinguish authorized users from unauthorized users in 5G V2X services.
3) *Integrity:* The integrity is to assure the information transmitted accurate and reliable against any falsification and modification from unauthorized entities.
4) *Availability:* The availability is to ensure the authorized users can always access the V2X services upon request, and the violation of availability refers to as DoS, which makes the services unaccessible to the users.

2) Security Attacks in 5G V2X: In the following, we review some possible attacks in 5G V2X.

Attacks in V2X Communications:

1) *Eavesdropping:* Due to the broadcast nature in wireless communication, message exchanged could be easily eavesdropped by attackers. For example, an attacker can easily install some receivers on the road to eavesdrop the messages transmitted by vehicles, pedestrians, and infrastructure [28]. However, even though all messages are encrypted, it is still possible for an attacker to infer the source and the destination of messages [29].
2) *Message Forgery:* An attacker could fabricate bogus V2X messages or false warnings to mislead the surrounding vehicles, pedestrians, and infrastructure to take wrong actions, which possibly causes some road accidents [7]. To deal with the forgery attacks, V2X entities check the integrity or validity of messages before accepting them.
3) *Jamming:* An attacker, no matter whether it is internal or external, attempts to viciously and continuously consume spectrum resources, e.g., by sending misleading and bogus V2X messages [7], to exhaust the available spectrum resources to disrupt the normal V2X communications. Thus, legitimate vehicles cannot gain available resources to transmit their data, making V2X services unavailable.
4) *Impersonation:* An attacker attempts to impersonate another legitimate vehicle by using a false vehicle identity. To successfully launch this attack, the attacker should have the capability to gain/forge the credentials of other legitimate vehicles [30]. More than often, impersonation attacks are the first step for other sophisticated attacks.
5) *Replay Attacks:* An attacker may resend V2X messages previously broadcast by other vehicles, pedestrians, and infrastructure to disrupt the traffic flow, which can cause the receiving vehicles to improperly react to nonexisting road conditions [30].
6) *MITM Attacks:* An attacker is positioned between two V2X communication entities, sniffs any exchanged information between them, and attempts to impersonate one of them [31]. This attack is disastrous because once it is successful and it will disclose the sensitive information and even lead to loss of property and human lives on the road.
7) *Sybil Attacks:* An attacker generates multiple identities and uses each identity to send different messages to other vehicles, pedestrians, and infrastructure. The goal of Sybil attacks is to make other vehicles, pedestrians, and infrastructure to believe that the messages indeed come from different vehicles, which, thus, misleads them to take the wrong action [7].

Attacks on Network Edge:

1) *Location Spoofing:* An edge server usually provides some location-based services in a specific area. However, an attacker can gain access to a service that is not valid at his/her current location by making him/her appear to be located somewhere that is covered by the service [7].
2) *DoS Attacks:* DoS attacks might be one of the most dangerous threats since they will hurt the availability of services and may cause traffic accidents. In addition, edge servers are more vulnerable to DoS attacks as they are resource-restricted.
3) *Fake Attacks:* An adversary may fake an edge server, such as a base station, a roadside infrastructure, or a local server to attract victims to connect to the faked edge server, which may result in the exposure of sensitive information for the victims [32], including access credentials and passwords.

Attacks on 5G Core Networks:

1) *Hijacking Attacks:* Hijacking attack on the 5G-core network is unique, which particularly exploits the vulnerability of SDNs. Once the vulnerabilities are exploited, the attacker will hijack the location of

various hosts, leading to the controller being overloaded by handling a large number of spoofed packets to paralyze V2X services [33].

2) *Saturation Attacks:* In the 5G core network, the saturation attack is referred to the situation that an attacker, after observing that OpenFlow networks lack the scalability between the data and control planes, will craft an inbound stream of flow requests to inundate communications between the controller and switches [34], so as to make the 5G V2X services unavailable.

3) *Link Fabrication Attacks:* In the 5G core network, OpenFlow uses the OpenFlow Discovery Protocol (OFDP) for topology management so as to build the entire network and handle the dynamics of a network. In particular, OpenFlow controllers use Link Layer Discovery Protocol (LLDP) packets to discover links among OpenFlow switches. The link fabrication attack is referred to the situation that an attacker injects fake LLDP packets between two switches to fabricate a nonexisting internal link, which will result in a DoS attack to compromise the 5G V2X services [35].

4) *Unauthorized Slice Accesses:* In the 5G core network, networking slices may be vulnerable to an unauthorized slice access attack, i.e., if a slice-specific authentication is not performed, an unauthorized attacker may consume resource of a network slice and cause DoS to legitimate V2X services [36]. To achieve an authorized network slice access, isolation is also crucial. Otherwise, an attacker, who has access to one slice, could launch an attack to other slices.

Attacks on Data Network/Internet:

1) *DoS Attacks:* In 5G V2X communications, the V2X communication will connect a large number of nodes to the data network to effectively improve the user experiences. However, those user devices might be compromised and used for initiating the DoS attacks, which will greatly degrade the performance of the target 5G V2X service [37].

2) *Malware Injection:* While the cloud computing in data networks can help deploy 5G V2X services efficiently, improper operations may introduce vulnerabilities into their applications, such as using outdated tools to maintain and manage these services, and these vulnerabilities could be exploited by attackers to inject some malwares to control the cloud server and even affect V2X users [38].

C. Privacy Issues in 5G V2X Services: Issues and Attacks

In this section, we present a series of privacy issues in 5G V2X services and identify some possible attacks.

1) Privacy Issues in 5G V2X: Due to the pervasive nature of 5G V2X services on roads, it is essential that the users/subscribers have their control over their privacy that may be leaked to the service providers, 5G core, edge servers, or other parties on roads. Here, we provide a list of privacy concerns in 5G V2X architecture.

1) *Identity Privacy:* Identity privacy leakage means the disclosure of the identity information, such as the name, address, occupation, telephone number, license number, visa number, and public-key certificate, which can be directly linked to a specific user. In 5G V2X, the subscriber's identity may be exposed to different layers. The international mobile subscriber identity (IMSI) of a mobile subscriber can be identified by eavesdroppers for tracking purposes in the 5G core network [39].

2) *Content Privacy:* Content privacy concerns the sensitive information in the disclosed content with different types, e.g., documents, videos, radios, and pictures [40], the exposure of which may result in the user privacy breaches. In 5G V2X, if not protected, the users' data may be leaked to others.

3) *Contextual Privacy:* Contextual privacy leakage refers to the situation that an attacker is able to link the source and the destination of a packet [41]. A global eavesdropper may be able to trace the message from the source to the destination in the V2X communication to learn the service that a specific user is accessing.

4) *Location Privacy:* Location privacy leakage refers to the situation that an adversary has the capability to control and access to the current and past locations of a specific user [42]. Current location-based services require the locations of the users who are willing to access their services, such as Google Maps and restaurant recommendation services.

2) Privacy Attacks in 5G V2X: To capture the private information, various attacks and malwares can be utilized to eavesdrop, monitor, and sniffer the messages and activities of victims. The traditional attacks on content privacy include eavesdropping attacks, MITM attacks, and impersonation attacks, which have been discussed in Section III-B. Some advanced attacks are also mentioned in the literature.

1) *Packet Analysis Attacks [43]:* An adversary identifies the sender's identity by analyzing a packet, e.g., the packet content recovery and the source inference, after capturing the packet.

2) *Packet Tracing Attacks [43]:* An adversary wanders and eavesdrops around the vehicular communications, and therefore, the source and the destination of the packet can be traced. In this attack, the adversary does not need to recover the content to infer the source and destination.

3) *Linkage Attacks (Correlation Attacks) [44]:* An adversary links the pseudonyms of a user based on the information exposed to the public, such as reputations and locations. In this way, although the user's real identity is hidden, the adversary still can group the pseudonyms that belong to the same user and learn more knowledge about the user, such as the trajectory.

4) *Movement Tracking Attacks [45]:* An adversary can capture a large number of messages in a certain area and attempt to trace a vehicle based on its physical positions and moving patterns by analyzing the captured messages.
5) *Identity Revealing Attacks [46]:* An adversary may collect vehicle's sensitive information or routine traffic messages to predict the identity, moving path, and physical position of a specific vehicle.
6) *Collusion Attacks [47]:* An adversary is capable of collaborating with other adversaries to learn more information about the target user than that it can acquire by itself, such as recovering the protected information or identifying the target user.
7) *Inference Attacks [48]:* An adversary gains knowledge about a subject by recognizing the differences between multiple subjects based on a large number of collected data from many individuals, and its goal is to identify the subject after which the adversary could profit from recovering the subject.
8) *Deanonymization/Reidentification Attacks [49]:* An adversary attempts to reidentify the owners of the data among the large volumes of acquired data, in which their owners' identity information have been removed, by analyzing the corelations and differences of the data.

IV. KEY STRATEGIES TO SECURE 5G V2X SERVICES

In this section, we present a comprehensive survey on the existing strategies that are potential to address the trust, security, and privacy issues in 5G V2X services.

A. Trust Management Strategies in 5G V2X Services

To enable secure and private V2X services, trust management strategies have been extensively investigated to manage the aforementioned trust issues. Considering the layered paradigm of 5G V2X systems, we review the trust management strategies proposed for each layer, respectively, as follows.

1) Trust Management Strategies in Data Networks/Internet: In data networks/Internet, various 5G V2X services are managed by different service providers. The trust relationship between a service provider and its users, such as vehicles and pedestrians, is the premise to develop a V2X service. Usually, a V2X service is initiated by the request from the user side, where the legality of the service provider needs to be verified at the beginning. The service providers are usually assumed to be honest but curious, i.e., semitrusted, and thus, during the identity authentication process, users should also prevent leaking their private information to the service providers, which will be further discussed in Section IV-C.

One classical identity authentication strategy is based on certification, which is proposed by the X.509 standard [50], [51]. Since an X.509 certificate binds the ownership of a public key and the named subject of the certificate. Trusted certificates are issued by a certificate authority or certification authority (CA). This allows system entities, i.e., service providers and users, to authenticate each other by using the signatures or assertions made based on the private key that corresponds to the certified public key for offline trust verification. To effectively manage the assigned certificates, the certificate revocation mechanisms are developed, where either the compromised or expired entity should be revoked by putting their existing certificates into the certificate revocation list (CRL) [50]. Since the CRL lookup is time-consuming to expel the revoked system entity, especially with a large number of system entities, great efforts have been made to accelerate the certificate revocation process, such as establishing the distributed CRL.

Although the aforementioned certificate-based trust strategies can be regarded as the first line of defense, the registered system entity may still send untrustworthy information, due to the defective sensors, computer viruses, selfish or malicious reasons, and so on. For example, in the parking navigation service, a legitimate vehicle may send faked parking information to guarantee its own parking space. Therefore, users in V2X services are similar to that of mobile social communications, whose trustworthy relationships can be managed in the self-organized social network strategies [52], [53]. The trust relationship in mobile social communications can be established in either centralized or distributed fashion. In a centralized scheme, the social connection between two system entities is established and maintained via existing cellular technologies. The established trust relationship among vehicles will be announced from the central controller to the whole system. On the contrary, the social relationship can be locally established among nearby system entities via distributed connections, such as Dedicated Short-Range Communications (DSRC) technology. As commonly observed, the centralized scheme is timely and reliable, while the distributed scheme is cost-effective and infrastructure free [52]. In addition, the direct trust obtained by a system entity will be propagated to its neighbor entities, where the topology- and evidence-based trust propagation methods have been fully explored. Sun *et al.* [23] propose to manage the trust propagation by jointly evaluating a system entity's action and recommendation trust scores, where these two scores are maintained separately to defend trust attacks, such as bad mouth attacks and newcomer attacks. Considering the dynamic nature of trust and reputation, the reevaluation and reputation fading, as well as redemption mechanisms, are introduced in [54], which can defend trust attacks, such as blackhole attacks conflicting behavior attacks. Sun *et al.* [53] further evaluate the uncertainty of trust using entropy, where the continuous trust value does not need to be transitive, matching the trust characteristics in V2X systems, and thus, trust attacks, such as Sybil attacks, can be effectively resolved.

2) Trust Management Strategies in 5G Core Networks: In 5G core networks, cellular communication services are managed by cellular operators. Since 5G cellular systems are evolved from previous generations for several decades, the trust management in 5G core networks is sophisticated for identifying and authenticating subscribers of 5G V2X services, such as vehicles and pedestrians [10], [55]. Evolved from the 4G cellular systems, strong cryptographic primitives, such as authentication protocols and key generation functions, are adopted to increase trust between communicating entities in 5G core networks. Instead of relying on physical USIM card, certificates, preshared keys, and token cards are allowed to use in 5G AKA protocols and EAP framework [56]. These authentication factors can provide different security levels for the V2X service.

In addition, the evolved new technologies in 5G systems, such as SDN and NFV, also improve the trustworthiness of 5G core networks by enhancing the system resilience [1], [57]. For example, the network slicing, enabled by SDN and NFV technologies, isolates groups with different network functions, where different network slicing matches different trust requirements of various 5G V2X services. Thus, safety- and entertainment-related V2X services with different trust requirements can be, respectively, operated in different network slicings, where the trust attacks toward entertainment-related V2X services will not affect the trustworthiness of safety-related V2X services [7].

3) Trust Management Strategies at Network Edge: Unlike conventional cloud servers that require unilateral trust, the introduced edge servers may be owned by different V2X service providers or cellular operators, which enables finer grained trust from users to servers [58]. Existing authentication strategies, such as the aforementioned trusted certificates, should be implemented to authenticate the edge servers and users in every trust domain. Meanwhile, various factors, such as the geographical location and resource ownership, might be considered in defining the authentication policies. For example, V2X services with a higher priority may be allowed to occupy additional resources when migrating VMs [59]. Due to the limited connectivity to CA, the infrastructure-based trust strategies might not be applicable for some parts of the infrastructures, where edge servers should be able to exchange compatible trust information [60].

The trustable edge servers may coexist with the malicious ones in a distributed edge server overlays. Distributed trust evaluation and management have been studied based on blockchain [61]. Blockchain is an open, distributed, and transparent public ledger used to maintain a continuously growing list of transactions in cryptocurrency, e.g., Bitcoin and Ethereum. For example, Bitcoin blockchain is a chain of blocks and managed by a group of nodes in a peer-to-peer network. The approach to building the blockchain with MEC was first proposed in [62], and the built blockchain is used to enhance the trust and support secure handover between edge nodes [63]. Blockchain removes trust dependence on a centralized party, which reduces the risk of single-point failure. The trust of each vehicle can be quantified, and reliable data management can, thus, be realized based on blockchain [64].

4) Trust Management Strategies in V2X Communications: In 5G V2X communications, different types of communications, including V2V, V2I, V2P, and V2N, coexist. In addition to the centralized trust management, e.g., for V2I/V2N communications, there are V2X services, e.g., V2V and V2P, rely on local information sharing and local decision making, whose trustworthiness should be managed in a distributed fashion. Therefore, both infrastructure-based centralized strategies, i.e., certificate-based trust strategies, and self-organizing-based social network strategies can be adapted in corresponding V2X communications, which have already been discussed in trust strategies for data networks [52], [54], [65]. However, different from the clear roles of entities in data networks, i.e., either a service provider or a user, a system entity in V2X communications may have different roles. For example, the receiving vehicle in a V2V communication may be the transmitter of a V2P communication at the same time. Thus, trust management should holistically evaluate the trustworthiness of each system entity based on different roles in V2X communications.

In addition, to handle different V2X communication scenarios, 5G V2X communications may coexist with DSRC-based V2X communications. When shifting from 5G V2X connections to DSRC-based V2X connections, the existing public key and certificate infrastructure can be reused for network access authentication. Furthermore, considering the high mobility in V2X communications, continuous trust management, based on the mobility support of previous 3GPP generations, has been adapted in 5G V2X systems. For example, in 4G cellular systems, each handover operation will lead to the security reconfiguration, which results in transmission interruptions and complex implementations. On the contrary, 5G cellular systems reuse the same configuration across handovers, where the security-sensitive functions are processed in the central unit of the base station.

B. Security Strategies in 5G V2X Services

After examining the trust management in 5G-V2X services, we proceed to look into security issues.

1) Security Strategies in Data Networks/Internet: Based on the potential attacks, in the following, we summarize the security strategies for the 5G V2X data networks.

1) *DoS Attacks:* DoS attacks aim to prevent the legitimate V2X entities from accessing the data network services, and they may have a catastrophic impact on the network performance. In 5G V2X data networks, DoS attacks can be launched by external

attackers or a large number of V2X internal entities (e.g., vehicles) connected to the data networks, which may be compromised and used for initiating DoS attacks. Since there are wide ranges of possibilities for DoS attacks, there is no general solution to these problems. Traditional DoS attack–defense mechanism includes analyzing data in the network. Specifically, if a message is found to be malicious, it will be rejected. Otherwise, it will be accepted [66]. Based on when the defense mechanism is applied, the solutions for addressing DoS attacks can be classified into three categories. First, before DoS attacks, some techniques can be applied to prevent the malicious traffic, including applying anomaly and signature-based detection methods, protecting data network with the Internet service provider, placing filtering devices at the network border to process the traffic before it reaches internal parts of the network, and absorbing DoS attacks with more network resource than usually required [66]. Second, during the attacks, many techniques can be used to detect the DoS attacks by checking whether the rate of flow of the packets reaches a given threshold or not, finding out anomaly inside the packets by checking them with the normal behavior of the packets and other machine learning-based detection techniques [66], [67]. Third, after the attacks, it is important to develop a technique to ensure that the attacks will not happen again [66]. One solution is to use traceback strategy to identify the source of the attack, and another solution is to incorporate proper response, e.g., compare the behavior of the packet with normal behavior and discard the packets that mismatch with normal behavior.

2) *Malware Injection:* In 5G V2X data networks, improper operations on the cloud computing may introduce vulnerabilities into their applications, which could be exploited by attackers to inject some malware to control the cloud server and even affect V2X application users [38]. In the literature, various techniques can be used to detect the malware in the cloud environment [68]. Chen and Zhao [69] proposed a technique that provides enhanced functionality for the detection of malware and enhanced forensic capability. At the same time, the growing maturity in machine learning algorithms has led to their application in malware detection. Thus, some machine learning-based malware detection schemes were proposed [70], [71]. In addition, other techniques, e.g., online forensics techniques, can also be applied to detect malware [72].

2) Security Strategies in 5G Core Networks: 5G core is affected by some of the vulnerabilities in SDN and NFV since these techniques are two of its building blocks. Hence, some of the works on these problems in SDN and NFV should also be helpful in 5G core networks.

Hong *et al.* [35] classify host location hijacking attacks and link fabrication attacks as topology poisoning attacks, which are based on the vulnerabilities in topology management services of existing OpenFlow controllers. In particular, these two attacks can be effective because of the lack of validation of the packets and APIs used for topology management. Hence, Hong *et al.* [35] proposed a security extension for the OpenFlow controller, called TopoGuard, to mitigate this type of attacks. In TopoGuard, the port manager is employed to maintain properties indicating the state of each switch port and will raise an alert when an illegal action corresponding current state happened. Moreover, TopoGuard uses a host prober and a topology update checker to verify the topology of the network dynamically.

Shin *et al.* [34] propose an extension, called connection migration, to reduce the amount of data-to-control-plane interactions. With the connection migration extension, the data plane will proxy the TCP handshake when a new flow request is received. Only those flow requests that complete the handshake will be reported to the control plane. Through the adoption of stateless TCP handshaking with SYN cookies, connection migration can address saturation attacks since malicious TCP connection attempts will not be handled by the control plane. Moreover, this article introduces triggers to manage flow rules under certain conditions. These two extensions make up AvantGuard, which makes OpenFlow networks more scalable and responsive to network threats.

3) Security Strategies at Network Edge: In V2X communications, a large number of V2X applications are location-based. Then, when an edge server is deployed to provide some location-based services, an attacker may attempt to gain access to a service that is not valid at his/her current location by launching location spoofing attacks, which will subvert the location-based services in V2X communications [7]. In order to prevent the location spoofing attacks, it is critical to deploy a location proof mechanism with which a V2X entity can prove that he/she is actually located in a specific location. Some of the existing works focus on designing the location proof mechanism. Brands and Chaum [73] proposed the first cryptographic distance-bounding scheme that provides the location proof by proving the upper bound of the distances between two objects. Based on Brands *et al.*'s work, several extended cryptographic distance-bounding schemes were proposed to resist attacks, such as distance hijacking [74]. Furthermore, based on these schemes, several works have proposed verifiable multilateration schemes to prove that an object is located in a certain area [75]. Apart from the works on location proof mechanisms, some existing works focus on detecting the location spoofing attacks. For example, Penna *et al.* [76] and Varghese *et al.* [77] addressed the same issue, respectively, by analyzing whether a node is sending forged location.

4) Security Strategies in V2X Communications: As mentioned earlier, V2X connects nodes near the roads to make a vehicle smarter, but it also presents some security challenges because of the heterogeneity of its nodes. In the following, we highlight the security strategies in V2X communications.

1) *Eavesdropping Attacks:* It cannot be easily traced because it is a passive attack, which does not disrupt any network operation. Encryption is a common technique to counter this type of attack. However, even though all messages are encrypted, it is still possible for an attacker to infer the source and the destination of messages [29]. In this case, some anonymous communication techniques can be employed to hide messages' source and destination, e.g., onion routing technique. In an onion network, messages are encapsulated in layers of encryption, and anyone eavesdropping on the network has no idea on the source and destination of the transmitted messages. Besides, friendly jamming also has been recognized as a promising approach to prevent eavesdropping attacks without bringing extra computing tasks [78]. The main idea is to introduce some friendly jammers to the networks, where these friendly jammers can generate a jamming signal to increase the noise level to the eavesdroppers so that they cannot successfully wiretap the legitimate communications. Note that the friendly jamming technique is cost-effective and does not require strong-computing capability [79], which is essential in the V2X scenario.
2) *Message Forgery:* A message forgery attack modifies the V2X messages, which may mislead the V2X entities to take wrong actions and possibly cause accidents. Data integrity verification is a common technique to allow the V2X entities to detect the integrity of the received messages, and it can be effectively achieved by the deployments of the Reed–Solomon code, checksums, trapdoor hash functions, message authentication code, digital signatures, and so on [80]. Since the integrity checking requires some verification techniques, external attackers cannot directly launch the attack because they do not hold any valid credentials [28]. Thus, most of the message forgery attacks are launched by the internal attackers. When a message forgery attack is mounted by an internal attacker, identifying the internal attacker is even more important than identifying the current message forgery attack. The traceability feature is an essential requirement to ensure that internal adversaries can be identified when a forgery attack is mounted [28].
3) *Jamming Attacks:* The jamming attack is considered to be a channel-related threat in contemporary networking deployment, and their impact on the network performance is often catastrophic [81] and may make some V2X applications fail to function in a certain area. In the literature, physical layer frequency hopping and direct sequence spread spectrum techniques can be employed to solve jamming attacks [7]. In addition, prior researches also explored algorithms to solve the jamming attacks in some specific network environments. For example, Toledo and Wang [81] designed a jamming attack detector for CSMA-/CA-based networks by computing how explainable is the occurring of each particular collision.
4) *Impersonation Attacks:* In V2X communications, the impersonation attack is that a V2X entity impersonates another V2X entity (e.g., vehicles) to broadcast the messages in the V2X network, which may have an impact on other entities and the V2X control system [82]. Thus, in order to prevent an impersonation attack, all messages should be authenticated and signed. Apart from data message authentication and signature, multiple solutions can be used to solve the impersonation attack, such as user authentication using a digital signature, employing a TA, and using variable MAC and IP addresses [7].
5) *Replay Attacks:* The replay attack is that a malicious adversary replays the transmission of previously generated frames in new connections [83], which may result in messages overflowing at the receiver side, complete DoS attack, and even session hijacking attack [84]. To address this issue, there are two strategies. The first one is to use a globally synchronized time for all V2X entities. The other one is to use a nonce (timestamp) [83]. Specifically, the authenticated timestamps can be attached to the V2X messages. Thus, the replay attack can be detected once the V2X entities receive the messages with past timestamps.
6) *MITM Attacks:* In the V2X communication scenario, the MITM attack refers to that a malicious V2X entity listens to the communication among V2X entities and injects false information between V2X entities. Based on the traditional Diffie–Hellman (DH) key exchange protocol, which is vulnerable to the MITM attack, several enhanced DH schemes have been proposed to counter MITM attacks [85]. In addition, a multiway challenge–response protocol, such as Needham–Schroeder [86], can also be used. Kerberos [86], which is based on a variant of Needham–Schroeder, is an authentication protocol used in many real systems, including Microsoft Windows [31]. There are also some works (e.g., [87]) adapting the Kerberos protocol to IoT, which could be used to enhance authentication in V2X.
7) *Sybil Attacks:* In a Sybil attack, the attacker generates multiple identities to illude the V2X entities to take the wrong action. In V2X communications, many threat detection protocols for Sybil attacks have been proposed, such as privacy-preserving detection of abuses of pseudonyms, session key certificate, and enhanced attacked packet detection algorithm for detecting the malicious nodes with multiple identities [88]. In addition, the cryptographic

technique can be employed to detect Sybil attacks. For example, Yan *et al.* [89] propose an encryption method to detect Sybil attacks, in which the identity of the vehicles should be provided along with the messages.

C. Privacy Strategies in 5G V2X Services

As discussed in Section III-C, 5G raises serious concerns on privacy leakage when enabling various V2X services and applications. Currently, many privacy-preserving strategies have been leveraged to prevent user privacy breach in each layer of 5G V2X.

1) Privacy Strategies in Data Networks/Internet: In data networks/Internet, a large number of privacy-preserving V2X services have been proposed to enable users to access these services without worrying about their privacy violation. As one of the anonymous authentication techniques, anonymous credential enables users to access V2X services without directly exposing real identities. Specifically, each user is assigned with an anonymous credential by the V2X service provider in data networks/Internet during the registration process, and it proves the ownership of this credential during service access. In this way, the service provider only learns that the user is eligible to access V2X services, without having the real identity of the user. The anonymous credential can be constructed using the blind signatures, the group signatures, or the pseudonyms.

A blind signature [90] is a form of digital signature in which the signer has the capability of generating a signature on a message without having the message. Au *et al.* [91] designed a new payment scheme for electric vehicles to protect the location privacy during electric charging and discharging from the BBS+ blind signature [92]. The supplier is allowed to generate the anonymous credentials, i.e., the BBS+ blind signature, for electric vehicles. In the charging or discharging, electric vehicles present the legality of charging or discharging by proving the validity of blind signatures using the Σ-protocol. The blind signatures are also leveraged to achieve identity or location privacy in other V2X applications, including automated valet parking [93], vehicle-to-grid applications [94], and electronic toll pricing [95]. The blind-signature-based anonymous credential enjoys two desirable features: one is that the credential can be used multiple times for service access, once the user receives the delegation, and the other is the perfect privacy protection. However, once the user's identity is perfectly preserved, the user cannot be traced even some misbehavior is detected. Therefore, Sun *et al.* [96] have combined the blind signature and secret sharing scheme to design a privacy-preserving scheme to protect vehicle's privacy while still offering an effective way to discover traffic law violators.

The group signature [97] allows a member of a group to anonymously generate the signature of a message on behalf of the group. Concretely, an entity generates the signature with its secret key on behalf of the group, and others can verify the signature using the public key of the group. Thereby, the group signature provides privacy, as signers are anonymous within the group. Different from the blind signature, in the group signature, there is a group manager who manages the member joining and revocation of the group, and is capable of revealing the original signer in case of disputes. Currently, many state-of-the-art short group signatures [98], [99] have been used to design privacy-preserving V2X services, including secure transportation system [100], cooperative driving [101], and smart parking navigation [102].

To preserve privacy in V2X services, both IEEE 1609.2-2013 and 3GPP TS 33.501 suggest to utilize pseudonyms, i.e., a vehicle has a base identity for service access, which can be chosen by the vehicle itself, the V2X service provider, or TA. In general, the pseudonyms are validated by the certificate authority that generates signatures using its secret key on the pseudonyms, and only the vehicles with valid signatures are deemed to be trusted. Park *et al.* [103] proposed an anonymous identity management system for access control of cloud service based on the pseudonyms. The transportation manager and the service manager collaboratively issue the RSU-binding pseudonymous tokens to vehicles based on identity-based cryptography and the pseudonyms chosen by the vehicles. Chim *et al.* [104] designed a secure and privacy-preserving navigation scheme from the real-time road information, in which the pseudonym issued by TA is used to generate the anonymous credential for the vehicle. To ensure the revocation of the misbehaving vehicles, TA is required to maintain a list containing the certificates of the revoked vehicles.

In addition to the anonymous credentials, other sophisticated techniques, such as cryptographic accumulators [105], spatial and temporal cloaking [106], and mixed network [107], can also be leveraged to build privacy-preserving V2X services.

2) Privacy Strategies in 5G Core Networks: To prevent subscriber privacy, which is considered at the top of security demand in mobile networks, pseudonyms have been defined in the 3GPP standard. Angermeier *et al.* [108] proposed a privacy-preserving LTE communication scheme in vehicular networks. Pseudonyms are assigned by network operators to the vehicles as permanent identifiers through vehicle manufacturers in a hidden way and used to negotiate the temporary identifiers for network access. Ahmed and Lee [109] designed a privacy-preserving LTE-based V2X service. To realize identifier privacy, the network operator distributes the pseudonyms to the vehicles on behalf of the long-term keys, and the vehicles generate the short-term keys (pseudonyms) for the secure exchange of V2X messages during V2X service registration. In both schemes, the pseudonyms are generated by the network operator who has the capability to support traceability, nonrepudiation, and nonframe-ability of the misbehaving vehicles.

Due to the entire network visibility of SDN and NFV, several cyberattacks have been introduced in poisoning network visibility, such as MITM attacks, distributed DOS attacks, and sniffer attacks, which results in severe damage on privacy [110]. In OpenFlow specification, the TLS protocol is not enforced to secure the communications in SDN, such that it is possible to learn the plaintext traffic for the SDN controller and the OpenFlow switches. Even worse, if the traffic is encrypted, an MITM attack is still feasible. Wang *et al.* [111] investigated the MITM attack on the SDN security protocols, which results in the privacy leakage for users and the interception of traffic. Anonymization is widely used in SDN networks to prevent privacy leakage. Mendonca *et al.* [112] proposed AnonyFlow, an efficient SDN-based anonymization service, where the Internet users offload trust to the primary service providers that assign temporary IP addresses and disposable flow-based identifiers to users. This anonymization feature is an additional service for a service provider. The SDN controller can coordinate the service implementation of customizing routing policies across switches based on the users' demands. Another approach to preventing privacy leakage in SDN networks is presented by Jafarian *et al.* [113], in which the network hosts are protected against online attackers. The attackers are able to remotely and randomly probe IP addresses in networks to identify victims and further detect vulnerabilities if the host responds. To protect the network hosts, in [113], the controller assigns each host a random, temporary virtual IP address related to the host's real IP address. The users are only able to access the hosts based on the virtual IP address. The translation between real IP address and virtual IP address is performed by the OpenFlow switches that are also responsible for choosing the virtual IP addresses from the unused addresses in the network for network hosts.

3) Privacy Strategies at Network Edge: Due to the physical proximity, it is possible for adversaries to eavesdrop the messages about victims in the edge layer. To prevent privacy leakage, both cryptography-based schemes [114], [115] and pseudonym-based schemes [116], [117] have been utilized in mobile fog/edge computing. To prevent the leakage of users' interested service types to curious edge servers in network slices selection, Ni *et al.* [118] proposed an efficient and secure service-oriented authentication framework for 5G IoT services. The users' identities are protected based on anonymous credentials, and a secure profile matching mechanism is presented to preserve both configured slice types and accessing service types of users. However, the cryptographic operations for content privacy preservation in [118] are complex, and the lightweight method is based on pseudonyms. Kang *et al.* [116] proposed a privacy-preserving pseudonym scheme for effective pseudonym management in the fog-supported Internet of Vehicles. The pseudonyms are managed and updated by the specialized fogs at the network edge, e.g., roadside infrastructure.

Differential privacy is an effective way to achieve location privacy in location-based services. In differential privacy, mathematical noise is generated and added into a small sample of the individual's records to limit the privacy impact on individuals in data publication. This technique has been deployed by Apple and Google to discover the usage patterns of a large number of users without compromising individual privacy. The main issue of different privacy is that the statistical location information becomes inaccurate after entailing large noise in the individuals' locations. Thus, the Laplace perturbation and exponential perturbation are the most popular approaches to generate the added noise and to ensure that the gap between the statistical results and the real results is negligible. Zhou *et al.* [119] proposed a privacy-preserving location-based service framework based on differential privacy. The location of users is preserved against the local edge server, but the latter still can provide local service to users based on the perturbed locations with high accuracy. In addition, the differential privacy has also been utilized to protect users' location in location-based services [120] and mobile crowdsensing [121] in which 5G network plays an important role in data exchange. For more details in the field of differential location privacy, we refer to the recent survey [122].

4) Privacy Strategies in V2X Communications: In the last decade, privacy-preserving V2X communications have been widely studied to guarantee the privacy of vehicles. Typical approaches include mix-zone approaches, group-oriented techniques, and pseudonym-based approach. Here, we discuss several representative works in each category.

Mix-Zone Approaches: Mix networks refer to those that utilize a chain of proxy servers as mixes to shuffle the messages from multisenders and return back in random to prevent adversarial tracing. Freudiger *et al.* [123] created mix zones at appropriate places and combined the designed mix zones into mix network to prevent the tracking of vehicles. Liu *et al.* [124] studied a new privacy attack on the mix-zone approaches in which the adversary can reveal a vehicle's identity and the moving trajectory using some side information and built multiple mix zones to prevent this attack. The strength of privacy preservation depends on the number of vehicles meeting at the same location. If the meeting opportunities are sparse, the strength becomes weak. Thereby, Yu *et al.* [107] proposed MixGroup to efficiently exploit the sparse meeting opportunities for pseudonym changing. MixGroup allows the vehicles to exchange their pseudonyms at the extended pseudonym-changing areas, such that the uncertainty of the pseudonym mixture is accumulatively enlarged. Subsequently, Zhang [125] designed a new cryptographic mix zone based on a one-time identity-based authentication and group key agreement scheme, which does not need fully trusted mixers and enables efficient key update for the first time.

Group-Oriented Techniques: As a typical approach of privacy preservation, group-oriented techniques have been widely studied and deployed in V2X communications to hide a specific user in a large group. Lin *et al.* [45] proposed a privacy-preserving authentication schemes for V2V communications based on group signature and identity-based signature. Conditional privacy preservation is realized, which means that the vehicle's privacy is preserved under the condition that no misbehavior is detected for that vehicle; if any dispute event happens, the real identity of the misbehaving vehicle is revealed with the aid of the authority. Although conditional privacy preservation is a promising property, it suffers from the problem of identity revocation management, which causes heavy overhead for the group manager, especially for the distributed environment. Therefore, several research works have been conducted to deal with the growing revocation list, and we refer the survey [11] for a comprehensive discussion on this issue. A ring signature is also one of the anonymous identity authentication techniques. A vehicle can create a ring signature using its secret key and other vehicles' public keys to make itself indistinguishable with these possible vehicles. Chaurasia and Verma [126] utilized the ring signature to design an anonymous message authentication scheme, in which the vehicles that sent the message are hidden in a crowd of the neighboring vehicles. Xiong *et al.* [127] and Jiang *et al.* [128] designed the privacy-preserving authentication schemes from ring signatures with the properties of revocable vehicle identity and simplified key management, respectively. How to utilize these variants to preserve identity privacy for vehicles, while supporting other desirable properties in V2X communications, is deserved to be investigated.

Pseudonym-Based Approaches: Pseudonymous communications can be achieved based on the public key cryptography by randomizing the public-key certificates to generate key pairs or symmetric cryptography by randomly choosing pseudoidentities for efficient authentication. One of the most prominent pseudonym-based security strategies is the security credential management system (SCMS), which is considered to be the leading candidate for secure vehicular communications in the United States. In SCMS, once the registration authority (RA) receives a request from a vehicle, it creates a batch of public keys and shuffles them before sending them to the pseudonym certificate authority (PCA). PCA creates valid certificates for all these keys and delivers the encrypted certificates to the vehicle. By doing so, neither RA nor PCA can link a pseudonym certificate to a specific vehicle, unless they collude. A similar idea has been also realized based on identity-based cryptography [96], [129], in which the pseudonyms are generated and issued by TA or key generation center (KGC) for anonymous authentication. To remove the strong dependence on TA, roadside infrastructures are allowed to issue the pseudonyms to improve the flexibility of pseudonym issuance [130], or the threshold-based secret sharing scheme is used to enable n authorities to collaboratively generate the secret key of the vehicle from the pseudonym and reveal the vehicle's identity at the presence of k out of n authorities [96].

V. OPEN PROBLEMS AND FUTURE DIRECTIONS

In this section, we present open problems and future research directions.

A. Secure Network Caching at Network Edge

Caching the frequently requested data at the storage spaces on edge devices is an effective and efficient way to reduce the latency of V2X services. However, it is hard to ensure the confidentiality of the cached data, from which the adversaries can infer the interested services of a target vehicle. To secure network caching, the following key issues should be addressed: 1) where and when to cache the requested data for vehicles; 2) how to choose the trustful edge devices for data caching; and 3) how to guarantee the cached data confidentiality when the edge nodes are compromised. To address these issues, cache placement strategies, data replacement approaches, and secure data retrieval schemes should be carefully investigated.

B. Security-Enhanced Network Slicing

The security and privacy of network slicing have not received much attention as yet. The key security issue is how to perform access authentication and authorization for a specific network slice. Access control to network slices requires additional authentication and authorization to prevent unauthorized vehicles from accessing the slices, as these unauthorized vehicles may consume resources that are assigned to eligible vehicles. To support additional authentication and authorization, the following issues should be solved: 1) how to generate the authentication identifiers and keys with backward and forward security from 3GPP SUPI; 2) how to manage the identifiers and keys for different network slices corresponding to the V2X services; and 3) how to achieve efficient authentication and authorization to guarantee low-latency V2X service access. In addition, the NSSAI may be linked to a particular service exclusively for drivers with special occupations, e.g., polices and doctors. If the NSSAI is transmitted in an unprotected way, the privacy of drivers who access this service will be leaked.

C. Privacy-Preserving Network Data Analytics

The NWDAF provides network data analytics services to 5G providers or V2X service providers, in which the statistical information or the predictive data are obtained from the historical data in one network slice [12].

To enable the specification of the types of analytics, each NWDAF provides the list of service IDs and collects the data from multiple sources related to the analyzed services, including the behavior data about individual vehicles or a group of vehicles, the number of vehicles present in a geographical area, and per spatial and temporal dimensions. However, the location or behavior data are quite sensitive from the perspective of drivers, from which the adversary can learn the mobility patterns of drivers. Thus, exploring efficient and privacy-preserving mechanisms for network data analytics is an essential task to secure 5G V2X communications.

D. Secure Driving for Automated Vehicles

To guarantee safe automated driving, every key procedure should be protected against hackers, including data collection, data exchange, data analytics, decision-making, and command control of automated vehicles. Secure 5G V2X communications only provide the reliability of data collection and data exchange, but it cannot ensure decision correctness and control security. It is of utmost importance to keep the resilience of safety features of the autonomy functions. However, due to the complexity of automated vehicles, it is difficult to ensure that each part on a vehicle works effectively at the presence of adversaries. The modern smart vehicles lack sufficient security protection. To ensure the resilience of autonomy functions, two research directions can be pursued: 1) how to achieve verifiable data analytics to identify the tiny miscalculations in machine learning; and 2) how to build security protection mechanisms on the vehicles, such as firewalls and intrusion detection systems.

VI. CONCLUSION

The 5G V2X services have been exponentially increasing and greatly benefited our daily lives. However, while offering diverse benefits to both drivers and passengers on roads, the connectivity of 5G V2X has also created a variety of concerns on trust, security, and privacy. In this article, we have presented a brief overview of key challenges in securing 5G V2X by identifying its concerns on trust, security, and privacy. In addition, we have also discussed the key strategies for secure 5G V2X services. Finally, we have also provided some open problems and future research directions in secure 5G V2X services. We expect that this article could shed light on secure 5G V2X research and implementation for both industry and academia in the near future. ■

REFERENCES

[1] P. Rost *et al.*, “Mobile network architecture evolution toward 5G,” *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 84–91, May 2016.

[2] M. Boban, A. Kousaridas, K. Manolakis, J. Eichinger, and W. Xu, “Use cases, requirements, and design considerations for 5G V2X,” 2017, *arXiv:1712.01754*. [Online]. Available: https://arxiv.org/abs/1712.01754

[3] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, “Security for 5G and beyond,” *IEEE Commun. Surveys Tuts.*, to be published.

[4] G. Naik, B. Choudhury, and J.-M. Park, “IEEE 802.11 bd & 5G NR V2X: Evolution of radio access technologies for v2x communications,” *IEEE Access*, vol. 7, pp. 70169–70184, 2019.

[5] F. Lyu *et al.*, “Characterizing urban vehicle-to-vehicle communications for reliable safety applications,” *IEEE Trans. Intell. Transp. Syst.*, to be published.

[6] A. Greenberg, “Hackers remotely kill a jeep on the highway with me in it,” *Wired*, vol. 7, p. 21, Oct. 2015.

[7] M. Muhammad and G. A. Safdar, “Survey on existing authentication issues for cellular-assisted v2x communication,” *Veh. Commun.*, vol. 12, pp. 50–65, Apr. 2018.

[8] G. Karagiannis *et al.*, “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, Nov. 2011.

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

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

[11] 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, Mar. 2015.

[12] *System Architecture for the 5G System*, document TS 33.501, version 15.2.0, 3rd Generation Partnership Project, 2018.

[13] *Study on Enhancement of 3GPP Support for 5G V2X Services*, document TR 22.886, version 15.2.0, 3rd Generation Partnership Project, 2018.

[14] *Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services*, document TS 23.287, version 16.2.0, 3rd Generation Partnership Project, 2019.

[15] *Security Architecture and Procedures for 5G System*, document TS 33.501, version 15.4.0, 3rd Generation Partnership Project, 2019.

[16] A. Festag, “Cooperative intelligent transport systems standards in Europe,” *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 166–172, Dec. 2014.

[17] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovács, “Enhancements of V2X communication in support of cooperative autonomous driving,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 64–70, Dec. 2015.

[18] A. Jahn, K. David, and S. Engel, “5G/LTE based protection of vulnerable road users: Detection of crossing a curb,” in *Proc. IEEE VTC-Fall*, Sep. 2015, pp. 1–5.

[19] L. Zhang, L. Yan, Y. Fang, X. Fang, and X. Huang, “A machine learning based defensive alerting system against reckless driving in vehicular networks,” *IEEE Trans. Veh. Technol.*, to be published.

[20] S. Meredith. (Apr. 2018). *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*. [Online]. Available: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

[21] K. Wahl-Jorgensen, L. Bennett, A. Hintz, and L. Dencik, “Introduction,” *Journalism, Citizenship Surveill.*, vol. 5, no. 3, pp. 256–261, 2017.

[22] A. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, 2007.

[23] Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, “A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks,” in *Proc. IEEE INFOCOM*, Apr. 2006, pp. 1–13.

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

[25] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, “Trust issues for vehicular ad hoc networks,” in *Proc. VTC-Spring*, 2008, pp. 2800–2804.

[26] D. Huang, X. Hong, and M. Gerla, “Situation-aware trust architecture for vehicular networks,” *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 128–135, Nov. 2010.

[27] J.-H. Cho, A. Swami, and I.-R. Chen, “A survey on trust management for mobile ad hoc networks,” *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[28] 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.

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

[30] D. Kang, J. Jung, D. Lee, H. Kim, and D. Won, “Security analysis and enhanced user authentication in proxy mobile IPv6 networks,” *PLoS ONE*, vol. 12, no. 7, p. e0181031, 2017.

[31] B. Wu, J. Chen, J. Wu, and M. Cardei, “A survey of attacks and countermeasures in mobile ad hoc networks,” in *Wireless Network Security*. Springer, 2007, pp. 103–135.

[32] K.-W. Huang and H.-M. Wang, “Identifying the fake base station: A location based approach,” *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1604–1607, Aug. 2018.

[33] R. Nagarathna and S. M. Shalinie, "SLAMHHA: A supervised learning approach to mitigate host location hijacking attack on sdn controllers," in *Proc. ICSCN*, Mar. 2017, pp. 1–7.

[34] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-guard: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM CCS*, 2013, pp. 413–424.

[35] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures," in *Proc. NDSS*, vol. 15, 2015, pp. 8–11.

[36] *Study on Security Aspects of Network Slicing Enhancement*, document TR 33.813, version 0.3.0, 3rd Generation Partnership Project, 2019.

[37] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[38] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Proc. CLOUD*, 2009, pp. 109–116.

[39] K. Norrman, M. Näslund, and E. Dubrova, "Protecting imsi and user privacy in 5G networks," in *Proc. EAI MOBIMEDIA*, 2016, pp. 159–166.

[40] A. Chaabane, E. De Cristofaro, M. A. Kaafar, and E. Uzun, "Privacy in content-oriented networking: Threats and countermeasures," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 3, pp. 25–33, 2013.

[41] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for eHealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[42] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proc. NDSS*, vol. 11, 2011.

[43] L. Rongxing, L. Xiaodong, and S. Xuemin, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[44] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 3, p. 6138251, 2016.

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

[46] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[47] A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5214–5224, Nov. 2009.

[48] J. Krumm, "Inference attacks on location tracks," in *Proc. PerCom*, 2007, pp. 127–143.

[49] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," 2009, *arXiv:0903.3276*. [Online]. Available: https://arxiv.org/abs/0903.3276

[50] X. Lin, R. Lu, C. Zhang, and, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[51] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1238–1246.

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

[53] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[54] S. Buchegger and J.-Y. L. Boude, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop Econ. Peer-to-Peer Syst.*, 2004, pp. 1–6.

[55] S. Chen *et al.*, "Vehicle-to-everything (v2x) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, Jun. 2017.

[56] *5G Security-Enabling a Trustworthy 5G System*, Ericsson, Stockholm, Sweden, White Paper, Mar. 2018.

[57] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[58] P. G. Lopez *et al.*, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, 2015.

[59] R. Roman *et al.*, "Mobile edge computing, fog: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[60] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges," 2016, *arXiv:1612.03184*. [Online]. Available: https://arxiv.org/pdf/1612.03184.pdf

[61] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[62] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11008–11021, Jun. 2018.

[63] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 22–31, May 2018.

[64] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.

[65] M. Kinateder, E. Baschny, and K. Rothermel, "Towards a generic trust model—Comparison of various trust update algorithms," in *Proc. IFIP TM*, 2005, pp. 177–192.

[66] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3655–3682, Dec. 2017.

[67] M. Sung and J. Xu, "IP traceback-based intelligent packet filtering: A novel technique for defending against Internet DDoS attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 14, no. 9, pp. 861–872, Sep. 2003.

[68] A. Bedi, N. Pandey, and S. K. Khatri, "Analysis of detection and prevention of malware in cloud computing environment," in *Proc. AICAI*, 2019, pp. 918–921.

[69] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Proc. ICCSEE*, vol. 1, Mar. 2012, pp. 647–651.

[70] S. Şahin, "On current trends in security and privacy of cloud computing," in *Proc. AICT*, 2013, pp. 1–5.

[71] W. Hardy, L. Chen, S. Hou, Y. Ye, and X. Li, "DL4MD: A deep learning framework for intelligent malware detection," in *Proc. DMIN*, 2016, pp. 61–67.

[72] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.

[73] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proc. EUROCRYPT*, 1993, pp. 344–359.

[74] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *Proc. IEEE Secur. Privacy*, May 2012, pp. 113–127.

[75] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 5, pp. 938–950, May 2013.

[76] K. Penna, V. Yalavarthi, H. Fu, and Y. Zhu, "Evaluation of active position detection in vehicular ad hoc networks," in *Proc. IEEE INCNN*, Jul. 2014, pp. 2234–2239.

[77] R. Varghese, T. Chithralekha, and C. Kharkongor, "Self-organized cluster based energy efficient meta trust model for Internet of Things," in *Proc. ICETECH*, 2016, pp. 382–389.

[78] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.

[79] X. Li, Q. Wang, H. Dai, and H. Wang, "A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack," *Sensors*, vol. 18, no. 6, p. 1938, 2018.

[80] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: A big picture," *Future Gener. Comput. Syst.*, vol. 49, pp. 58–67, Aug. 2015.

[81] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 347–358, Sep. 2008.

[82] M. S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. ICSPCS*, Dec. 2012, pp. 1–9.

[83] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security attacks and its possible solutions," *J. Inf. Oper. Manage.*, vol. 3, no. 1, p. 301, 2012.

[84] I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, "One-time cookies: Preventing session hijacking attacks with stateless authentication tokens," *ACM Trans. Internet Technol.*, vol. 12, no. 1, pp. 1:1–1:24, 2012.

[85] A. S. Khader and D. Lai, "Preventing man-in-the-middle attack in Diffie–Hellman key exchange protocol," in *Proc. ICT*, 2015, pp. 204–208.

[86] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[87] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "3-level secure Kerberos authentication for smart home systems using iot," in *Proc. NGCT*, 2015, pp. 262–268.

[88] C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. H. Anajemba, and A. K. Bashir, "On detection of sybil attack in large-scale VANETs using spider-monkey technique," *IEEE Access*, vol. 6, pp. 47258–47267, 2018.

[89] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Comput. Commun.*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008.

[90] D. Chaum, "Blind signatures for untraceable payments," in *Proc. EUROCRYPT*, 1983, pp. 199–203.

[91] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 3–18, Jan. 2014.

[92] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in *Proc. SCN*, 2006, pp. 111–125.

[93] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 2893–2905, Mar. 2019.

[94] H. Wang, B. Qin, Q. Wu, L. Xu, and

J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2340–2351, Nov. 2015.

[95] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "PrETP: Privacy-preserving electronic toll pricing," in *Proc. USENIX Secur. Symp.*, vol. 10, 2010, pp. 63–78.

[96] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[97] D. Chaum and E. Van Heyst, "Group signatures," in *Proc. ASIACRYPT*, 1991, pp. 257–265.

[98] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Crypto*, 2004, pp. 41–55.

[99] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. CT-RSA*, 2016, pp. 111–126.

[100] N. Ekedebe, W. Yu, C. Lu, H. Song, and Y. Wan, "Securing transportation cyber-physical systems," in *Securing Cyber-Physical Systems*. Boca Raton, FL, USA: CRC Press, 2015, pp. 163–196.

[101] G. Neven, G. Baldini, J. Camenisch, and R. Neisse, "Privacy-preserving attribute-based credentials in cooperative intelligent transport systems," in *Proc. VNC*, Nov. 2017, pp. 131–138.

[102] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6504–6517, Jul. 2018.

[103] Y. Park, C. Sur, and K.-H. Rhee, "Pseudonymous authentication for secure V2I services in cloud-based vehicular networks," *J. Ambient Intell. Humanized Comput.*, vol. 7, no. 5, pp. 661–671, 2016.

[104] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.

[105] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: A case study of anonymous authentication," *Pervasive Mobile Comput.*, vol. 41, pp. 259–269, Oct. 2017.

[106] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. MobiSys*, 2003, pp. 31–42.

[107] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016.

[108] D. Angermeier, A. Kiening, and F. Stumpf, "PAL—Privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication," in *Proc. ACM VANET*, 2013, pp. 1–10.

[109] K. J. Ahmed and M. J. Lee. "Secure LTE-based V2X service," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3724–3732, Oct. 2017.

[110] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.

[111] X. Wang, N. Gao, L. Zhang, Z. Liu, and L. Wang, "Novel MITM attacks on security protocols in SDN: A feasibility study," in *Proc. ICICS*, 2016, pp. 455–465.

[112] M. Mendonca, S. Seetharaman, and K. Obraczka, "A flexible in-network IP anonymization service," in *Proc. ICC*, 2012, pp. 6651–6656.

[113] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "OpenFlow random host mutation: Transparent moving target defense using software defined networking," in *Proc. HotSDN*, 2012, pp. 127–132.

[114] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[115] S. Jiang, J. Liu, M. Duan, L. Wang, and Y. Fang, "Secure and privacy-preserving report de-duplication in the fog-based vehicular crowdsensing system," in *Proc. GLOBECOM*, 2018, pp. 1–6.

[116] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.

[117] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 712–719, Jan. 2018.

[118] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.

[119] L. Zhou, L. Yu, S. Du, H. Zhu, and C. Chen, "Achieving differentially private location privacy in edge-assistant connected vehicles," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4472–4481, Jun. 2019.

[120] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," *Trans. Data Privacy*, vol. 9, no. 1, pp. 15–48, 2016.

[121] L. Wang, D. Zhang, D. Yang, B. Y. Lim, and X. Ma, "Differential location privacy for sparse mobile crowdsensing," in *Proc. ICDM*, 2016, pp. 1257–1262.

[122] P. Vincent, B. Antoine, B. M. Sonia, and B. Lionel, "The long road to computational location privacy: A survey," 2018, *arXiv:1810.03568*. [Online]. Available: https://arxiv.org/abs/1810.03568

[123] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. WiN-ITS*, 2007.

[124] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 972–980.

[125] L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2998–3010, Dec. 2017.

[126] B. K. Chaurasia and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," in *Transactions on Computational Science XIII*. Springer, 2011, pp. 147–156.

[127] H. Xiong, Z. Guan, J. Hu, and Z. Chen, "Anonymous authentication protocols for vehicular ad hoc networks: An overview," in *Proc. ACNS*, 2016, pp. 53–72.

[128] Y. Jiang, Y. Ji, and T. Liu, "An anonymous communication scheme based on ring signature in VANETs," 2014, *arXiv:1410.1639*. [Online]. Available: https://arxiv.org/abs/1410.1639

[129] 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.

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

ABOUT THE AUTHORS

Rongxing Lu (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012.

He is currently an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada. His current research interests include applied cryptography, privacy-enhancing technologies, and the Internet of Things–big data security and privacy.

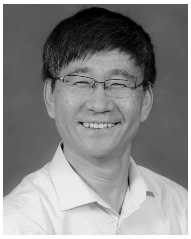
Dr. Lu was awarded the most prestigious Governor General's Gold Medal. He received the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award in 2013.

Lan Zhang (Student Member, IEEE) received the B.S. and M.S. degrees from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2013 and 2016, respectively. She is currently working toward the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA.

Her current research interests include wireless networking and network security for various cyber–physical systems.

Jianbing Ni (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2018.

He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Queen’s University, Kingston, ON, Canada. His current research interests include applied cryptography and network security, with a focus on cloud computing, smart grid, mobile crowdsensing, and the Internet of Things.



Yuguang (Michael) Fang (Fellow, IEEE) received the M.S. degree from Qufu Normal University, Shandong, China, in 1987, the Ph.D. degree from Case Western Reserve University, Cleveland, OH, USA, in 1994, and the Ph.D. degree from Boston University, Boston, MA, USA, in 1997.

He joined the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA, in 2000, where he has been a Distinguished Professor since 2019. He held a University of Florida Research Foundation (UFRF) Professorship from 2006 to 2009 and for the term 2017–2020.

Dr. Fang is also a Fellow of the AAAS. He received the U.S. National Science Foundation Career Award in 2001, the Office of Naval Research Young Investigator Award in 2002, the Best Paper Award from IEEE ICNP in 2006, the 2010–2011 UF Doctoral Dissertation Advisor/Mentoring Award, the 2014 IEEE Communications Society WTC Recognition Award, the 2015 IEEE Communications Society CISTC Technical Recognition Award, and the IEEE Vehicular Technology Outstanding Service Award in 2018. He has been serving on several editorial boards of technical journals. He was the Editor-in-Chief of the IEEE WIRELESS COMMUNICATIONS from 2009 to 2012 and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2013 to 2017.