A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy

Zhaojun Lu, Gang Qu, *Senior Member, IEEE*, and Zhenglin Liu

***Abstract*— Vehicular ad hoc networks (VANETs) are becoming the most promising research topic in intelligent transportation systems, because they provide information to deliver comfort and safety to both drivers and passengers. However, unique characteristics of VANETs make security, privacy, and trust management challenging issues in VANETs' design. This survey article starts with the necessary background of VANETs, followed by a brief treatment of main security services, which have been well studied in other fields. We then focus on an in-depth review of anonymous authentication schemes implemented by five pseudonymity mechanisms. Because of the predictable dynamics of vehicles, anonymity is necessary but not sufficient to thwart tracking an attack that aims at the drivers' location profiles. Thus, several location privacy protection mechanisms based on pseudonymity are elaborated to further protect the vehicles' privacy and guarantee the quality of location-based services simultaneously. We also give a comprehensive analysis on various trust management models in VANETs. Finally, considering that current and near-future applications in VANETs are evaluated by simulation, we give a much-needed update on the latest mobility and network simulators as well as the integrated simulation platforms. In sum, this paper is carefully positioned to avoid overlap with existing surveys by filling the gaps and reporting the latest advances in VANETs while keeping it self-explained.**

***Index Terms*— VANETs, security, privacy, trust management, simulation tools.**

I. Introduction

In recent years, intelligent transportation systems (ITSs) [1] have gained a lot of popularity in both industry and academia. In addition to providing entertainment services on vehicles, the main motivation of ITSs is to improve road safety and driving conditions [2]. In order to share the critical driving information, vehicular ad hoc networks (VANETs) are established with two types of communication, namely vehicle-to-vehicle (V2V) and vehicles-to-infrastructure (V2I) communication [3]. As shown in Fig. 1, in V2V communication, vehicles communicate with nearby vehicles to exchange information; and in V2I communication, vehicles communicate directly with roadside units (RSUs) [4]. Dedicated short range communication (DSRC) radio [5] and a couple of IEEE standards can be used for V2V and V2I communications in VANETs.

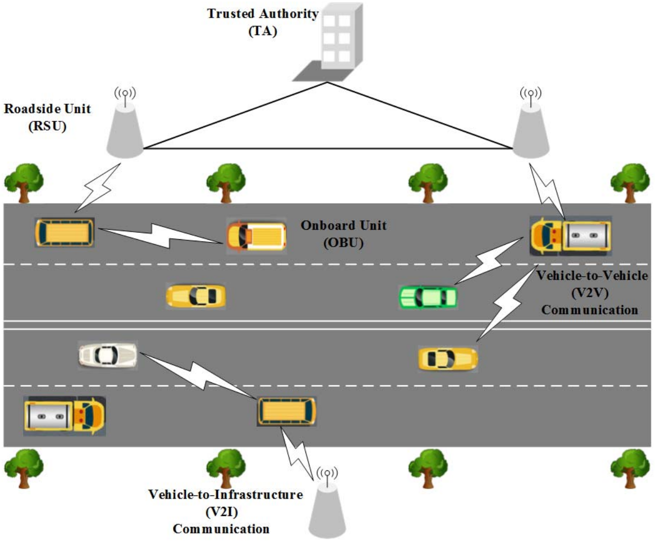


Fig. 1. System model of vehicular ad hoc networks (VANETs).

Unique characteristics such as high mobility and volatility of VANETs have made it vulnerable to various kinds of external and internal attacks [6]. These attacks have caused three main concerns in the design of secure VANETs: security, privacy and trust. Many researchers have proposed various methods to ensure security, preserve privacy and establish trust management for VANETs.

Several excellent surveys have been published in recent years, which all cover the background of VANETs such as the requirements, challenges, different types of threats and corresponding solutions. However, each survey has its own emphasis and shortcomings. The 2014 survey by Engoulou *et al.* [6] summarizes characteristics and challenges of VANETs and proposes solutions to various security issues but with little coverage on privacy-preserving methods. Another 2014 survey by Al-Sultan *et al.* [7] gives a comprehensive treatment on VANETs that starts from the architecture and concludes with simulation tools, simulate protocols and applications. Many new simulation tools have been developed since then and Section VII in this article can be considered an update. The 2015 review by Qu *et al.* [8] and the 2016 survey by Azees *et al.* [4] focus on the authentication methods with conditional privacy preservation in addition to common security concerns.

Manuscript received August 15, 2017; revised January 30, 2018; accepted March 21, 2018. Date of publication April 23, 2018; date of current version January 31, 2019. This work was supported by the National Science Foundation of China under Grant 61376026 and Grant 61176026. The Associate Editor for this paper was S. C. Wong. *(Corresponding author: Zhenglin Liu.)*

Z. Lu and Z. Liu are with the School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: liuzhenglin@hust.edu.cn).

G. Qu is with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20742 USA.

Digital Object Identifier 10.1109/TITS.2018.2818888

This survey is complementary to the above work in that we focus on topics that they did not cover and new results reported in the past several years. Meanwhile, for the convenience of readers of different background, we try to make this survey self-contained by covering the fundamentals of VANETs and all three security related topics. With this goal in mind, after a short review of the system model, communication patterns, and other characteristics of VANETs in Section II, we cover VANETs security, trust, and privacy as follows: well-studied security topics are covered without detailed elaboration; discussion on privacy features the less-covered anonymous authentication schemes and location privacy protection mechanisms; a systematic and in-depth survey on VANETs trust management; the latest VANETs simulation tools and platforms are reported.

A. Security

The core security problem is how to make the V2V and V2I communication channels secure. A good approach for security should provide high quality services in terms of availability, confidentiality, authentication, integrity and non-repudiation [4]. Since the solutions to deal with these threats and attacks are similar to those in other well-studied fields such as mobile ad hoc networks (MANETs) and the Internet, this will not be the focus of this survey. We will only list in Section III some representative works in VANETs along with each of the above security metrics.

B. Privacy

Privacy means only dedicated individuals in VANETs should have the right to access and control of vehicle information, including vehicle's real identity and the location profile. Anonymity authentication [9] is commonly used to preserve privacy. Section IV elaborates five categories of anonymous authentication schemes based on their different underlying employed cryptographic mechanisms: symmetric cryptograph, public-key infrastructure, identity-based signature, certificateless signature, and group signature. However, merely anonymity is not enough to prevent the tracking attacker from reconstructing the trajectory of the target vehicle even if the broadcasted messages keep complete anonymous [10]. In Section V, we explain how tracking attack works and present several location privacy protection mechanisms as supplementary of anonymous authentication.

C. Trust

In VANETs, trust management deals with how a vehicle can trust other vehicles and the received messages [11]. Three popular trust management models are discussed in Section VI: entity-centric trust models, data-centric trust models and combined trust models. We also analyze the efficiency of these models according to the properties of desirable trust management in VANETs.

Finally, we survey the simulation tools used in various VANETs studies. Such tools are critical in delivering results close to real-life scenarios. A short description and comparison of the state-of-the-arts mobility simulators, network simulators, and integrated simulation platforms can be found in Section VII.

II. Overview of VANETs

In this section, we first introduce the system model of VANETs including the onboard unit (OBU), roadside unit (RSU), and trusted authority (TA). Then we list the communication patterns in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication and the underlying standards implemented in VANETs. Finally, we explain the unique characteristics of VANETs in comparison with MANETs, which make the security, privacy preservation, and trust management difficult issues.

A. System Model

As shown in Fig. 1, VANETs consist of three major components: OBU, RSU, and TA. OBU of each vehicle is connected with a sensor network to exchange velocity, steering information, etc. and can communicate with other vehicles' OBUs and nearby RSUs [4]. All RSUs along the road are interconnected with each other. TA is responsible for the management of all the RSUs through a wired connection.

- OBU: Onboard Unit

An OBU is equipped in every vehicle as a transceiver to communicate with other vehicles' OBUs and RSUs. An OBU consists of a resource command processor (RCP), storage, network device, and sensors. Sensors such as global positioning system (GPS) collect information to send to the OBU. Then the OBU monitors and gathers the information to form messages, which are sent to neighboring vehicles and RSUs through wireless medium [4].

- RSU: Roadside Unit

The RSUs are generally stationary devices deployed along the road or at dedicated locations such as at intersections or parking lots [7]. The RSUs have network devices for dedicated short range communication (DSRC) as well as communication with the infrastructural network. The main functions of RSUs include: (i) Extending the communication range of VANETs by relaying the messages to other OBUs and RSUs. (ii) Running safety applications such as traffic condition reporting or accident warning. (iii) Providing Internet connectivity to OBUs.

- TA: Trusted Authority

TA is responsible for the trust and security management of the entire VANETs including verifying the authenticity of vehicles and revoking nodes in the case of vehicles broadcasting fake messages or performing malicious behavior [4]. Thus, the TA needs to have high computational power and sufficient storage capacity.

B. Communication Patterns

V2V communication is among vehicles in ad hoc mode [12]. In V2V, vehicles can transmit or exchange valuable information such as traffic conditions and accidents with each other [2]. V2I communication is used to broadcast information

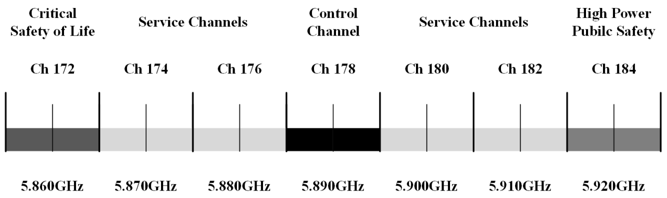


Fig. 2. Seven channels of dedicated short range communication (DSRC).

between the network infrastructure and vehicles [12]. In V2I, a vehicle can establish a connection with RSUs to connect and communicate with the Internet [2]. The communication patterns in VANETs can be divided into four categories as described by Fuentes *et al.* [13]:

- Warning Message Propagation among Vehicles

In case of emergency situations, it is crucial to send warning messages to a particular vehicle or to a group of vehicles. Because of the strict time constraint, an efficient routing protocol is required to transmit the warning messages in a security manner.

- Group Communication among Vehicles

In order to facilitate group communication among a set of vehicles, this communication pattern should consider the issue of high dynamic and scalability of the group.

- Beaconing among Vehicles

Beacon messages are periodically sent to all nearby vehicles and RSUs, which contain the property values such as velocity, acceleration, location etc. [14]

- Warnings between Infrastructure and Vehicles

In order to ensure road safety, warning messages are broadcasted by RSUs to all the vehicles in its range when potential dangers are detected or expected, especially in intersections with complex road conditions [14].

C. Standards

Communication system of VANETs is standardized to integrate all the features from the physical to the application layer [2]. The main standards dealing with VANETs includes dedicated short range communications (DSRC), wireless access in vehicular environments (WAVE) and IEEE 802.11p.

- DSRC: Dedicated Short Range Communications

The federal communications commission (FCC) allocated a spectrum of 75 MHz band wide from 5850 to 5925 GHz for DSRC [15]. As shown in Fig. 2, the DSRC band is divided into seven channels with 10 MHz range for each channel. These channels are numbered 172, 174, 176, 178, 180, 182 and 184 from low to high, where channel 178 is the control channel and the other six are service channels [2]. Service channel 172 is reserved for critical safety of life that requires high availability and low latency and service channel 184 is reserved for public safety that requires high power.

- WAVE: Wireless Access in Vehicular Environments

The WAVE IEEE 1609 family defines an architecture and a complementary set of standardized protocols, services and interfaces to establish communications of V2V and V2I [16]. The security services as well as a wide set of applications for transportation are also defined in WAVE.

- IEEE 802.11p

IEEE 802.11p is added to the family of IEEE 802.11 protocols to accommodate vehicular networks [2]. 802.11p specifies the definitions of the physical and medium access layers for VANETs.

D. Characteristics

Compared with other types of MANETs, VANETs have the following unique characteristics. These characteristics are critical in the study of security, privacy, and trust management in VANETs as we will show in the following sections.

- Mobility

Vehicles in VANETs are normally moving at high speed. Therefore, a little delay in V2V communication can results in many problems [17].

- Dynamic Network Topology

The topology of VANETs changes quickly due to high mobility of the vehicles. This makes the VANETs vulnerable to attacks and it is difficult to identify malicious vehicles.

- Real-time Constraints

The transmission of information in VANETs has a particular time limit range. This is designed to give the receiver sufficient time to make decisions and take corresponding actions promptly.

- Computing and Storage Capability

It is ordinary to process large amount of information among vehicles and infrastructures in VANETs. Thus, the computing and storage capability is absolutely a challenging issue.

- Volatility

It is normal that the connections between two nodes in VANETs occur just once because of their mobility. The connections between nodes would remain for a limited period of time within a few wireless hops [6]. Thus, it would be difficult to ensure the security of personal contacts in VANETs

III. Security

The driving force behind VANETs is to provide comfort and safety to drivers and passengers. Therefore, effective security mechanisms should be designed to ensure the appropriate operation of VANETs. The key security services are availability, confidentiality, authenticity data integrity and non-repudiation [4]. In Fig. 3, the services and their corresponding threats and attacks are listed, which will be elaborated next in this section.

A. Availability

Availability ensures that the network and applications remain operational even in the presence of faulty or malicious conditions [18].

1) Denial of Service (DoS) Attack [19]: Inside or outside attackers perform the DoS by jamming the communication channel or overriding the resources in VANETs. The attackers may be distributed, which is called distributed denial of service (DDoS) [20]. The main goal is to prevent authorized nodes from accessing the services [17].

2) Jamming Attack [21]: The attacker disrupts the communications channel by using a strong signal with the equivalent frequency.

3) Malware Attack [22]: When malware is installed into the OBUs and RSUs, attackers can penetrate into the VANETs to disrupt the normal functionality.

4) Broadcast Tampering Attack [23]: Inside attackers may broadcast fake warning messages, which will conceal the correct safety messages to authorized vehicles.

5) Black Hole and Gray Hole Attack [24]: Black hole and gray hole attack will drop the packet while relaying them in the network. It is more difficult to detect gray hole attack because the attackers behave normally first but drop messages anytime without specific objectives.

6) Greedy Behavior Attack [25]: The malicious vehicles abuse the media access control (MAC) protocol by increasing the bandwidth at the cost of other vehicles.

7) Spamming Attack [26]: The attacker injects large amount of spam messages in the VANETs system, which will occupy the bandwidth to cause collisions.

B. Confidentiality

Confidentiality guarantees that only the designated receiver is able to access the data while outside nodes cannot understand confidential information that pertains to each entity. Cryptographic solutions can provide confidentiality [2].

1) Eavesdropping Attack [27]: Eavesdropping aims at extracting confidential information from the protected data. For example, stealing identity information or tracking the target vehicle through collecting location data.

2) Traffic Analysis Attack [4]: The attacker listens to the message transmission and then analyze its frequency and duration to gather confidential information.

C. Authenticity

Authentication is a mechanism to protect the VANETs against a malicious entities, and is considered to be the first line of defense against various attacks in VANETs [4].

1) Sybil Attack [28]: A sybil node can forge many fake identities to disrupt the normal operations of VANETs. It falsely informs other vehicles that there is traffic jam and enforce them to change their routes and leave the road clear.

2) Tunneling Attack [29]: A tunneling attack is similar to the wormhole attack [23]. The attackers connect two far-away parts in VANETs through a tunnel, or extra communication channel. As a result, the long-distance nodes can communicate as neighbors.

3) GPS Spoofing [30]: An attacker can generates false GPS signals stronger than the original signals from the trusted satellites to deceive the vehicles that it is available in a different location.

4) Free-Riding Attack [31]: In cooperative authentication scheme, selfish vehicles may take advantages of others' authentication contributions without making their own. Such selfish behavior is called free-riding attack that will bring about a serious threat to cooperative message authentication.

D. Integrity

Integrity ensures that the content of a message is not modified during transmission, which protects against the unauthorized creation, destruction or modification of data.

1) Message Suppression/Fabrication/Alteration Attack [29]: The attacker alters some part of the transmitting message to bring about an unauthorized effect.

2) Masquerading Attack [22]: The masquerading attacker can use the stolen passwords to enter VANETs as a valid user to broadcast false messages.

3) Replay Attack [14]: The attackers may continuously re-inject previously received beacons and messages back on to the network, which will confuse the traffic authorities when identifying vehicles in emergency incidents.

E. Non-Repudiation

Non-repudiation ensures that the sender and receiver of messages cannot deny its transmission and reception in case of dispute [32].

1) Repudiation Attack [4]: The attacker may deny the fact of sending or receiving critical messages in case of dispute.

IV. Privacy-Preserving Authentication

Privacy means individuals have the right to fully control information about themselves and decide the details of information communicated with others. The privacy of vehicles should be seriously considered besides security issues. Anonymous authentication is a common method to preserve privacy of vehicles in VANETs. Anonymity is the state of being unidentifiable within a set of subjects, which can be provided by pseudonyms. A digital pseudonym is a bit string used as a unique identifier for authentication without any personal identifiable information. Therefore, a pseudonym allows authentication of a specific entity without knowing its real identity [9]. Based on the employed cryptographic mechanisms, anonymous authentication schemes can be distinguished into five categories.

A. Schemes Based on Symmetric Cryptography

Symmetric cryptography has high computational efficiency and lower communication overhead that uses message authentication code (MAC) to authenticate messages. The sender generates the MAC for each message using the shared secret key. All nodes in an anonymity set using the same secret key and can verify the MAC attached with the massage. In 2005, Choi *et al.* [33] first combine symmetric authentication with the use of short-lived pseudonyms in VANETs. In their scheme, an authority sends each vehicle a unique identifier and a seed value to generate short-lived pseudonyms. Individual secret keys are shared between RSUs and vehicles. Only RSUs can verify MACs since RSUs share individual secret keys with vehicles. Xi *et al.* [34] suggest that vehicles keep a random keyset for authentication without central authority so that user privacy is preserved under the zero-trust policy in 2007. Anonymity is achieved by sharing the keys between

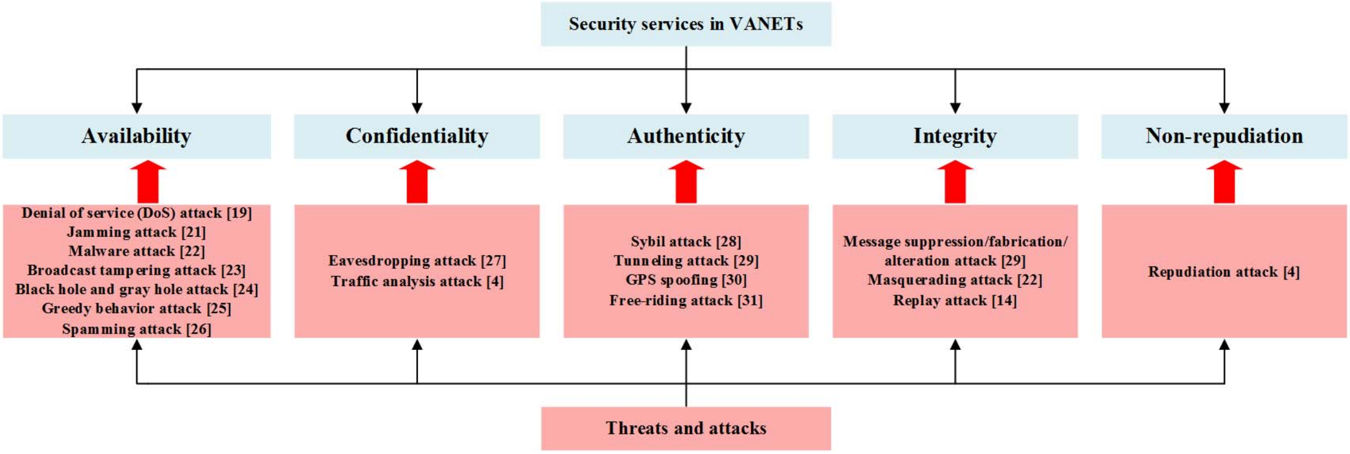


Fig. 3. Security services and the corresponding threats and attacks [2].

different random sets and is enhanced by using independent keys for authentications at neighboring RSUs.

However, there are two issues in symmetric cryptography based authentication. First, the key management in VANETs is vulnerable and will lead to overhead in communication and storage. Second, this scheme is lack of non-repudiation property so that it cannot provide authentication for each vehicle. In 2016, Vijayakumar *et al.* [35], [36] propose dual authentication and key management techniques for secure data transmission in VANETs. On the one hand, a dual authentication scheme provides a high level of security in the vehicle side to effectively prevent the unauthorized vehicles entering into the VANETs. On the other hand, a dual group key management scheme efficiently distributes a group key to the users for group keys update when the users join or leave the group.

B. Schemes Based on Public Key Infrastructure

Basically, vehicles are equipped with public/private key pairs for pseudonymous communication. Public-key certificates are used in public key infrastructure (PKI) as a secure and reliable method to authenticate a vehicle, which contains a vehicle's public key and the digital signature of a certification authority (CA) for authentication. Vehicles generate signature using the secret key and short-term pseudonyms. The signature and corresponding certificate will be attached to the message. The certificate based signature is verified by the receivers without revealing the sender's real identity.

CAs are responsible for long-term certificates issuance and management. In [37], vehicles request short-term pseudonyms from CAs in certain intervals. In order to alleviate the overhead of communication with CAs, self-issuance approaches of pseudonym [38] have been proposed to enable vehicle to generate pseudonyms by themselves. A novel pseudonym changing strategy [27] is presented in 2012 to restrict the lifetime of pseudonyms to hamper tracking. When vehicles gather at social spots such as a road intersection or a free parking lot, the pseudonyms are changed simultaneously if the anonymity set size (ASS) reaches a threshold. However, this strategy cannot perform well in low density scenarios. Pseudonym-identity mappings [9] are maintained for resolvability of pseudonyms in case of dispute investigation. Thorough protection is necessary to prevent abusing or leaking the sensitive privacy of the mappings. In 2010, Schaub *et al.* [39] propose a new approach that directly embedded resolution information in pseudonyms which are accessible only by multiple cooperative authorities. V-token approach has a scalability advantage because it distributes specific resolution information to each vehicle.

Revocation of pseudonym certificate is another challenge limited by scalability issues. If a vehicle's long-term certificate is revoked, it cannot obtain new pseudonyms from CAs or pseudonym providers. However, it is not practical for OBDs to verify pseudonyms against a certificate revocation list (CRL) due to the huge number of messages and large CRLs. Although several scalable CRLs distribution methods [40], [41] have been proposed after 2010, they cannot prevent a revoked vehicle from continue communicating in the network until all the pseudonyms are expired [9]. The high computational cost in the CRL checking process makes it infeasible to verify a large number of messages in a particular period in VANETs [42]. In 2017, Azees *et al.* [43] propose an efficient anonymous authentication scheme with conditional privacy preserving (EAAP) for VANETs. Based on bilinear pairing [44], the trusted authority (TA) in EAAP does not require storage of the anonymous certificates of vehicles and RSUs. In case of any disputes, the trust authority has the ability to revoke the anonymity of a misbehaving vehicle and disclose its real identity. Then the revoked identity is placed in the identity revocation list (IRL) maintained by the TA.

C. Schemes Based on Identity-Based Signature

Identity-based signature (IBS) [45] uses node's identifier as the public key and sign messages with the private key generated from the identifier. The sender's identifier is adequate to verify the signature without the need of additional certificates or explicit public keys. In IBS scheme, private key generator (PKG) acts as the third trusted authority for generation and assignment of private keys. In 2017, Karati *et al.* [46] introduce a new identity-based signcryption (IBSC) scheme using bilinear pairing with rigorous security analysis based on the intractability of decisional modified bilinear Diffie-Hellman inversion (MBDHI) and modified bilinear strong Diffie-Hellman (MBSDH) assumptions under formal security model without considering the concept of the random oracle, which demonstrates that IBSC scheme is provably secure.

There are four steps in IBS scheme: *Setup*, *Key Extraction*, *Signature Signing*, and *Verification*.

- *Setup*: The PKG computes a master key s and public parameters *param*. Then PKG sends *param* to all vehicles publicly.
- *Key Extraction*: PKG uses the mater key s and the vehicle's *ID* to compute a private key sek_{ID}. Then PKG sends private key sek_{ID} to the corresponding vehicle through secure channel.
- *Signature Signing*: Given a message M, timestamp T and private key sek_{ID}, the algorithm generates a signature *SIG*.
- *Verification*: Given the *ID*, M and *SIG*, the verification algorithm will determine whether *SIG* is valid or not.

In 2001, Boneh and Franklin [47] first use bilinear pairings on elliptic curves to establish the efficient ID-based encryption scheme. For the purpose of reducing the computational cost in the IBS scheme for VANETs, Lu *et al.* [48] propose a novel authentication framework using ID-based online/offline signature (IBOOS) in 2012. In the improved IBOOS [49] for VANETs, the signing process is separated into an online phase and an offline phase. The efficiency of verification is higher compared with that of IBS because the pairing process is accelerated. However, the requirement of much storage space for offline process makes IBOOS unsuitable for VANETs.

Compared with traditional PKIs, IBS eliminates the requirement of certificates in the verification of public keys. Thus, there is no need to distribute public keys with associated certificates. Moreover, IBS avoid the management of CRLs that cause heavy overhead in PKI-based schemes. However, all the private keys are generated by PKG in IBS. It means that PKG knows the private key of each vehicle in VANETs, which is the escrow problem. To address the escrow problem, Zhang *et al.* [50] suggest an efficient protocol called distributed aggregate privacy-preserving authentication (DAPPA) with multiple TAs in 2017. As shown in Fig. 4, system parameters and master secret are generated by root TA. Then the root TA issues a corresponding certificate for each RSU. Since each RSU has an initial private-public key pair and the issued certificate, it is responsible for authentication as the lower-level TA. Each vehicle has pre-loaded secret to establish secure channels with RSUs. When entering the RSU's communication range, vehicles request the shares of its private key. Within the authorized period, the vehicle generates a one-time private key and a one-time ID-based aggregate signature with the shares for each message. Then other vehicles can use the sender's ID to verify the signature. On one hand, the root TA merely know the system master secret but cannot obtain a vehicle's secret shares from the RSUs. On the other hand, the RSUs cannot access the vehicle's secrets from the root TA. DAPPA solves the escrow problem using a one-time private key that is unknown by root TA. However, it increases the system complexity dramatically because vehicles must request shares from next RSU when running out of the previous RSU's range. Moreover, the generation of one-time private key and the one-time ID-based aggregate signature will result in delay that reduce communication efficiency in VANETs.

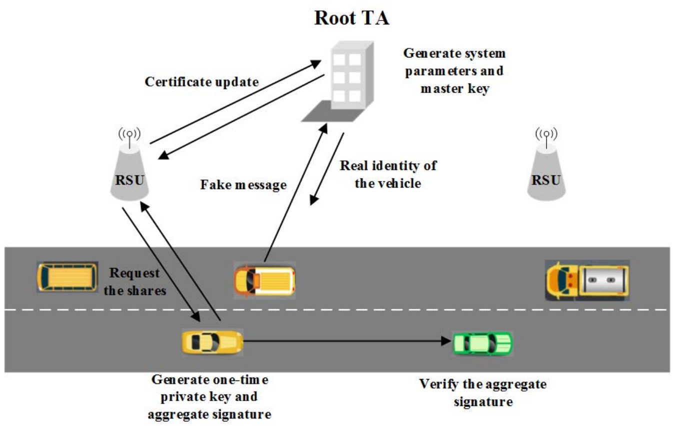

Root TA
Generate system parameters and master key
Certificate update
RSU
Fake message
Real identity of the vehicle
RSU
Request the shares
Generate one-time private key and aggregate signature
Verify the aggregate signature

Fig. 4. Distributed aggregate privacy-preserving authentication (DAPPA) protocol.

D. Schemes Based on Certificateless Signature

For the purpose of eliminating the costly management of certificates in PKI based scheme and solving the escrow problem in IBS, Al-Riyami and Paterson [51] first present certificateless public key mechanism in 2003. Unlike traditional PKI based scheme, no certificates are required in certificateless cryptography to guarantee the authenticity of public keys [52]. In certificateless cryptography, key generation center (KGC) acts as a semi-trusted third party that is responsible for supplying the user with a partial private key *DIDi* computed from user's identity *IDi*. Then user generates the actual private key with a secret value and the partial private key supplied by KGC. In contrast with ID-based cryptography, the KGC cannot access this private key. Then, the user uses the public parameters and the secret value to generate his public key *PKIDi*.

There are six algorithms in certificateless signature (CLS) scheme: *Setup*, *Partial Private Key Extract*, *Set Secret Value*, *Set Public Key*, *Sign* and *Verify* [51]. KGC performs the *Setup* and *Partial Private Key Extract*. Each algorithm is described as follows.

- *Setup*: This algorithm uses a security parameter k to generate the master secret key *msk* and master public key *mpk*. Then it also generates a public parameter *param* that is shared by all nodes.
- *Partial Private Key Extract*: This algorithm generates a partial private key D_{ID} using the master secret key *msk*, the master public key *mpk*, system parameter param and an identity *ID*.
- *Set Secret Value*: This algorithm generates a secret value x_{ID} using the master public key *mpk* and system parameter *param*.

- *Set Public Key*: This algorithm generates the public key PK_{ID} using the master public key *mpk*, system parameter *param*, an identity *ID* and *ID*'s secret value x_{ID}.
- *Sign*: This algorithm generates a certificateless signature σ using the master public key *mpk*, system parameter *param*, an identity *ID*, *ID*'s secret value x_{ID}, partial private key D_{ID} and a message M.
- *Verify*: This algorithm verify the signature using the master public key *mpk*, system parameter *param*, an identity *ID*, *ID*'s public key PK_{ID} and a message/signature pair (M, σ).

In the security models of CLS scheme, two types of adversaries are considered, i.e. super type I adversary A_I and super type II adversary A_{II} [52]. A_I simulates the real-world adversary who is able to obtain *ID*'s some valid signatures through eavesdropping on the target receivers. Then A_I will launch key replacement attack to replace *ID*'s public key with $PK^{'}_{ID}$ and generate valid signatures. A_{II} simulates the malicious KGC who has the master secret key and is able to launch eavesdropping attack on signatures and make signing queries. In recent years, several improved certificateless signature scheme called certificateless short signature (CLSS) [53]–[56] have been proved secure against A_I and A_{II} in the random oracle model. Because the proof process is complicated, we will not explain it in detail.

The security of most CLSS are based on bilinear pairings. Respectively, G_1 and G_2 are the additive and multiplicative groups with the same prime order q. And e: $G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing function, in which P is the generator of G_1. The properties of a bilinear pairing is as follows [57]:

- **Bilinear**: $\forall a, b \in Z_p^*$ and $\forall S, R \in G_1$, $e(aP, bP) = e(P, P)^{ab}$ and$e(S + R, P) = e(S, P)e(R, P)$.
- **Nondegenerate**: There exist two points $S \in G_1$ and $R \in G_1$ such that $e(R, S) \neq e(P, P)$.
- **Computable**: There exists an efficient algorithm to compute $e(R, S)$ for $\forall S, R \in G_1$.

However, a pairing operation consumes more computational power than an elliptic curve multiplication point operation [56]. After 2014, [58] and [59] propose CLS schemes without pairing to increase the efficiency. In order to guarantee the security of CLS schemes without pairing, the signature length must be very large, which is unacceptable for bandwidth limited and storage limited devices in VANETs. In 2015, [60] and [61] present a new certificateless aggregate signature scheme for V2I communication based on CLSS. Conditional privacy preservation is achieved by mapping the messages broadcasted by a vehicle to a pseudo identity. In case of dispute, the authority is able to retrieve the real identity from any pseudo identity. Since the deployment of CLSS in VANETs rely critically on efficient implementations of pairing primitives, several studies on hardware accelerators [62], [63] have been proposed to increase the efficiency of CLSS dramatically. Therefore, CLSS is a promising privacy-preserving authentication scheme in VANETs.

E. Schemes Based on Group Signature

The privacy of vehicles are preserved in group signature based schemes by allowing valid group members sign messages anonymously on behalf of the group [8]. Only the group manager has the capability to identify who is the actual sender. The main drawback of group signature is that it is usually time consuming to verify the signature, which is not suitable for time-stringent applications in VANETs.

In 2007, Lin *et al.* [64] propose a group signature and identity-based signature (GSIS) as a conditional privacy-preserving protocol for VANETs. On one hand, GSIS utilizes short group signature to sign the messages to provide anonymity and traceability requirements. On the other hand, it employs an additional identity-based signature scheme for messages to save bandwidth.

It is complicated to define the group manager (GM) in a group. In 2010, Zhang *et al.* [65] suggest that RSUs maintain the groups. When first entering the range of a RSU or the current private member key expires, the vehicle can request a new private member key. Park *et al.* [66] present RSU-based distributed key management (RDKM) in 2011 to manage the group key. Instead of having one management entity, RSUs also take charge of managing a part of the group key in a distributed manner.

In order to mitigate the overhead of revocation, distributed key management is a promising approach which divides whole VANETs into several subregions managed by each regional group manager. In 2012, Sun *et al.* [67] design distributed key management scheme (DKM) in VANETs that restricts authorization within a particular region and duration. However, the anonymity property of group signature still makes it possible for a malicious user to broadcast fake messages. Malina *et al.* [68] present a solution based on short-term linkable group signature and categorized batch verification. It is efficient to broadcast a group temporary revocation list (GTRL) between group managers for revocation of malicious members. In 2017, Islam *et al.* [69] propose an efficient password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) protocol for VANETs to provide group-key generation, user leaving, user join, and password change facilities. PW-CPPA-GKA is lightweight in terms computation and communication since it is bilinear-pairing-free.

V. Location Privacy

Most of the applications in VANETs (such as navigation system, accidents avoidance and even automatic driving) depend on the beacon messages broadcasted periodically by vehicles [70]. A beacon message (*ID*, t, s) contains the vehicle's identity, the timestamp and the state of the vehicle including the GPS coordinates, vehicle speed etc., which is used to avoid collision and to provide the location based services (LBSs). However, there exists a severe privacy threat for vehicles since the location information and the state of vehicle in beacon messages could be collected and misused. As defined in [71], the location privacy is the degree to which a spatial characteristic of an entity cannot be linked to its identity. By analyzing the beacon messages, any public, private, commercial, or criminal attackers could create detailed location profiles of vehicles and consequently their drivers [10]. Possession of such location profiles seriously threaten the privacy of drivers because there is generally a strong correlation between a vehicle and its driver. It is dangerous for a driver if his whereabouts are exposed to malicious criminals.

As elaborated in Section IV, there are many privacy protection mechanisms focusing on anonymous authentication, e.g. using pseudonyms for authentication that do not contain any identifying information. Several pseudonym updating and exchanging algorithms [72] have been presented to enhance the privacy of vehicles. Although pseudonyms provide identity privacy, we believe that privacy is more than anonymity. The sensitive information in the beacon messages will reveal the location privacy of vehicles. Moreover, vehicles are more vulnerable to tracking attack than mobile telephones. First, vehicles should broadcast beacon messages continuously as defined by the protocol of VANETs [73]. Second, clutter or false measurements are not allowed in beacon messages since the accuracy is significant for safety related applications. Third, the vehicles move under the constraints of traffic rules and roads. It is much easier to predict the dynamics of the target vehicle than the unpredictable movements of mobile telephones. Therefore, tracking attacks to vehicles are able to achieve high efficiency and accuracy using non-complex approaches. By analyzing the beacon messages, the attackers could launch tracking attack to get the private information of the target vehicle.

In this section, we first introduce the treat model and explain how tracking attackers exploit the information in anonymous beacon messages to reconstruct the trajectory of the target vehicle. Then, we present the state-of-the-art location privacy protection mechanisms aimed at thwarting the tracking attack and simultaneously guaranteeing the quality of the LBSs.

A. Threat Model

As shown in Fig. 5, we assume a global passive adversary (GPA) [71] who has access to LBSs and RSUs. The methods, behaviors, and goals of GPA are defined as follows:

1) Methods: A GPA has access to the data of RSUs and LBSs applications. He has knowledge of the road maps, traffic conditions, home owner names and addresses and geographical coordinates. A GPA may be an "insider" with legitimate authority to monitor these systems, or the attacker may have acquired/hacked such access illegally [74].

2) Behaviors: The GPA's behaviors are assumed to be passive, which means the GPA can only eavesdrop on the broadcasted beacon messages. The GPA can obtain data over a wide region for hours, days, months, or even longer periods of time. There exist other approaches for a GPA to track a target vehicle. For example, a video-based approach using traffic monitoring cameras is able to visually identify the target [75]. However, the adversary has to undertake overwhelming cost like cameras with sufficient high resolution to track the target vehicle. This paper only considers beacon messages broadcasted through DSRC even though other information from other devices may be useful to GPA.

3) Goals: The basic goal of the GPA is to reconstruct the trajectory of a target vehicle in order to determine whether it was at a given place at a given time. And the future goal is to track any specific vehicle in real-time.

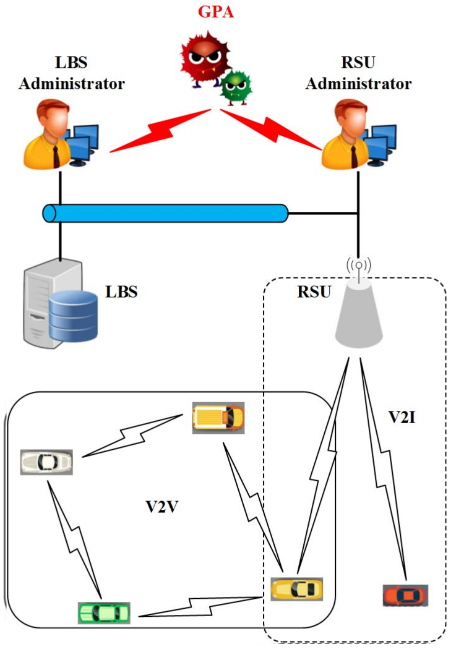


Fig. 5. Global passive adversary for vehicles' location privacy.

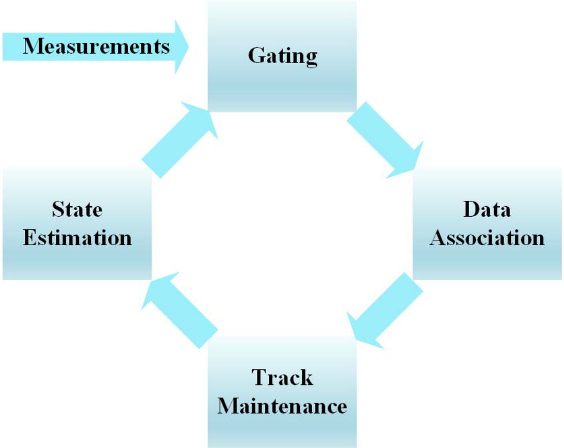


Fig. 6. Components of multiple targets tracking (MTT).

B. Tracking Attack

Several works [10], [73] have questioned the effectiveness of anonymous authentication in the protection of vehicles' location privacy and have successfully implemented the tracking attack in the simulator under the assumption that the beacon messages are completely anonymous. Vehicle tracking is considered to be a typical multiple target tracking (MTT) problem [73], which assumes a set of noisy measurements or observations detected by a sensor periodically every time interval which is called a scan. The goal is to determine the best estimate of the target's state and the associated probability in each scan. As explained in Fig. 6, the major components of MTT include *State Estimation*, *Gating*, *Data Association*, and *Track Maintenance*.

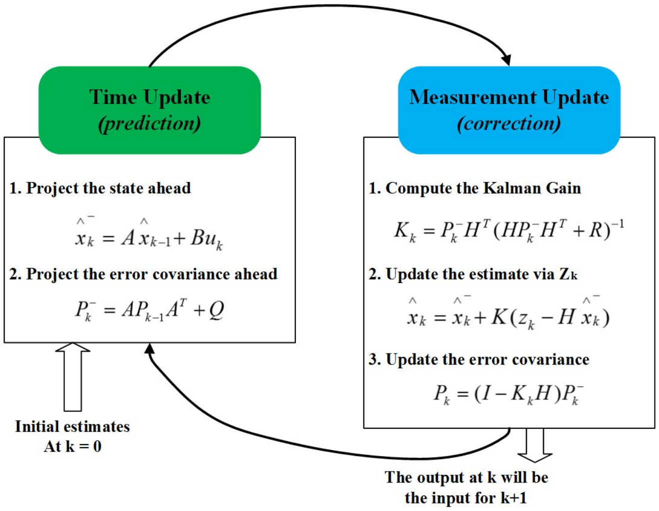

Time Update
(prediction)
1. Project the state ahead
$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_k$
2. Project the error covariance ahead
$P_k^- = AP_{k-1}A^T + Q$
Measurement Update
(correction)
1. Compute the Kalman Gain
$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1}$
2. Update the estimate via Zk
$\hat{x}_k = \hat{x}_k^- + K(z_k - H\hat{x}_k^-)$
3. Update the error covariance
$P_k = (I - K_k H)P_k^-$
Initial estimates
At k = 0
The output at k will be
the input for k+1

Fig. 7. The prediction phase and correction phase in recursive Kalman filter.

1) State Estimation: From the internal network of a vehicle, we can get the vehicle state including the GPS coordinates, velocity, and steering wheel angle [76]. Unfortunately, it is impossible to identify the exact vehicle state since the GPS receiver, speedometer, etc. are still imperfect sensors with limited precision. In order to track a vehicle with the noisy measurements, we should better estimate its exact state using a state estimation filter, e.g. Kalman filter [77]. It gives a better estimate or correction for a state x_k at time k taking into account both the previous states $x_1, x_2, x_3, \ldots, x_{k-1}$ and the inaccurate measurement z_k detected at time k [73]. As explained in Fig. 7, the Kalman filter is a set of mathematical equations that provide an efficient recursive method to estimate the state of a stochastic process, which minimizes the mean of the squared error. Due to space limitations, the detailed principle of the Kalman filter can be found in [77].

2) Gating: In the tracking attack, a data association should be performed to assign each measurement to the correct target vehicle. Because of the high traffic density, a validation process or gating should be performed before the state estimation to avoid unnecessary computation. The goal of gating is to eliminate the measurements that are less likely to be broadcasted from the target vehicle to relieve the computationally overhead of data association process. The gating process forms a validation area around the track and any measurement located outside this area will be excluded from the data association.

3) Data Association: It is likely to have several measurements that are validated for the target vehicle. Data association is necessary to avoid incorrect or sub-optimal solutions [73], [78]. The probability P_{ij} of assigning a measurement j to track i is defined as:

$$P_{ij} = \frac{G_{ij}}{T_i + M_j - G_{ij}}, \quad G_{ij} = \frac{e^{-d_{ij}^2/2}}{(2\pi)^{N_m/2}\sqrt{|S_i|}}$$

G_{ij}: the Gaussian likelihood function associated with the assignment of measurement$j$ to track i.

T_i: the sum of likelihood functions G_{ij} of track i.

M_j: the sum of likelihood functions G_{ij} of measurement$j$.

d_{ij}^2: the normalized distance between the measurement$j$ and track i defined in the Kalman filter.

$|S_i|$: the determinant of the residual covariance matrix defined in the Kalman filter.

N_m: the dimension of the measurement vector.

After all probabilities are calculated, the optimal associations that maximize the sum of probabilities will be used to update each track individually.

4) Tracking Maintenance: The tracking maintenance is a separate or joint process with data association to handle track initiation, confirmation and deletion. When a received measurement is not assigned to a previously established track, a new track is initiated as a tentative track until it is confirmed in subsequent scans. On the other hand, if a track is not updated for a while, it should be deleted to avoid computational overhead.

C. Protection Mechanisms Against Tracking Attack

The simulation results in [10] and [73] show that the random noise in measurements and the time interval of beacon messages have significant influence on the accuracy of the tracking attack. Generally, larger measurement noise and longer time interval of beacon messages make the tracking attack more difficult. However, the quality of LBSs is important for safety applications, which requires precise and frequent vehicle state update. Therefore, it is crucial to take into account the trade-off between the location privacy and the quality of the LBSs when designing and evaluating the privacy protection mechanisms [79].

1) Pass and Run: In 2014, Dunbar and Qu [80] propose a *Pass and Run* protocol for vehicular delay tolerant networks (VDTNs) to address the vehicle location privacy problem in regards to communication with RSUs. The basic idea is to pass the messages to other nodes/vehicles in the VDTNs instead of submitting them directly to the RSUs. Using this method, the vehicle and the messages it generates may travel in different path. The mobility of the vehicles and delay of submission to the RSU will add obfuscation in the location and time domain, and thus render the exact location of the source vehicle and the time when the message is generated. As illustrated in Fig. 8, the first message from S may be passed to vehicle 1, then vehicle 2, then vehicle 3, and eventually sent to RSU Z. Meanwhile, the second message is also passed to vehicle 1 and sent to RSU X earlier than the first message; and finally the third message will be delivered to RSU Y via the relay of vehicles 1 and 2 and arrive Y earlier than the first message too. From this information, it will be hard for the roadside infrastructure to discover the driving path of vehicle S. In this example, the message receiving record would suggest two consecutive right turns. Therefore, the location privacy is preserved.

The major shortcoming of the *Pass and Run* protocol is that the submission delay of the messages dramatically increases, which makes it unsuitable for some applications that require real-time traffic information.

2) Mix-Zones: Mix-zones [81], [82] are special regions where the adversary cannot eavesdrop the V2V and V2I

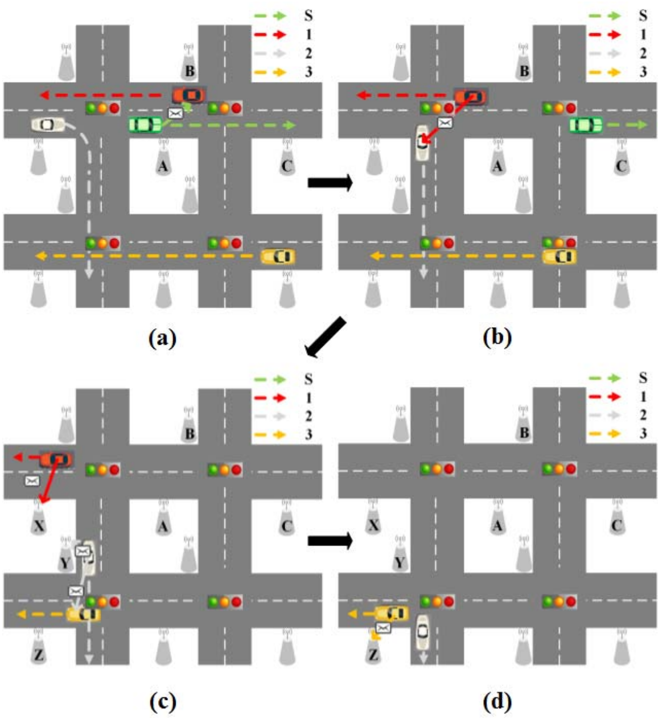


Fig. 8. Example sequence of events for *Pass and Run* protocol: (a) Vehicle S passes three messages to vehicle 1. (b) Vehicle 1 passes the first and third messages to 2. (c) Vehicle 1 sends the second message to X; vehicle 2 passes the first message to 3 and sends the third message to Y; S is moving out of the scene. (d) Vehicle 3 passes the first message to Z.

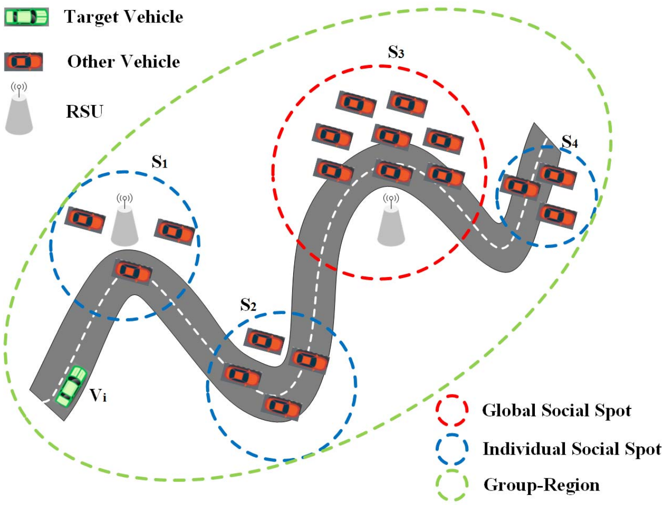


Fig. 9. Group region [75].

communication. A tracking attacker has to locate the target vehicle from several vehicles exiting in the same mix-zone, which is difficult if the mix-zone has high traffic density. Thus, building numbers of mix-zones in cities can effectively prevent the vehicles from being tracked. Although mix-zone can protect the vehicles' location privacy, the safety and liability may be impaired because LBSs also cannot get the broadcasted messages from the mix-zones.

The effectiveness of mix-zones depends on the number of vehicles entering the zones and changing its pseudonyms simultaneously. How to deploy mix-zones in a large city is a challenging problem [82]. In order to efficiently exploit the potential opportunities for pseudonym mixture, Yu *et al.* [75] propose MixGroup in 2016 to integrate the group signature mechanism with mix-zones that constructs extended pseudonym-changing regions where vehicles are allowed to successively exchange their pseudonyms. As illustrated in Fig. 9, there are global and individual social spots along the path of the target vehicle $\mathrm{V_i}$. Conventionally, the target vehicle is allowed to change its pseudonyms in the global social spot $\mathrm{S_3}$ where there are 8 other vehicles. To efficiently leverage the individual social spots $\mathrm{S_1}$ with 3 other vehicles, $\mathrm{S_2}$ with 4 other vehicles, and $\mathrm{S_4}$ with 3 other vehicles, MixGroup strategically combines all the social spots to constitute an extended group region. Then, $\mathrm{V_i}$ is allowed to accumulatively exchange pseudonyms with vehicles that it meets in the group region. Therefore, $\mathrm{V_i}$ will meet in total $3+4+8+3 = 18$ other vehicles instead of 8 other vehicles, so that the opportunities for pseudonym mixture are significantly increased. In this way, location privacy is preserved without heavy impact on the quality of LBSs.

3) Obfuscation-Based Approaches: As mentioned before, low accuracy of location information and long time interval of beacon messages make the tracking attack difficult. Reference [83] believes that decreasing the accuracy of location information makes it easier to protect the location privacy of vehicles because many LBSs do not need that accurate location information to provide an acceptable quality of service to vehicles. In 2015, Emara *et al.* [79] propose an obfuscation privacy scheme which perturbs position and beacon frequency. They use Monte Carlo analysis to measure the impact on a safety application by estimating the probability of correctly identifying the application's fundamental factors. The results show that compared with mix-zone, it can protect the location privacy of vehicles by increasing more tracker confusions with less cost of safety and liability. In 2017, Takbiri *et al.* [84] incorporate the major tools in location privacy protection to investigate the degree of location privacy when obfuscation and anonymization are employed.

VI. Trust Management

Trust management is an inherent issue in VANETs. Various authentication methods are utilized to ensure the messages are broadcasted by authorized vehicles. However, it cannot prevent an authorized vehicle from broadcasting bogus or altered messages malevolently. These bogus or altered messages may not only decrease the transportation efficiency, but may also cause accidents that can threaten human's life in the worst cases [85]. For example, vehicle A broadcasts a warning message to warn the vehicles behind it that A is out of control. When vehicle B receives this warning message, it is crucial for B to determine the trustworthiness of the message and take a quick response. In this case, it is impractical to ask neighbor vehicles or a trusted third party (TTP) for help due to the strict time constraint. If this warning message is bogus, it is dangerous for vehicle B to brake hard. How to establish trust among authenticated vehicles is a serious issue. It is desirable that each vehicle in VANETs can detect dishonest vehicles and the malicious messages sent by them.

Because of unique characteristics of VANETs, some challenges are presented for trust management such as decentralization and scalability [86]. Moreover, it is common that two vehicles may interact with each other just once and there is no guarantee to meet in the future [87]. Thus, it is impossible to depend on centralized systems such as TTP to build long-term relationships.

A. Significant Properties of Effective Trust Management

In order to design a desirable trust management model for VANETs, there are several significant properties to be considered as follows.

- **Decentralization**

Decentralized trust management is suitable for VANETs because of high dynamic and distributed nature of VANETs. Public/private key pair is required for distributed mutual verification of vehicles. The trustworthiness of a vehicle is determined either using V2V interactions or depending on the real world role of drivers in a decentralized fashion.

- **Real-time Constraint**

The real-time constraint is strict in trust management models, especially propagating warning messages among vehicles. It is important to promptly determine the trustworthiness of a warning message so that the driver has enough reaction time to avoid dangerous situation. When designing trust management models, the latency for making a decision should be limited in the millisecond level if an emergency happens.

- **Information Sparsity**

The situation of information sparsity or a total lack of information is prevalent in VANETs. The information received in the direct interaction is important and the weight of such information should increase in trust calculation mechanism. Alternatively, RSUs should be utilized to determine the trust level of any available information.

- **Scalability**

In rush hour with a high density of vehicles, there will be a large number of messages broadcasted. Quick responses in emergency situations by analyzing the redundant information received from other vehicles is critical.

- **Privacy**

Identity and location privacy is always a crucial concern in VANETs. PKI can be used for authentication without needing any sensitive information from the sender.

- **Robustness**

Trust management system may become the target of attackers. The trust-distortion attacks [88] can mislead the trust-based network operations by deceiving the trustworthiness computation. And the estimation of trustworthiness for another node will be distorted. Thus, it is of great importance to ensure the robustness of the trust management itself. On one hand, the process of calculating the trustworthiness of a node should be robust. On the other hand, there should be detection mechanism as well as penalty mechanism to detect and punish the malicious node as long as it attacks the trust management system.

B. Trust Management Models in VANETs

Trust management methods based on third trust party (TTP) have been proposed [89]–[91]. Bißmeyer *et al.* [89] present a central evaluation scheme running on vehicles and RSUs to identify attackers and exclude them from the network. It uses trust and reputation information from misbehavior reports to guarantee VANET's long-term functionality. Li *et al.* [90] propose an announcement scheme for the evaluation of message reliability. The scheme focuses on the robustness and fault tolerance against temporary unavailability of the central server. Li *et al.* [91] propose a reputation-based global trust establishment (RGTE) scheme to share the trust information in VANETs based on statistical laws. Generally speaking, TTP-based trust management methods need a reputation server or a reputation management center to establish a global reputation system. However, such centralized infrastructure may be a target for attackers, the cost is high to maintain the normal function of TTP and could be higher or recovery from failure. Thus, methods based on centralized infrastructure is not suitable for VANETs.

Another approach to establish trust management in VANETs is to use clusters [92]–[96]. Kumar and Chilamkurti [92] propose a trust aware collaborative learning automata based intrusion detection system (T-CLAIDS) for trust management in VANETs. It relies on the high density of vehicles in a given region to design a classifier that can be tuned based on the so-called collaborative trust index (CTI) in order to detect any malicious activity. Wahab *et al.* [93] use reputation that is linked to network's services as incentives and design a two-phase model to motivate nodes to cooperate during cluster formation and to detect misbehaving nodes after clusters are formed. Sedjelmaci and Senouci [94] implement an accurate and lightweight intrusion detection framework called AECFV to protect VANETs against most dangerous attacks. AECFV uses a secure clustering algorithm to select a cluster head (CH) based on vehicle's mobility and trust level. Yang *et al.* [95] utilize RSUs to establish a cluster consensus-based trust management scheme. The CH is generated based on V2V and V2I communications and takes responsibility for intra-cluster trust management. Ltifi *et al.* [96] use Petri Nets to model active vehicles that are able to make decision on the trustworthiness of alert messages based on an effective cooperation model for VANETs. These methods improve the cooperation among vehicles in VANETs by forming a cluster and selecting a CH according to some specific algorithm. Safety information aggregated from all vehicles in the cluster is used to calculate the trustworthiness of vehicles and messages. Consensus is achieved through cooperation of all vehicles. The major drawback of cluster-based trust management methods comes from the ephemeral nature of VANETs. The correctness of CH's decision normally depends on the scale of the cluster, which means that cluster-based methods may fail in regions of low vehicle density. Moreover, the contact between each vehicle in VANETs is short lived so that it is difficult to maintain a stable cluster for the purpose of trust management.

It is practical to deploy decentralized trust models that do not fully depend on the static infrastructures. These models can be classified into three categories: (1) entity-centric trust models, (2) data-centric trust models, and (3) combined trust models [86]. As shown in Fig. 10, several representative models will be explained in detail.

1) Entity-Centric Trust Models: Entity-centric trust models aim at estimating the trustworthiness of vehicles [97]. The main methods to achieve this efficiently and accurately is to establish a reputation system or to make decision according to the opinions of neighbors. There are several typical works. Minhas *et al.* [98] develop a multifaceted trust modeling approach to detect the entities that are generating malicious data. This method incorporates role-, experience-, priority-, and majority-based trust to make real-time decision. Mármol and Pérez [99] suggest a trust and reputation infrastructure-based proposal (TRIP) relying on RSUs to distinguish malicious or selfish vehicles in VANETs with high efficiency and accuracy. Three different sources of information are considered when estimating the reputation score for each vehicle: direct previous experiences with the target vehicle, recommendations from surrounding vehicles, and the recommendation from a central authority. Haddadou *et al.* [100] propose a distributed trust model (DTM^2) to allocate credits to vehicles with secure management. Self-selection mechanisms are created in the network that will exhaust the credit of the misbehaving vehicles. Generally, the correctness of data from other vehicles can be guaranteed. Since vehicles move quickly on the road, it is difficult to collect enough information to calculate the reputation score of a specific node. Moreover, how to ensure the security of the reputation system itself is another serious issue that have not been resolved.

2) Data-Centric Trust Models: Data-centric trust models focus on estimating the trustworthiness of received data [97]. In order to accurately verify the trustworthiness of the received data, the models need cooperative information from various sources such as neighbor vehicles or RSUs. Gurung *et al.* [101] design a trust model to estimate the trustworthiness of a message directly according to various factors including content similarity, content conflict and route similarity. Huang *et al.* [102] develop a voting system with different voting weights based on its distance from the event. The opinion from the vehicle closer to the event possesses higher weight when evaluating the trustworthiness of a message. Rawat *et al.* [103] propose a deterministic approach to measure the trust level of the received message by using received signal strength (RSS) for distances calculation and the vehicle's geolocation (position coordinate). Hussain *et al.* [104] suggest email-based social trust and social networks-based trust to establish and manage data level trust. The major drawbacks of data-centric trust models are latency and data sparsity. Respectively, large number of data from various sources may contain redundant information, which will increase latency or overwhelm the significant information. On the contrary, data sparsity is prevalent in VANETs. It is unrealistic for data-centric trust models model to perform well without enough information.

3) Combined Trust Models : Both entity and data are the major focuses in this category [97]. Combined trust models not only evaluate the trust level of vehicles but also calculate the trustworthiness of data [105]. Thus, these models inherit the benefits and drawbacks of entity-centric and data-centric trust models. Attack-resistant trust management scheme (ART) proposed by Li and Song [106] estimates the trustworthiness of both vehicles and messages to cope with malicious attacks in VANETs. Trustworthiness of data is evaluated based on the received data from multiple vehicles. Trustworthiness of a node is determined based on functional trust and recommendation trust, which respectively indicates whether a node can fulfill its functionality and what is the trust level of the recommendations from it. The proposed scheme does not take account of data sparsity, which is pervasive in VANETs

VII. Simulation Tools

When developing applications for VANETs, security, trust and privacy should be seriously considered. However, there are many obstacles when emulating the performance and security of applications due to the nature of VANETs such as high mobility, network complexity and decentralization. In order to obtain accurate results, it is essential to design simulation tools to simulate the real VANETs.

Simulation tools for VANETs consist of mobility simulator and network simulator. Respectively, mobility simulator is used to create a mobility model for stimulating the vehicles' movement pattern. Network simulator is responsible for evaluation of the operation of VANETs and highlighting the existing issues. The ultimate purpose of simulation tools is to provide results closest to real-world observation.

A. Mobility Simulator

In VANETs, the regulation of vehicle movements should be connected with the simulation tools to create a random topology according to the circumstances of each vehicle [7]. Since it is difficult for network simulator to present a real-world traffic scenario, several mobility simulators can be employed to generate mobility model for each vehicle. It is possible to generate movement traces on the fly and allow network simulation to influence mobility simulation [107]. According to the granularity of the examined traffic flows, mobility simulators can be classified into two categories: macroscopic and microscopic models.

METACOR [108] models treat traffic like a liquid at a large scale, which cannot present vehicles' behavior precisely. Thus, METACOR is good at providing the macro perspective of the traffic.

VanetMobiSim [109] reviews the macroscopic and microscopic mobility description and details the additions to both scopes. However, VanetMobiSim cannot gain any feedback after parsed trace files are sent to the network simulator with high efficiency.

SUMO [110] employs an extension of car-following model proposed by Stefan Krauβ [111]. SUMO is a purely microscopic traffic simulation and can import city maps with

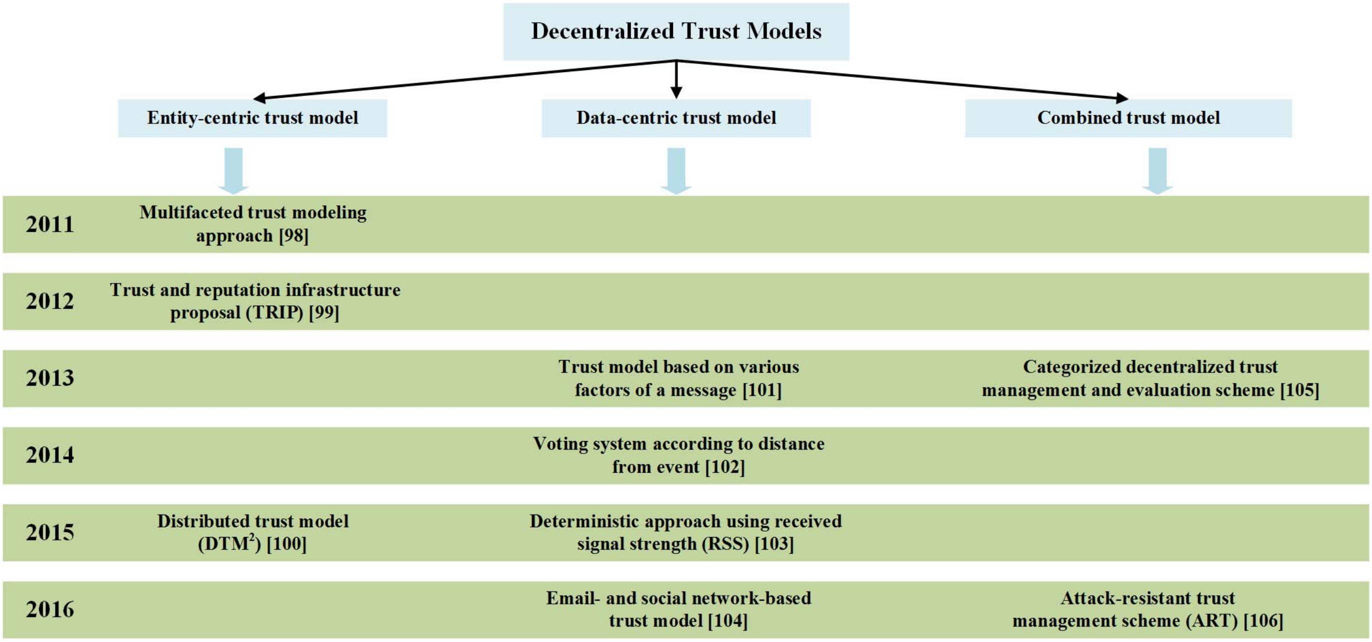

Decentralized Trust Models
Entity-centric trust model
Data-centric trust model
Combined trust model
2011
Multifaceted trust modeling approach [98]
2012
Trust and reputation infrastructure proposal (TRIP) [99]
2013
Trust model based on various factors of a message [101]
Categorized decentralized trust management and evaluation scheme [105]
2014
Voting system according to distance from event [102]
2015
Distributed trust model (DTM²) [100]
Deterministic approach using received signal strength (RSS) [103]
2016
Email- and social network-based trust model [104]
Attack-resistant trust management scheme (ART) [106]

Fig. 10. Decentralized trust models proposed in recent years.

different file formats. Each vehicle is described in detail by explicitly defining several parameters including an ID of vehicle, the departure time, and the vehicle's route etc. [110] Moreover, SUMO is capable of high-performance simulations for huge networks and is able to process feedback from network simulator.

Compared with METACOR and VanetMobiSim, SUMO is more suitable for V2V and V2I communications in which the individual vehicle's behavior should be taken into account and the feedback of each vehicle should be uploaded to network simulator for further processing.

B. Network Simulator

Various network simulators such as NS-2 [112], NS-3 [113], GlomoSim [114] and OMNeT++ [115] have been used to evaluate the performance and security of routing protocols in VANETs. High level programming languages such as C++ or Java are used to develop the simulators.

Originally, NS-2 was developed for networking research to substantially support for simulation the transmission control protocol (TCP), routing, and multicast protocols over wired networks [112]. NS-2 uses C++ in comprehensive protocol implementation and uses objective tool command language (OTcl) for the simulation configuration, which is a significant advantage for rapid generation of large scenarios [7]. The major drawback of NS-2 is that users need to program the node manually to find nearby nodes and establish communication.

NS-3 is developed to deal with this drawback, while it is different from NS-2 in several aspects [7]. In order to enhance the scalability and the modularity, NS-3 provides interface for Python scripting and an architecture to integrate several open source software [113].

The global mobile information system simulator (GlomoSim) is able to run on shared-memory symmetric processor (SMP) to divide the network into separate modules as parallel processes [114], which has high efficiency to support millions of nodes in a single simulation. However, GloMoSim is designed using the parallel discrete event simulation capability provided by Parsec, a parallel programming language and currently supports protocols for a purely wireless network. GloMoSim uses the Parsec compiler to compile the simulation protocols. Thus, its compatibility is not as good as NS-2 and NS-3.

The OMNeT++ discrete event simulation environment has been created with the simulation of communication networks, multiprocessors and other distributed systems to be as general as possible [115]. OMNeT++ is significantly different from NS-2 and NS-3 whose goal is to build a network simulator. While OMNeT++ focuses on providing a simulation platform and the basic machinery and tools for researchers to design simulation models, which makes it more flexible and suitable for the high-mobility VANETs.

C. Integrated Simulation Platform

Mobility simulator should be able to process feedback from network simulator to modify the traffic parameters. SUMO is preferred to generate a mobility models for simulation because it has significant features: First, SUMO has a road network importer that is compatible with different source formats and can generate demand and routing utilities. Second, it has a remote control interface to efficiently simulate single junctions and whole cities [116]. There are several integrated simulation platform using SUMO and different kind of network simulators for VANETs.

Network Simulation Environment (TraNS) is specially developed for VANETs and consists of two open-source simulators: SUMO [110] and NS-2 [112]. In TraNS, NS-2 can use realistic mobility models and influence the behavior of SUMO based on the V2V communication [117]. The major drawback is that TraNS can neither support large-scale simulations nor model the cost of securing protocols of VANETs.

An integrated wireless and traffic platform for real-time road traffic management solutions (iTETRIS) [118] aims at extending the advanced simulation of VANETs for evaluating services and applications for road traffic management. iTETRIS integrates SUMO [110] and NS-3 [113] to provide a real-time closed-loop coupling simulation platform, which can be regarded as a logical extension of TraNS [117]. Compared with NS-2, NS-3 is stable even the number of vehicles is very large. The idea of clear distribution of responsibilities is suitable for implementing own applications conveniently for developers [116].

The vehicles in network simulation (Veins) framework [107] combining SUMO with OMNET++ [115] is a further integrated simulation platform, which provides high level architecture (HLA) to allow the interaction between SUMO and other network simulators [116]. The significance of bidirectional coupling has two aspects. On one hand, the network simulation is able to directly control the mobility simulation for simulation of the communication's influence on the traffics in VANETs. On the other hand, information including position or planned route can be provided by mobility simulation as feedback to the network simulation. Veins provides all necessary functionality to perform bidirectional coupling that has higher accuracy in the evaluation of developed protocols [107].

VIII. Conclusion

Providing comfort and safety to both drivers and passengers is the major goal of VANETs, which are becoming a promising research field in ITSs. However, security, privacy and trust management are challenging issues due to the unique characteristics of VANETs. In this survey, we first review the basic knowledge of VANETs. Then the main security services with their threats and attacks are explained briefly. We have discussed the anonymous authentication schemes used to protect privacy of each vehicle. Next, three types of trust models are summarized as well as the significant properties to establish efficient trust management in VANETs. Considering that future applications in VANETs are required to be evaluated on aspects of performance and security, integrated simulation platforms with the idea of bidirectional coupling are introduced finally. In summary, this survey avoids the overlap with existing surveys on well-studied security topics, focusing on novel privacy-preserving methods and trust models, fills the gaps and reports the recent advances in VANETs.

We believe that the future research direction of VANETs should focus on privacy preservation and trust management. With the popularity of V2V and V2I communications, the valuable traffic information will be shared among all vehicles with high efficiency. The drivers and passengers will pay more and more attention to the trustworthiness of the huge amount of information and seek perfect protection for their privacy, which requires the VANETs to provide a trustworthy communication environment and simultaneously protect the vehicles' identity and location privacy.

References

[1] M. Alam, J. Ferreira, and J. Fonseca, "Introduction to intelligent transportation systems," in *Intelligent Transportation Systems*. Cham, Switzerland: Springer, 2016, pp. 1–17.

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

[3] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Veh. Commun.*, vol. 1, no. 1, pp. 33–52, 2014.

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

[5] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2008, pp. 2036–2040.

[6] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[7] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

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

[9] 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.

[10] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Proc. 7th Int. Conf. IEEE Wireless On-Demand Netw. Syst. Services (WONS)*, Feb. 2010, pp. 176–183.

[11] S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, "Anomaly detection for Internet of vehicles: A trust management scheme with affinity propagation," *Mobile Inf. Syst.*, vol. 2016, 2016, Art. no. 5254141.

[12] S. S. Kaushik, "Review of different approaches for privacy scheme in VANETs," *Int. J.*, vol. 5, no. 2, 2013.

[13] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, *Overview of Security Issues in Vehicular Ad-Hoc Networks*. Hershey, PA, USA: IGI Global, 2010.

[14] B. G. Premasudha, V. R. Ram, J. Miller, and R. Suma, "A review of security threats, solutions and trust management in VANETs," *Int. J. Next-Generat. Comput.*, vol. 7, no. 1, pp. 38–57, 2016.

[15] Federal Communications Commission, "Amendment of the commission rules regarding dedicated short-range communication service in the 5.850-5.925 GHz band," FCC, Washington, DC, USA, Tech. Rep. FCC 02-302, 2002.

[16] *ITS Standards Fact Sheets of IEEE*, IEEE Standard 1609, ITS, Apr. 2014. [Online]. Available: http://www.standards.its.dot.gov/factsheets/factsheet/80

[17] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," *Int. J. Comput. Sci.*, vol. 2, no. 1, pp. 88–96, 2013.

[18] Y. Qian and N. Moayeri, "Design of secure and application-oriented VANETs," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2008, pp. 2794–2799.

[19] K. Verma, H. Hasbullah, and A. Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," in *Proc. IEEE 3rd Int. Adv. Comput. Conf. (IACC)*, Feb. 2013, pp. 550–555.

[20] I. A. Sumra, H. B. Hasbullah, and J.-L. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," in *Vehicular Ad-hoc Networks for Smart Cities*. Singapore: Springer, 2015, pp. 51–61.

[21] R. Minhas and M. Tilal, "Effects of jamming on IEEE 802.11p systems," Chalmers Univ. Technol., Gothenburg, Sweden, Tech. Rep. EX 086, 2010.

[22] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. 6th Int. Conf. IEEE Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2012, pp. 1–9.

[23] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.

[24] K. Jain and D. Goyal, "Design and analysis of secure vanet framework preventing black hole and gray hole attack," *Int. J. Innov. Comput. Sci. Eng.*, vol. 3, no. 4, pp. 9–13, 2016

[25] M. N. Mejri and J. Ben-Othman, "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 5032–5037.

[26] F. Sabahi, "The security of vehicular adhoc networks," in *Proc. 3rd Int. Conf. IEEE Comput. Intell., Commun. Syst. Netw. (CICSyN)*, Jul. 2011, pp. 338–342.

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

[28] J. Grover, V. Laxmi, and M. S. Gaur, "Sybil attack detection in VANET using neighbouring vehicles," *Int. J. Security Netw.*, vol. 9, no. 4, pp. 222–233, 2014.

[29] 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.

[30] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. ION GNSS*, 2005, pp. 1285–1290.

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

[32] F. Al-Hawi, C. Y. Yeun, and M. Al-Qutayti, "Security challenges for emerging VANETs," in *Proc. 4th Int. Conf. Inf. Technol. (ICIT)*, 2009, pp. 3–5.

[33] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proc. 1st ACM Int. Workshop Quality Service Security Wireless Mobile Netw.*, 2005, pp. 79–87.

[34] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. 8th Int. Symp. IEEE Auto. Decentralized Syst. (ISADS)*, Mar. 2007, pp. 344–351.

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

[36] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2439–2450, 2017.

[37] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility," in *Proc. IEEE Intell. Veh. Symp.*, Jun. 2007, pp. 541–546.

[38] K. Zeng, "Pseudonymous PKI for ubiquitous computing," in *Proc. Eur. Public Key Infrastruct. Workshop*, 2006, pp. 207–222.

[39] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2010, pp. 1–6.

[40] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal, "Analysis of certificate revocation list distribution protocols for vehicular networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[41] E. N. Michael and L. O. Henry, "Scalable certificate revocation list distribution in vehicular ad hoc networks," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2010, pp. 54–58.

[42] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generat. Comput. Syst.*, vol. 78, pp. 943–955, Jan. 2016.

[43] 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.

[44] I. F. Blake, V. K. Murty, and G. Xu, "Refinements of Miller's algorithm for computing the Weil/Tate pairing," *J. Algorithms*, vol. 58, no. 2, pp. 134–149, Feb. 2006.

[45] A. Shamir *et al.*, "Identity-based cryptosystems and signature schemes," in *Crypto*, vol. 84. Berlin, Germany: Springer, 1984, pp. 47–53.

[46] A. Karati, S. H. Islam, G. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments," *IEEE Internet Things J.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/document/8013031/

[47] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO*. Berlin, Germany: Springer, 2001, pp. 213–229.

[48] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in *Proc. Comput., Commun. Appl. Conf. (ComComAp)*, Jan. 2012, pp. 345–350.

[49] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Advances in Cryptology-CRYPTO*. Berlin, Germany: Springer, 2001, pp. 355–367.

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

[51] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Asiacrypt*, vol. 2894. Berlin, Germany: Springer, 2003, pp. 452–473.

[52] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signature revisited," in *Information Security and Privacy*. Berlin, Germany: Springer, 2007, pp. 308–322.

[53] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Comput. Standards Inter.*, vol. 31, no. 2, pp. 390–394, 2009.

[54] R.-H. H. Chun-Ifan and P.-H. Ho, "Truly non-repudiation certificateless short signature scheme from bilinear pairings," *J. Inf. Sci. Eng.*, vol. 27, pp. 969–982, 2011.

[55] D. He, B. Huang, and J. Chen, "New certificateless short signature scheme," *IET Inform. Secur.*, vol. 7, no. 2, pp. 113–117, 2013.

[56] J.-L. Tsai, "A new efficient certificateless short signature scheme using bilinear pairings," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2395–2402, Dec. 2017.

[57] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. Adv. Cryptol. ASIACRYPT*, 2001, pp. 514–532.

[58] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings," *Int. J. Commun. Syst.*, vol. 27, no. 7, pp. 1083–1090, 2014.

[59] K.-H. Yeh, K.-Y. Tsai, and C.-Y. Fan, "An efficient certificateless signature scheme without bilinear pairings," *Multimedia Tools Appl.*, vol. 74, no. 16, pp. 6519–6530, 2015.

[60] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015.

[61] A. K. Malhi and S. Batra, "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks," *Discrete Math. Theor. Comput. Sci.*, vol. 17, no. 1, p. 317, 2015.

[62] T. Kerins, W. P. Marnane, E. M. Popovici, and P. Barreto, "Efficient hardware for the tate pairing calculation in characteristic three," in *CHES*, vol. 3659. Berlin, Germany: Springer, 2005, pp. 412–426.

[63] J.-L. Beuchat *et al.*, "FPGA and ASIC implementations of the ETAT pairing in characteristic three," *Comput. Elect. Eng.*, vol. 36, no. 1, pp. 73–87, 2010.

[64] 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.

[65] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[66] M.-H. Park, G.-P. Gwon, S.-W. Seo, and H.-Y. Jeong, "RSU-based distributed key management (RDKM) for secure vehicular multicast communications," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 644–658, Mar. 2011.

[67] Y. Sun, Z. Feng, Q. Hu, and J. Su, "An efficient distributed key management scheme for group-signature based anonymous authentication in VANET," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 79–86, Jan. 2012.

[68] L. Malina, J. Castellà-Roca, A. Vives-Guasch, and J. Hajny, "Short-term linkable group signatures with categorized batch verification," in *Proc. Int. Symp. Found. Pract. Secur.*, 2012, pp. 244–260.

[69] S. K. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generat. Comput. Syst.*, to be published.

[70] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Inf. Sci.*, vol. 387, pp. 165–179, May 2017.

[71] G. P. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 9, pp. 2658–2667, Sep. 2016.

[72] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 24, nos. 1–2, pp. 49–64, 2017.

[73] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," Tech. Univ. München Inst. Für Inf., Munich, Germany, Tech. Rep. TUM-I1343, Apr. 2013.

[74] G. Corser *et al.*, "Privacy-by-decoy: Protecting location privacy against collusion and deanonymization in vehicular location based services," in *Proc. IEEE Intell. Veh. Symp.*, Jun. 2014, pp. 1030–1036.

[75] 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. Depend. Sec. Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016.

[76] A. Riener and J. Reder, "Collective data sharing to improve on driving efficiency and safety," in *Proc. 6th Int. Conf. Autom. User Int. Interaction Veh. Appl. ACM*, 2014, pp. 1–6.

[77] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Trans. ASME, D, J. Basic Eng.*, vol. 82, pp. 35–45, 1960.

[78] P. Konstantinova, A. Udvarev, and T. Semerdjiev, "A study of a target tracking algorithm using global nearest neighbor approach," in *Proc. Int. Conf. Comput. Syst. Technol. (CompSysTech)*, 2003, pp. 5–290.

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

[80] C. Dunbar and G. Qu, "A DTN routing protocol for vehicle location information protection," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Oct. 2014, pp. 94–100.

[81] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, "MixZone in motion: Achieving dynamically cooperative location privacy protection in delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4565–4575, Nov. 2013.

[82] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su, "Mix-zones optimal deployment for protecting location privacy in VANET," *Peer Peer Netw. Appl.*, vol. 8, no. 6, pp. 1108–1121, 2015.

[83] C. A. Ardagna, M. Cremonini, S. D. C. di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," *IEEE Trans. Depend. Sec. Comput.*, vol. 8, no. 1, pp. 13–27, Jan. 2011.

[84] N. Takbiri, A. Houmansadr, D. L. Goeckel, and H. Pishro-Nik, "Limits of location privacy under anonymization and obfuscation," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 764–768.

[85] Y.-C. Wei and Y.-M. Chen, "Efficient self-organized trust management in location privacy enhanced VANETs," in *Proc. Int. Workshop Inf. Secur. Appl.*, 2012, pp. 328–344.

[86] J. Zhang, "Trust management for VANETs: Challenges, desired properties and future directions," *Int. J. Distrib. Syst. Technol.*, vol. 3, no. 1, pp. 48–62, 2012.

[87] S. Eichler, C. Schroth, and J. Eberspächer, "Car-to-car communication," in *Proc. VDE-Kongr., Innov. Eur.*, Aachen, Germany, Oct. 2006.

[88] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, 2nd Quart., 2016.

[89] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. ACM*, 2012, pp. 73–82.

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

[91] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th Int. Conf. IEEE Intell. Netw. Collaborative Syst. (INCoS)*, Sep. 2013, pp. 210–214.

[92] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Comput. Elect. Eng.*, vol. 40, no. 6, pp. 1981–1996, 2014.

[93] O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles," *Comput. Commun.*, vol. 41, pp. 43–54, Mar. 2014.

[94] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Elect. Eng.*, vol. 43, pp. 33–47, Apr. 2015.

[95] S. Yang, J. Li, Z. Liu, and S. Wang, "Managing trust for intelligence vehicles: A cluster consensus approach," in *Proc. Int. Conf. Internet Veh.*, 2015, pp. 210–220.

[96] A. Ltifi, A. Zouinkhi, and M. S. Bouhlel, "Smart trust management for vehicular networks," *World Acad. Sci., Eng. Technol., Int. J. Elect., Comput., Energ., Electron. Commun. Eng.*, vol. 10, no. 8, pp. 1114–1121, 2016.

[97] S. A. Soleymani *et al.*, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 146, 2015.

[98] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.

[99] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012.

[100] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.

[101] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Secur.*, 2013, pp. 94–108.

[102] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer Peer Netw. Appl.*, vol. 7, no. 3, pp. 229–242, 2014.

[103] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc Sensor Wireless Netw.*, vol. 24, nos. 3–4, pp. 283–305, 2015.

[104] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, "A hybrid trust management framework for vehicular social networks," in *Proc. Int. Conf. Comput. Social Netw.*, 2016, pp. 214–225.

[105] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A categorized trust-based message reporting scheme for VANETs," in *Advances in Security of Information and Communication Networks*. Berlin, Germany: Springer, 2013, pp. 65–83.

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

[107] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2010.

[108] N. Elloumi, H. Haj-Salem, and M. Papageorgiou, "Metacor: A macroscopic modeling tool for urban corridors," in *Proc. Triennal Symp. Transp. Anal.*, vol. 1. 1994, pp. 135–150.

[109] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular mobility simulation for VANETs," in *Proc. 40th Annu. IEEE Simulation Symp. (ANSS)*, Mar. 2007, pp. 301–309.

[110] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo—Simulation of urban mobility: An overview," in *Proc. 3rd Int. Conf. Adv. Syst. Simulation SIMUL*, ThinkMind, 2011, pp. 23–28.

[111] S. Krauß, "Microscopic modeling of traffic flow: Investigation of collision free vehicle dynamics," Ph.D. dissertation, Univ. Cologne, Köln, Germany, 1998.

[112] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in NS-2," in *Proc. 10th ACM Symp. Modeling, Anal., Simulation Wireless Mobile Syst.*, 2007, pp. 159–168.

[113] G. F. Riley and T. R. Henderson, "The NS-3 network simulator," *Modeling and Tools for Network Simulation*. Berlin, Germany: Springer, 2010, pp. 15–34.

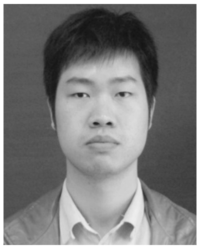
[114] T. R. Andel and A. Yasinsac, "On the credibility of manet simulations," *Computer*, vol. 39, no. 7, pp. 48–54, Jul. 2006.

[115] A. Varga and R. Hornig, "An overview of the OMNET++ simulation environment," in *Proc. 1st Int. Conf. Simulation Tools Techn. Commun., Netw. Syst. Workshops (ICST)*, 2008, p. 60.

[116] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO-simulation of urban mobility," *Int. J. Adv. Syst. Meas.*, vol. 5, nos. 3–4, pp. 128–138, 2012.

[117] M. Piorkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux, "Trans: Realistic joint traffic and network simulator for VANETs," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 12, no. 1, pp. 31–33, 2008.

[118] V. Kumar *et al.*, "iTETRIS: Adaptation of ITS technologies for large scale integrated simulation," in *Proc. 71st. IEEE Veh. Technol. Conf. (VTC-Spring)*, May 2010, pp. 1–5.



Zhaojun Lu received the B.S. degree in electronic science and technology from Huazhong University of Science and Technology, Wuhan, China, in 2013, where he is currently pursuing the Ph.D. degree in microelectronic and solid-state electronics. He is also a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park. His research interests include embedded system security, very large-scale integration design, and vehicular ad hoc network security.

Gang Qu (SM'07) received the B.S. and M.S. degrees in mathematics from University of Science and Technology of China, Hefei, China, in 1992 and 1994, respectively, and the Ph.D. degree in computer science from University of California at Los Angeles, Los Angeles, CA, USA, in 2000. He joined University of Maryland at College Park, College Park, MD, USA, where he is currently a Professor with the Department of Electrical and Computer Engineering and the Institute for Systems Research. He is a member of the Maryland Cybersecurity Center and the Maryland Energy Research Center. He is also the Director of the Maryland Embedded Systems and Hardware Security Laboratory, College Park, and the Wireless Sensors Laboratory.

His primary research interests are in the area of embedded systems and very large-scale integration (VLSI) computer-aided design (CAD) with a focus on low-power system design and hardware-related security and trust. He studies optimization and combinatorial problems and applies his theoretical discovery to applications in VLSI CAD, wireless sensor network, bioinformatics, and cybersecurity. He has received many awards for his academic achievements, teaching, and service to the research community. He serves as an Associate Editor of IEEE EMBEDDED SYSTEMS LETTERS and *Integration, the VLSI Journal*.

Zhenglin Liu received the Ph.D. degree from the Department of Electronic Science and Technology, Huazhong University of Science and Technology, Wuhan, China, in 2001. He is currently a Professor with the School of Optical and Electronic Information, Huazhong University of Science and Technology. His main research interests include embedded system security and very large-scale integration design.