A Security and Privacy Review of VANETs

Fengzhong Qu, *Senior Member, IEEE*, Zhihui Wu, Fei-Yue Wang, *Fellow, IEEE*, and Woong Cho, *Member, IEEE*

***Abstract*—Vehicular ad hoc networks (VANETs) have stimulated interest in both academic and industry settings because, once deployed, they would bring a new driving experience to drivers. However, communicating in an open-access environment makes security and privacy issues a real challenge, which may affect the large-scale deployment of VANETs. Researchers have proposed many solutions to these issues. We start this paper by providing background information of VANETs and classifying security threats that challenge VANETs. After clarifying the requirements that the proposed solutions to security and privacy problems in VANETs should meet, on the one hand, we present the general secure process and point out authentication methods involved in these processes. Detailed survey of these authentication algorithms followed by discussions comes afterward. On the other hand, privacy preserving methods are reviewed, and the tradeoff between security and privacy is discussed. Finally, we provide an outlook on how to detect and revoke malicious nodes more efficiently and challenges that have yet been solved.**

***Index Terms*—VANETs, security, privacy, survey.**

I. Introduction

VEHICULAR ad hoc networks (VANETs) are distributed, self-organized networks built up by many high-speed vehicles. All vehicles in the network would install onboard units (OBU), which would integrate the vehicles' wireless communications, micro-sensors, embedded systems, and Global Positioning System (GPS) [1]. These smart vehicles could then communicate with each other as well as with roadside units (RSU), such as traffic lights or traffic signs, which would then improve the driving experience and make driving safer [2]–[4]. For example, vehicles could exchange messages concerning real-time traffic conditions so that drivers would be more aware of their driving environment and take early action in response to an unusual situation [5].

Despite these advantages, VANETs come with their own set of challenges, particularly in the aspects of security and privacy. Lack of authenticated information shared in the network may lead to malicious attacks and service abuses, which could pose great threats to drivers [6], [7]. In addition, unlike traditional wired networks which are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks could come from various sources and target all nodes [8], [9]. Furthermore, VANETs are an example of mobile ad hoc networks (MANETs) [7], which means they not only inherit all the known and unknown security weaknesses associated with MANETs [10], but due to the unique features of these types of networks, such as the high mobility of the nodes and the large scale of the network, VANETs are more challenging [5], [11]. Therefore, a novel mechanism to guarantee the primary security requirements, such as authentication, integrity, and nonrepudiation needs to be developed before VANETs can be practically launched [12].

However, authentication in this mobile environment poses a privacy risk to the users. During authentication, the network can be aware of the whereabouts of a specific user at a specific time [6], [13]. Malicious vehicles could trace the targeted driver's activities based on the information provided for authentication. Hubaux *et al.* [14] tried to address these privacy problems by using anonymity schemes and, relying on temporary pseudonyms. However, with these privacy preserving proposals [15], [16], malicious vehicles could still be anonymous, which would make it difficult for the trusted authority, such as vehicle administration office, to track the malicious vehicles and revoke their access. To overcome these problems, the concept of conditional privacy preservation was proposed. Lin *et al.* [17] introduced a secure and conditional privacy preserving protocol for VANETs by integrating the techniques of group signature and identity-based signature. The authorities were able to reveal the real identities of malicious vehicles and update the certificate revocation list accordingly. However, these mechanisms fell short since they required a vast amount of storage space for anonymous keys and safety message anonymous authentication. Although researchers came up with ideas to address this problem [18], [19], most of the schemes relied heavily on tamper-proof devices (TPDs), which if attacked and cracked, the whole system would be compromised. Recently, Horng *et al.* [20] provided a software-based solution to reduce verification time and alleviate the computational workload of RSUs, which will be described in more detail in Section III.

From previous parts we could see that, to enlighten the readers, we should first familiarize them with the background knowledge of VANETs such as the requirements, challenges, types of attackers involved in security and privacy preserving solutions. After the goals of the solutions are explicit to readers, technologies involved are categorized and their advantages and disadvantages are discussed to provide some ideas for researchers when they try to optimize their algorithms. Further, we provide an outlook on how to detect and revoke malicious

Manuscript received July 20, 2014; revised December 5, 2014 and April 27, 2015; accepted May 20, 2015. Date of publication June 17, 2015; date of current version November 23, 2015. This work was in part supported by the National Natural Science Foundation of China under Grants 61001067, 61172105, and 61371093, by SKLMCCS through the Open Research Project under Grant 20120107, and by the Ministry of Transport under Project 2012-364-X03-104. The Associate Editor for this paper was X. Cheng.

F. Qu and Z. Wu is with the Ocean College, Zhejiang University, Hangzhou 310058, China (e-mail: jimquf@zju.edu.cn).

F.-Y. Wang is with the Institute of Automation Chinese Academy of Sciences, Beijing 100190, China.

W. Cho is with the Department of Computer System Engineering in Jungwon University, Goesan 367-805, Korea.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2015.2439292

nodes more efficiently and challenges that have yet been solved. In summary, our paper could provide a framework for future research. Many surveys about VANETs have been written. Richard *et al.* [21] summarized channel characteristics and challenges in VANETs and then presented solutions to security and privacy problems respectively. We give supplementary information in the part of solutions proposed to ensure security by categorizing algorithms of digital signature involved in various security models and analyzing several models, including their modifications of the original algorithms and effects, in the same category. The part of solutions to ensure privacy in our paper is organized by presenting three commonly used anonymous authentication methods. We also point out problems that still exist to be solved in both parts. Shidrokh *et al.* [22] reviewed a sufficient number of articles to obtain the threats, challenges and security models in VANETs. The paper presented security models chronologically in a table. Since the deployment of VANETs in reality needs to ensure security, in the meanwhile, preserve the driver's privacy, we consider privacy issues along with security problems in VANETs. Ghassan *et al.* [23] summarized solutions to the security problems using VPKI (Vehicular Public Key Infrastructure) and analyzed the advantages and disadvantages of these methods. However, the models and references the paper introduced were not sufficient. Furthermore, they failed to address VANET privacy issues either. Saif *et al.* [24] provided a comprehensive survey about VANETs, which encompassed the network architecture, wireless access technologies, security challenges and simulation tools. This survey gave an overview of VANETs but did not focus on security and privacy issues.

Unlike these surveys, we not only analyze the security and conditional privacy preserving models based on 114 related articles published between 2004 and 2014, we present these models in a clear and extensive design: we first introduce the basic ideas of most of the security models and point out the parts that will be different. Then, we classify the security models according to the cryptography algorithms involved. Furthermore, we discuss the tradeoff between security and privacy in VANETs, while emphasizing a compromise in devising a security scheme.

The rest of paper is organized in the following way: Section II presents the threats, challenges and requirements of VANETs, Section III introduces the basic ideas and technologies involved in existing security models from 2004–2014 publications, Section IV presents the privacy issues and existing solutions, Section V discusses the tradeoff between security and privacy, and Section VI concludes the review.

II. Threats, Challenges, and Requirements in VANETs

In this section, we first define the types of attackers. It is important because different types may need different methods to avoid their malicious attacks. Then we clarify the requirements that the security and privacy preserving protocols should meet. The more and more stringent requirements proposed by the complicated real life situation represent one of the driving forces that motivate researchers to come up with new methods.

The U.S. Federal Communications Commission (FCC) has allocated 75 MHz of Dedicated Short-Range Communications (DSRC) spectrum at 5.9 GHz to be used for V2V and V2R communications [25]. DSRC is a wireless protocol which allows data to be easily monitored, altered and forged, including sensitive data information concerning the drivers' privacy [26]. Therefore, how to secure information exchanged in VANETs and keep the user' privacy have become two big challenges which set back the large scale deployment of VANETs. Researchers have been dedicated to solving these problems, and many novel models have been proposed. Before investigating the security models of VANETs, we should first identify the threats and requirements of security.

A. Threats

Raya *et al.* [27] categorized attackers into four basic types: outsiders versus insiders, malicious versus rational, active versus passive, and local versus extended. Outsiders differ from insiders in the aspect of network authentications. Outsiders are not authenticated while insiders are. Malicious attackers differ from rational attackers in the aspect of intentions. Malicious attackers cause accidents just for fun, while rational attackers do so for specific purposes. Active attackers differ from passive attackers in the aspect of behaviors. Active attackers send fake or modified messages to other vehicles, while passive attackers only monitor the network and eavesdrop on communications between other nodes to collect useful information for future attacks. Local attackers differ from extended attackers in the aspect of the scope the attackers could control. Local attackers only perpetrate attacks in a limited range while extended attackers attack across the network.

We will now provide a general classification of attacks. The basic types of attacks adversaries could perpetrate are briefly summarized in Table I and detail descriptions are as follows:

a) Bogus information: This attack happens when information sent by the adversaries, including certificates, warnings, security messages, and identities [23], is not true. The adversaries may alter or even fake data, or send data captured earlier in time, to confuse other drivers. For example, a sybil attack [28], [29], an attack that happens when the adversaries create a large number of pseudonymous, and acts like they are more than a hundred vehicles, may tell other vehicles that there is traffic jam ahead, and force them to take alternate routes, even though there is no traffic jam.

b) Denial of service: This attack happens when adversaries send irrelevant bulk messages in order to jam the communication channel used in VANETs and consume the computational resources of the other nodes [17]. The goal behind this kind of attack is to bring the network down, consequently rendering the VANET unavailable [21], which could have fatal consequences to drivers if an emergency occurred.

c) Impersonate: This attack happens when the adversaries pretend to be authenticated vehicles or RSUs [30]. The adversaries use the legitimate identities they hacked into to insert malicious information in the network, which would

TABLE I
BASIC TYPES OF ATTACKS IN VANETS

Types	Descriptions	Purposes
Bogus information	Adversaries alter or fake data and distribute the false information in the network.	To disturb public order and fool other drivers for specific illegal purposes.
Denial of service	Adversaries insert irrelevant bulk messages to VANETs.	To jam the communication channel and consume the computational resources of the other nodes, consequently rendering the VANET unavailable.
Impersonate	Adversaries pretend to be legitimate nodes, like authenticated RSUs or vehicles.	To insert malicious information in the network, which would not only fool other vehicles but also make the innocent drivers whose identifies were taken be removed from the network and denied service.
Eavesdropping	Adversaries are located in vehicles or false RSUs.	To collect vehicle-specific information from overheard vehicular communications.
Message suspension	Adversaries hold onto messages before sending them.	To prevent registration and insurance authorities from learning about collisions involving the attackers vehicle and/or to avoid delivering collision reports to roadside access points.
Hardware tampering	Adversaries manipulate on board hardware in vehicles and RSUs.	To disturb public order for illegal purposes.

not only fool other vehicles but also make the innocent drivers whose identities were taken be removed from the network and denied service.

d) Eavesdropping: This attack happens when an attacker is located in a vehicle, be it stopped or moving, or in a false RSU [21].The collection of vehicle-specific information from overheard vehicular communications is easy in a wireless network. The attackers obtain the target vehicles' confidential data, including the drivers real identities, their preferences or even their credit card codes, which seriously violates the privacy of the drivers.
e) Message suspension: This attack happens when adversaries hold onto messages before sending them. An attacker selectively drop packets of messages from the network, which may hold critical information for the intended receiver, and the attacker suppresses these packets and can use them again in the future. One goal of such an attack would be to prevent registration and insurance authorities from learning about collisions involving the attacker's vehicle and/or to avoid delivering collision reports to roadside access points.
f) Hardware tampering: This attack happens when the sensors, other on board hardware RSUs [31] are manipulated by adversaries. For example, an adversary can relocate a tampered RSU to launch a malicious attack, such as tampering the traffic lights to always be green when the malicious attack is approaching an intersection.

B. Requirements

Jean *et al.* [14] discussed the security and privacy issues in VANETs, and pointed out that the primary requirements to secure VANETs were: message integrity, source authentication and vehicle anonymity. Sha *et al.* [15] presented scalability as a further supplement to these requirements. Given that drivers should be informed of emergencies as early as possible, since the driver who receives a warning message must have sufficient time to react, time constraints were also suggested as requirement [32], [33]. In the past few years, considerable research effort has been made into VANET security protocols. In summary, the primary requirements for security in VANETs are as follows:

a) Integrated messages as well as efficiently authenticated sources: First, the senders of broadcast messages should be authenticated as legitimate nodes, which could efficiently prevent outsider attacks [34]. Secondly, messages collected should be consistent with the raw data from the road, which would mean that information shared in the VANETs is not maliciously fabricated, and is instead unmodified and consistent with similar data generated in close space and time. Furthermore, since authentication needs to be performed before data can be collected and the service delivered, the latency of authentication should be as short as possible [35], [36].
b) Confidentiality and non-repudiation: Confidentiality in VANETs protects the confidential information of drivers, such as their real identity. All sensitive information should be encrypted and not available to adversaries. However, confidentiality is conditional. For those malicious adversaries, privacy could be revoked and their real identities would be broadcast to all the vehicles in VANETs. Furthermore, a sender should not be able to deny the transmission of a message. One of the applications of VANETs is tracking the responsible car in case of an accident. It may be crucial for an accident investigation to determine the correct sequence and content of messages exchanged before an accident to determine the fault and the cause.
c) Availability and scalability: Communication in VANETs should be supported by alternative means when the communication channel breaks down. During traffic congestion, there may be a large number of authentication requests delivered to the authentication server. The network may then be brought down, and to ensure the ongoing communication between vehicles and vehicles to infrastructures, an alternative channel should be provided.

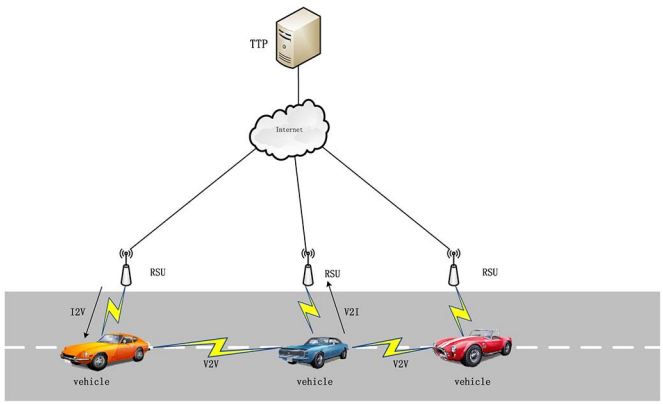

Fig. 1. System architecture in VANETs.

III. Basic Ideas and Solutions to Security Issues

Many solutions have been proposed in the literature to address the security problems of VANETs. Some mechanisms propose a solution for one or more of the security requirements. In this section, we first introduce the security architecture which serves as the basic block of solution models, and then explain the general secure process in Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication scenarios respectively, and point out technologies involved in these processes. After the processes are clear to readers, readers could have the concept of authentication and know the function of authentication algorithms. Thus, in the following part, we further analyze in details these algorithms, including their classifications, advantages and disadvantages and modifications of the original algorithms to fit the security requirements in VANETs. We then present several solutions which combined two or more specific algorithms to meet higher security level.

A. Security Architecture

The VANETs consist of three components (see Fig. 1): a trusted third party, roadside infrastructures, and vehicles [37]–[40].

a) Trusted third party: a trusted third party (TTP), which refers to a trusted administration with sufficient computational and storage resources where all vehicles register and get their certificates for VANET usage, is responsible to hold the credentials and the identities of vehicles and to reveal the real identities of nodes whose certifications have been revoked. In addition, they are also in charge of RSUs. TTPs are fully trusted by all entities [42]. In reality, a large number of TTPs exist and each one of them is responsible for a specific geographical region. Each vehicle and RSU should be registered with exactly one TTP.

b) Roadside units: RSUs are infrastructures fixed on the roadside, which are fully controlled by TTPs. RSUs are quite vulnerable because they are easily exposed to attackers, so we must put minimal trust in RSUs. For enhanced security, RSUs could directly communicate with TTP and if TTP considers that a specific RSU has been compromised, it could revoke the RSU's access.

Fig. 2. The format of messages delivered in V2V scenario.

c) Vehicles: Vehicles are the moving nodes in the network, which are loaded with an OBU and a tamper-proof device. The OBU is used to enable vehicles to wirelessly communicate with each other and RSUs, and the TPD is used to store cryptographic materials, such as an Electronic License Plate (ELP) that is installed on every new vehicle and provides a unique ID number, and process cryptographic operations. TPD is a good second defense layer but should not be exclusively relied upon.

B. Basic Ideas

Though various schemes have been proposed, the basic ideas in securing VANETs have many similarities. In VANETs, communication can be divided into two scenarios: vehicle-to-vehicle communication and vehicle-to-infrastructure communication. In both scenarios, the first step is for vehicles to physically provide the required identity information, including their ELPs, drivers' identities, home addresses, etc., to the TTP as part of the registration process. The registration of each vehicle in TTP is necessary because the service is only to be provided to valid clients and is the initial protection step. TTP then assigns the private and public key pairs, along with the vehicle's certificate, to each vehicle with a valid identity. This procedure involves the generation of key pairs, which usually utilizes digital signature algorithms (algorithms will be detailed in the next part. This process may differ across models, since some models propose employing RSU-aided message authentication schemes [43]–[45]. In these schemes, vehicles get their authentications from nearby RSUs instead of TTP.

In V2V communication scenario, vehicles could communicate with each other when in a wireless range or in a multi-hop mode, exchanging road condition information such as emergencies, accidents or congestions [46], [47]. Before sending a message, a vehicle should first digitally sign the message to avoid being exposed directly to attackers while simultaneously helping protect their privacy. This procedure involves digital signature schemes that will be analyzed in detail in next part. The format of a message is defined by the researchers in the reviewed papers, but some critical elements should always be included, such as the vehicle's signature and/or certificates, message payload and timestamp (see Fig. 2). In [17], the message periodically broadcast by the OBU encompasses five components: group ID, message payload, timestamp, OBU's signature and valid time. Group ID is used to identify to which group the individual vehicle belongs to. The message payload is traffic-related messages, such as speed, direction, position, current time, brake status, steering angle, acceleration or deceleration, traffic conditions, traffic events, etc., which could help other drivers be aware of the road condition and take early actions to respond to an emergency. Timestamp is used to prevent the message replay attack. OBU's signature is used to help others validate the integrity of the message. Valid time

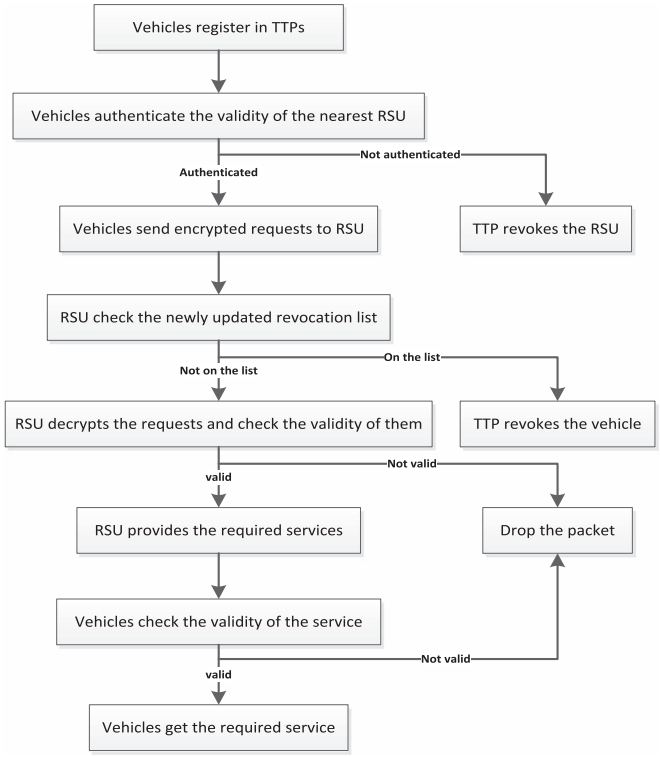

Fig. 3. The process of vehicles requiring services from the nearest RSU.

is defined as the time the message would be last in VANETs. Once the message is received, the receiving vehicle should first verify the validity of the message by checking the signatures of the safety message, in order to ensure that the message is sent by valid vehicles and is not altered during transmission. This procedure involves the verification techniques.

In V2I scenarios, vehicles send requests to the nearest RSU when the vehicles want to get access to services provided by the RSU, such as Internet service or, information about the nearest restaurant. Fig. 3 presented the process of vehicles requiring services from the nearest RSU. In many schemes [48], [49], vehicles should first authenticate themselves with RSU to get permission to allow them to broadcast messages. When a vehicle passes by the RSU, it should also authenticate the validity of the RSU in case it is a fake RSU. Once the RSU is authenticated, the vehicle sends the encrypted request messages and its certificate to the RSU. The RSU decrypts the request and then looks up the newly updated revocation list retrieved from TTP to check whether the vehicle is entitled to obtain the service. If the certificate is on the revocation list, the RSU rejects the request, otherwise the vehicle is authenticated. If the vehicle is authenticated, the RSU sends the response back to the vehicle and provide the service request. The vehicle should also check the validity of response after receiving it. Note that, the certificate revocation list (CRL) is a commonly used scheme to revoke the access of malicious nodes. The IEEE 1609.2 standard [50] states that VANETs will depend on such certificate revocation lists to ensure revocation of these nodes to VANETs. However, CRL has a significant drawback [51]–[53]. Specifically the list becomes increasingly larger with the increasing number of revoked nodes, and therefore the storage needs increase and the time delay to check the list increases. Furthermore, the timely distribution of the CRL is also a challenge. Thus, various alternative key revocation schemes and CRL dissemination schemes have been devised [54]–[57].

Raya *et al.* [58] devised compressed CRLs using bloom filters, which are also used in [59] in common scenarios to dramatically reduce storage requirements, to revoke TPD's access when all certificates of a given vehicle need to be revoked and to distribute revocation protocol for a temporary revocation of an attacker. Kenneth *et al.* [60] proposed incremental updates to a CRL and an epidemic fashion propagation scheme, where the TTP distributes the newly update CRL to a small number of RSUs in high vehicle density locations and the RSU then infects each passing vehicle with the CRL update. Each infected vehicle then infects every vehicle it encounters. Papadimitratos *et al.* [16] took advantage of the regional TTPs' setup to decrease the size of the CRLs. Regional TTPs will only manage the certificates of vehicles in their region. The scheme Wang *et al.* presented in [61] utilized TPDs to revoke vehicles, which release vehicles from maintaining a huge CRL to record the revoked vehicles. When the TTP wants to revoke a node Vi, it broadcasts the node's original pseudo-identity. Once Vi receives the pseudo-identity, the TPD of Vi deletes all the cryptographic material stored on the TPD to make the TPD invalid. As a result, Vi's access is revoked and it can no longer generate traffic messages.

C. Technologies for Security Improvement

Authentication is a cryptographic primitive process that allows the receiver of a message to ascertain that the contents of a message were not modified during transmission, and to determine the source of the message. An authentication scheme fails if it fails to detect adversaries pretending to be another entity or modifying messages sent by others. In order to achieve broadcast authentication in VANETs, the use of a public key infrastructure (PKI) is commonly adopted, including by IEEE1609.2. A PKI uses a public and a private cryptographic key pair to secure the exchange data in the network. However, conventional PKI cannot satisfy the requirements of VANETs, as it cannot preserve conditional privacy of drivers and the verification time is too long.

Digital signature is a common way to enhance the security of VANETs based on PKI. Digital signature schemes are designed to provide the electronic counterpart to handwritten signatures, to ensure the origin authenticity, the integrity and non-repudiation of messages. Digital signatures are easily transportable, cannot be imitated, and can be automatically time-stamped. A digital signature scheme typically is compromised of three functions: a) generating public and private key pairs, b) ensuring confidentiality by encrypting and decrypting messages, and c) ensuring authenticity by creating and verifying the signature. However, one digital signature scheme on its own would not satisfy all the requirements in VANETs, such as short verification time and light computation overhead. Thus, security schemes usually involve more than one digital signature algorithm, which would be explained in detail in what follows in this section.

Digital signatures could be implemented by various algorithms. The choice of algorithms in VANETs should be based

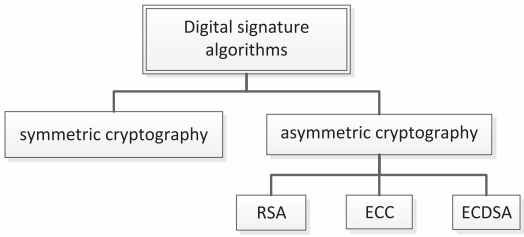

Fig. 4. Algorithms of digital signature.

on two principles: a) rapid execution speed of the signature generation and verification operations, and b) small size of the key, signature, and certificate. Algorithms could then be categorized into two classes: symmetric cryptography and asymmetric cryptography (see Fig. 4).

Symmetric cryptography, which is also known as private-key cryptography, uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. Xi *et al.* [6] proposed the symmetric random key-set approach to reduce OBU's overhead. In their scheme, symmetric random key-sets are sets of symmetric keys drawn from a shared key pool and one key is shared by a set of members. The key set is installed in the TPD when the vehicle registers with the TTP. However, symmetric cryptography has the main drawback of not being able to ensure non-repudiation. Thus, despite the simple algorithm of symmetric cryptography, researchers seldom adopt symmetric cryptography on its own.

Asymmetric cryptography, which is also known as public-key cryptography, uses a pair of keys (public and private key pairs) to encrypt and decrypt a message to ensure data security. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature. The public key and private key are mathematically linked. Identity-based cryptography (IBC) is a type of asymmetric cryptography, and identity-based signature is based on this type of cryptography. The biggest advantage of identity-based signature is that the public key of an entity could be derived from its public identity information, such as name, e-mail address, etc, which avoids the use of certificates for public key verification in the conventional PKI scheme. Most existing algorithms of IBC are based on the bilinear pairing in a pairing domain where the Discrete Logarithm Problem (DLP) for pairing in groups is difficult. Pairing-based cryptography is pairing elements of two cryptographic groups to a third group to therefore construct cryptographic systems, which is beyond scope of this review and we will not describe this pairing theory. Several researchers have proposed security solutions using IBCs. Li *et al.* [62] proposed a scheme that uses identity based signature to authenticate V2I and I2V communication. Sun *et al.* [63] proposed a scheme that uses identity based encryption for encryption, authentication and nonrepudiation. Considering that the IBC infrastructure avoids the use of certificates for public key verification and the exchange of public keys, this greatly improves the computation and communication efficiency. Furthermore, Li *et al.* [8] proposed a non-interactive ID-based scheme which uses members'identities to establish a secure trust relationship in V2V communication.

RSA, Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA) are three commonly adopted asymmetric algorithms. In RSA, the public key contains a large non-prime number, the RSA modulus, which is chosen as the product of two large primes. The security of RSA is based on the difficulty of the integer factorization problem. The size of an RSA key refers to the bit-length of the RSA modulus [64]. Due to the efficiency of RSA, the generation of key pairs and the public-key based pseudonym in the current public key in [62] was implemented by an RSA algorithm.

ECC is an approach based on the algebraic structure of elliptic curves over finite fields [65]. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplication given the original and product points. ECC algorithm has the advantage of providing much shorter key sizes and system parameters than RSA. Huang *et al.* [18] proposed a scheme inspired by the concept of batch verification to simultaneously authenticate multiple requests sent from different vehicles using ECC. In the scheme, the TPD is responsible in generating pseudo identity and corresponding private key based on ECC using the system parameters issued by the TTP. However, the size of digital signatures is typically very large, which would greatly affect the authentication and verification efficiency.

ECDSA is the elliptic curve analog of the digital signature algorithm (DSA) [64]. IEEE 1609.2 [50] proposed the use of ECDSA to verify messages [66]. Ahren *et al.* [67] used a combination of TESLA++ and ECDSA based digital signature scheme to ensure security in VANETs. The sender broadcasts an authenticated message and receivers perform two types of verification: a TESLA++ verification, as well as a digital signature verification when the application requires non-repudiation. In addition to the commonly used aforementioned signature algorithms, Sun *et al.* [68] proposed an efficient pseudonymous authentication scheme based on hash chains, bilinear parings [69]–[71] and the Schnorr signature algorithm. The Schnorr signature algorithm is used when the TTP generates a signature.

Compared with symmetric cryptography, asymmetric cryptography is slower because of the complexity of its algorithm. However, as stated previously, symmetric cryptography has the problem that if the key is discovered or intercepted by others, messages can easily be decrypted. Therefore, asymmetric cryptography is more likely to be used to enhance security regardless of its computation overhead. However, symmetric cryptography is still utilized in some models as an assistant to asymmetric cryptography. Specifically, in [72], researchers proposed a mechanism denoted as TESLA [73], which uses symmetric cryptography, delay key disclosure and time synchronization to provide the necessary asymmetry for broadcast authentication [67]. Applying TESLA to VANETs could reduce the overhead associated with authentication. Burmester *et al.* [74] proposed another hybrid scheme, which employed symmetric and public key operations to authenticate messages and use pseudonyms to enhance privacy. Klaus *et al.* [75] also devised a hybrid scheme, which used asymmetric cryptography to secure messages involved in road safety while other messages such as the periodically broadcast telematic messages, are protected using symmetric cryptography.

As stated previously, a single digital signature scheme would not satisfy the requirements in VANETs, such as non-repudiation, short verification time, and light computation overhead. Li *et al.* [8] proposed a non-interactive ID-based scheme which uses member' identities to establish a secure trust relationship between communicating vehicles, and uses a blind signature-based scheme for vehicle-to-roadside device communication, allowing authorized vehicles to anonymously interact with RSUs. This scheme has minimum storage needs because the service provider does not need to maintain authorized credentials per user. Li *et al.* [62] proposed a different scheme that utilized RSA, because of its rapid computational rate, to generate each vehicle's pseudonyms. In this scheme the generation of pseudonyms does not affect the efficiency of authentication during communication, employs ECC-based ID-based online/offline signatures in intervehicle communication and uses ECC-based signature to further reduce the computation overhead. Together, this speeds up the authentication process and identity-based signature in vehicle-to roadside communication. A further proposal by Lin *et al.* [17] used group signature to secure the communication between vehicles, where messages can anonymously be signed by the sender and their real identity only available to authorities. In this scheme, RSUs could digitally sign each message launched by the RSUs using an identity based signature, which would greatly reduce signature overhead.

Signature verification is likely to be used much more often than signature generation, as certificates and signed documents are circulated over networks. To further enhance the efficiency of signature verification, batch verification is a commonly adopted scheme [76]. Batch verification significantly increase the speed of signature verification and alleviates the computational workload of the RSUs by authenticating multiple signatures at the same time rather than one by one. Zhang *et al.* [12] employed an identity-based batch verification (IBV) scheme for communications between vehicles and RSUs. The IBV scheme enhances the system's performance by allowing RSUs to verify a large number of messages at once instead of verifying them one by one. However, the proposed scheme relies heavily on TPDs and furthermore, if one signature is inaccurate, the whole batch will be dropped, which is very inefficient. Another batch verification method was proposed by Horng *et al.* [20]. The authors proposed a software-based solution to satisfy the security and privacy requirements in VANETs. Several other papers also detail schemes using batch verification to meet the stringent verification requirements of VANETs [45], [76], [77]. By using batch verification, lower message overhead and higher success rates would be achieved in VANETs.

Considering the privacy requirements in VANETs, conventional digital signatures may not protect the drivers' privacy because other nodes could discover the identity of the message sender. Therefore, anonymous digital signature has been proposed. Anonymous digital signature is a special type of digital signature [79], [78]. In an anonymous digital signature scheme, given a digital signature, an unauthorized entity, cannot determine the signer's identifier. An anonymous signature using a group public key is commonly known as a group signature [80], [81]. Valid group members could anonymously sign an arbitrary number of messages on behalf of the group, and it would then be computationally difficult to identify the actual sender by anyone other than the group manager. There are also many other signature schemes used in securing VANETs, such as blind signature and ID-based signature. Different signature schemes are employed based on different requirements. Furthermore, combining digital signature with hash function and message authentication codes could enhance the security level in VANETs and help mitigate specific types of attacks. For example, Karlof *et al.* proposed the use of distillation codes to mitigate computational DoS attacks in broadcast authentication where malicious parties insert spurious data in an attempt to interfere with error correction. Additionally, Li *et al.* [8] employed a one-way hash chain [68], [82] to enhance efficiency in computation. In summary, solutions to security problems in VANETs tend to use digital signatures as a basic solution.

IV. Privacy Preserving Solutions

Keep the privacy of authenticated users is another aspect to be considered along with security problems. The major principle is to make authentication process anonymous. In this section, we present two commonly used anonymous authentication methods and analyze several proposed solutions utilized these methods to achieve privacy. Problems remain to be solved are also discussed.

In both wired and wireless networks, privacy has always been a key concern, and many researchers have devoted decades of work to tackling this problem. Even so, while the level of privacy could be enhanced, the most ideal situation where the users' information could never be traced, may never come to fruition. Given the large scale and frequent usage of the Internet and cellular networks, small little flaws in the aspect of privacy seem to be acceptable. Still, privacy is a decisive factor in the public's acceptance of and the commercial deployment of VANETs [22]. Leaking drivers' private profiles could lead to serious consequences. For example, location tracking of any vehicle provides access to past and current locations of the vehicle [83]. Once the location history has been accumulated, adversaries could infer the driver's personal interests and daily routine by combining these data with additional information. The information could then be misused for crimes, such as abductions or automobile thefts.

Security has been one of the most challenging problems in VANETs and should be considered along with privacy. To secure the communication in VANETs, the data must be authenticated. Through authentication, the network can be aware of the precise location of a specific user at a specific time, which ensures that the TTP could intervene in the vehicle when an issue arises. For example, when a vehicle has an accident on the road and leaves the scene, the TTP could reveal the real identity of the vehicle and track it until the police were able to catch up with the responsible vehicle. However, some drivers are not willing to let the TTP have access to their confidential information. Therefore, how to preserve privacy while still enabling authentication has become one of the main challenges of implementing VANETs [6]. The tradeoff between security and privacy will be explained in detail in Section V.

Anonymous authentication is a very active topic for securing VANETs and can be roughly divided into three categories namely, the group-signature-based schemes, pseudonymous authentication schemes, and hybrids schemes. Another privacy-related study in VANETs focused on strengthening the location privacy of drivers [68]. Users' privacy mainly refer to their identity privacy and location privacy. The basic ideas of the schemes are to use group signature and pseudonymous authentication to hide the vehicles' real identity to adversaries and not allow them to be traced. Group-signature-based schemes achieve these goals by permitting valid group members to anonymously sign an arbitrary number of messages on behalf of the group, which is then computationally difficult to identify the actual sender by anyone but group manager. Lin *et al.* [17] proposed a conditional privacy-preserving protocol for VANETs. This paper utilized short group signature to sign the messages sent by vehicles, which provides anonymity of the signers and could meet the anonymity and traceability requirements of VANETs implementation. But the group signature verification is usually time consuming, which make it unsuitable for some time-stringent VANET applications. In [17], the time to verify the safety message grew linearly with the number of revoked nodes in the revocation list, which led to more time being consumed when the revocation list grew even larger. Based on this observation, the efficient conditional privacy preservation protocol was devised by Lu *et al.* [45]. When a vehicle passes by an RSU, it asks the RSU for a short-time anonymous key certificate, which would be constructed by employing group signature based on bilinear pairing. The vehicle could then broadcast messages within the valid time defined in the messages, so it would then become unnecessary for the vehicles to have a copy of the CRL. Note that the identity-based signature is used in the process of the verification, which reduces the storage overhead and verification time. But there is no efficient revocation scheme in ECPP.

Pseudonymous authentication schemes achieve privacy preserving by frequently changing the pseudonyms and having random silent periods [84]. How to generate such a large number of pseudonyms and what triggers the pseudonyms updates, has raised the attention of many researchers. The methods to provide each vehicle with continuously changing pseudonyms could be summarized as follows:

a) Preload pseudonyms in TPDs: preloading each vehicle with multiple pseudonyms/certificates obtained from the TTP is useful, since signing different messages with different keys makes it difficult for an attacker to link these messages to one particular vehicle. Raya *et al.* [27] proposed preloading anonymous keys, the TTP's public key and the electronic license plate on the vehicle. A vehicle should then change its anonymous key after having used it to sign message for the time period of one minute, and each vehicle should be preloaded with 43800 anonymous keys per year. Sun *et al.* proposed a different prestored strategy, where each vehicle could obtain a large set of pseudonymous certificates from the TTP during the vehicle's inspection. However, we could infer that these mechanisms are far from efficient, because each vehicle would need a large storage capacity to store the certificates, and once a malicious node is detected, the authority would have to exhaustively search a large database to find the ID related to the misbehaving anonymous public key.
b) Getting pseudonyms with the assistance of RSUs: When a vehicle is new in the network, or its pseudonym has expired, it could send a request to the RSU for a Short Time Pseudonym (STP), thus avoiding the overhead and delay caused by OBU pseudonyms storage management. Zhang *et al.* [43] proposed an RSU-aided message authentication scheme. A vehicle contacts the nearest RSU to get the symmetric secret key and pseudo ID. Note that the pseudo ID is shared with several vehicles so that the route of a specific vehicle cannot be traced. In the meantime, the RSU could still identify a specific vehicle by finding the symmetric key shared with the vehicle. However, the scheme requires frequent pseudonym requests between a node and the RSU, and considering the limited wireless channel bandwidth, it is inefficient and difficult for an RSU to transmit hundreds of certificates for each passing vehicle while providing infotainment dissemination services at the same time, especially when the vehicle density is high.
c) Generating pseudonyms by vehicles: Huang *et al.* [78] devised a pseudonymous authentication with a conditional privacy scheme, which does not need to preload numerous pseudonym certificates in the TPD or provide identity certificates to the RSU. The vehicle instead uses the ticket issued by TTP to authenticate itself with the RSU and obtains a pseudonym tokens. Then the vehicle could generate its pseudonyms with the token. This process would utilize the BLS short signature schemes.

Although the pseudonym mechanism theoretically can ensure that the relationship between a pseudonym and the vehicle's real identity would not be revealed, however, an attacker could still learn the true identity of the node by analyzing the log information. Thus, changing the pseudonyms with some frequency has been proposed. Ideally, a vehicle would switch its pseudonym after every message; however this is not plausible, as the set of stored pseudonyms would be quickly exhausted. Frequently changing pseudonyms, along with random silent period, therefore becomes a way to enhance the reliability of the pseudonym implementation. Random silent period means a time period during which a vehicle does not do any operation requiring VANETs, then replaces its pseudonym. When the silence ends, the vehicle will carry out activities with a new pseudonym. In this case, random has two meanings: the duration of silence is random and the quiet time is also random. Thus, the appropriate condition to change pseudonyms needs to be well designed. Brijesh *et al.* [85] proposed a privacy sustaining strategy based on an appropriate pseudonym update. They found that time and place for pseudonym updates are affected by several factors: the amount of neighborhood traffic, the rate of neighborhood traffic change and the capabilities of the adversaries.

V. The Tradeoff Between Security and Privacy

In this section, the tradeoff between security and privacy is discussed because how to keep a balance when security and privacy cannot be met satisfactorily at the same time is an important topic for discussion.

The tradeoff between security and privacy in VANETs should be discussed in regard to 3 aspects:

First, authentication used to secure VANETs may pose a privacy risk to the users. Through authentication, the network is aware of the precise location of a specific user at a specific time to ensure that the TTP could intervene in the vehicle when an issue arises. However, some drivers may not want to be monitored by the TTP since it would seem to violate their privacy.

Secondly, many privacy preserving protocols enhance the level of privacy in the cost of safety. For example, researchers utilize random silent period to achieve unlinkabililty. However, traditional safety message broadcast period of hundreds of milliseconds cannot assure unlinkability. An increase in the random silent period enlarges the safety message period, and the resulting location privacy is obtained at the cost of safety [83].

Thirdly, CRL is the traditional way to revoke malicious nodes, and requires a large storage space due to the scale of VANETs. Researchers have proposed many other revocation mechanisms, which take advantage of caching strategies combined with hashing techniques to enhance the availability of the revocation service. However, the process of checking the certificate status would be more likely to leak users privacy information compared with the traditional CRL approach.

VI. Conclusion and Future Work

From the body of this paper, we can clearly conclude that with increasingly stringent security requirements, such as less verification time, less computational load and less reliance on temperproof hardware, the technologies involved in the solution of VANETs security and privacy become much more complex, from one pure digital signature algorithm to different algorithms. In addition, security and privacy preserving should be achieved at the same time, which brings to light the tradeoff between security and privacy that researchers must take into account.

To familiarize the readers with the background knowledge of VANETs, we first present the architecture of VANETs, threats and requirements for the security issues in this field. Then we further deepen our review by providing the general authentication processes in V2V and V2I communication scenarios and pointing out algorithms involved in these processes. The algorithms are categorized and discussed in details afterward. Furthermore, conditional privacy preserving methods and the tradeoff between security and privacy are provided.

Researchers are devoted to putting forward efficient authentication schemes to further reduce the great time and computation cost in the process of verification and revocation. On the one hand, researchers need to enhance the certificate revocation process to revoke illegal nodes. Instead of focusing on reducing the cost of refreshing the CRL, researches could turn to other fast revocation check schemes, which release vehicles from maintaining a huge CRL to record the revoked vehicles. On the other hand, researchers could detect legitimate vehicles that have a great chance to become malicious in advance based on their physical motion patterns, which could minimize their possible security attacks. In addition, up to now, most of the security models fail to resist adversaries inside the network which could not be ignored if deploy VANETs in reality. For example, the communication of legitimate vehicles could not be traced even when the responsible RSUs have been compromised by adversaries.

Further, according to simulation results of most of the proposed security and privacy preserving schemes, the message loss ratio is near 0 and end-to-end delay is lower than 20ms, which are quite desirable. More performance evaluation of these schemes should be conducted on a large-scale VANET, with varying vehicle mobility models, like creating a stronger threat model in which an adversary can utilize more character factors to track a vehicle.

References

[1] F. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: An IEEE intelligent transportation systems society update," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 68–69, Oct. 2006.

[2] X. Shen, X. Cheng, L. Yang, R. Zhang, and B. Jiao, "Data dissemination in vanets: A scheduling approach," *IEEE Tran. Intell. Transp. Syst.*, vol. 15, no. 5, pp. 2213–2223, Oct. 2014.

[3] X. Shen, R. Zhang, X. C. L. Yang, and B. Jiao, "Cooperative data dissemination via space-time network coding in vehicular networks," in *Proc. IEEE GLOBECOM*, Atlanta, GA, USA, Dec. 9–13, 2013, pp. 3406–3411.

[4] L. Yang and F. Wang, "Driving into intelligent spaces with pervasive communications," *IEEE Trans. Intell. Syst.*, vol. 22, no. 1, pp. 12–15, Jan. 2007.

[5] L. Xiao *et al.*, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[6] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. IEEE ISADS*, Sedona, AZ, USA, Mar. 21–23, 2007, pp. 344–351.

[7] Y. Wei, *Wireless Network Security*. Henan, China: Higher Educ. Press, 2013.

[8] L. Chun, H. Min, and C. Yen, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 1, no. 12, pp. 2803–2814, Jan. 2008.

[9] F. Qu and L. Yang, "On the estimation of doubly-selective fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1261–1265, Apr. 2010.

[10] J. Blum, A. Eskandarian, and J. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 5, no. 4, pp. 347–351, Dec. 2004.

[11] X. Cheng *et al.*, "Cooperative mimo channel modeling and multi-link spatial correlation properties," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 388–396, Feb. 2012.

[12] Z. Lei, W. Qian, A. Solanas, and J. Domingo, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Tran. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[13] K. Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1345–1358, Sep. 2011.

[14] J. Hubaux, S. Capkun, and J. Epfl, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May 2004.

[15] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proc. IEEE Int. Conf. Commun. Netw.*, Beijing, China, Oct. 25–27, 2006, pp. 1–8.

[16] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: A position paper," in *Proc. Workshop Standards Privacy User-Centric Identity Manage*, 2006, p. 7.

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

[18] H. Jiun, Y. Lo, and C. Hung, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular Ad Hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

[19] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[20] S. Horng *et al.*, "b-specs+: Batch verification for secure pseudonymous authentication in vanet," *IEEE Tran. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

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

[22] S. Goudarzi *et al.*, "A systematic review of security in vehicular Ad Hoc network," in *Proc. 2nd Symp. WSCN*, Tabuk, Saudi Arabia, Dec. 13–16, 2013, pp. 1–10.

[23] G. Samara, W. Salihy, and R. Sures, "Security analysis of vehicular ad hoc networks," in *Proc. 2nd Int. Conf. Netw. Appl., Protocols Services*, Alor Setar, Malaysia, Sep. 22–23, 2010, pp. 55–60.

[24] S. Sultann, M. Doori, A. Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, no. 2014, pp. 380–392, Mar. 2013.

[25] F. Qu, F. Wang, and L. Yang, "Intelligent transportation spaces: Vehicles, traffic, communications, and beyond," *IEEE Commun. Mag.*, vol. 48, no. 1, pp. 136–142, Nov. 2010.

[26] X. Cheng, C. Wang, D. Laurenson, S. Salous, and A. Vasilakos, "An adaptive geometry-based stochastic model for non-isotropic mimo mobile-to-mobile channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4824–4835, Sep. 2009.

[27] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proc. SASN*, Alexandria, VA, USA, Nov. 2005, pp. 11–21.

[28] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular Ad Hoc networks," in *Proc. MobiQuitous*, Philadelphia, PA, USA, Aug. 6–10, 2007, pp. 1–8.

[29] S. Park, B. Aslam, D. Turgut, and C. Zou, "Defense against sybil attack in vehicular Ad Hoc network based on roadside unit support," in *Proc. IEEE Military Commun. Conf.*, Boston, MA, USA, Oct. 2009, pp. 1–7.

[30] P. Kamat, A. Baliga, and W. Trappe, "Secure, pseudonymous, and auditable communication in vehicular Ad Hoc networks," *Security Commun. Netw.*, vol. 1, no. 2008, pp. 233–244, Jun. 2008.

[31] Y. Qian and N. Moayeri, "Design of secure and application-oriented vanets," in *Proc. IEEE Veh. Technol. Conf.*, Singapore, May 11–14, 2008, pp. 2794–2799.

[32] M. Raya and J. Hubaux, "Securing vehicular Ad Hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jun. 2007.

[33] F. Ghaleb, M. Razzaque, and I. Isnin, "Security and privacy enhancement in vanets using mobility pattern," in *Proc. IEEE ICUFN*, Da Nang, Vietnam, Jul. 2–5, 2013, pp. 184–189.

[34] T. Leinmuller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," in *Proc. IEEE 4th Annu. Conf. Wireless Demand Netw. Syst. Services*, Oberguyrgl, Austria, Jan. 2007, pp. 84–91.

[35] X. Cheng, C.-X. Wang, B. Ai, and H. Aggoune, "Envelope level crossing rate and average fade duration of nonisotropic vehicle-to-vehicle ricean fading channels," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 62–72, Aug. 2013.

[36] X. Cheng, C.-X. Wang, D. Laurenson, S. Salous, and A. V. Vasilakos, "New deterministic and stochastic simulation models for non-isotropic scattering mobile-to-mobile rayleigh fading channels," *Wireless Commun. Mobile Comput.*, vol. 11, pp. 829–842, Oct. 2011.

[37] P. Papadimitratos *et al.*, "Architecture for secure and private vehicular communications," in *Proc. IEEE ITST*, Sophia Antipolis, France, Jun. 6–8, 2007, pp. 1–6.

[38] F. Li and Y. Wang, "Routing in vehicular Ad Hoc networks: A survey," *IEEE Tran. Veh. Technol.*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[39] P. Papadimitratos *et al.*, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[40] K. Plößl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular Ad Hoc networks," in *Proc. IEEE 1st Int. Conf. Availability, Rel. Security*, Vienna, Austria, Apr. 2–5, 2006, pp. 374–381.

[41] C. Cseh, "Architecture of the dedicated short-range communications (DSRC) protocol," in *Proc. IEEE Veh. Technol. Conf.*, Ottawa, ON, Canada, May 18–21 1998, pp. 2095–2099.

[42] M. Raya and J. P. Hubaux, "Security aspects of inter-vehicle communications," in *Proc. Swiss Transp. Res. Conf.*, Ascona, Switzerland, Mar. 2005, pp. 1–3.

[43] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "Raise: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE ICC*, Beijing, China, May 19–23, 2008, pp. 1451–1457.

[44] C. Gañán, J. Muñoz, O. Esparza, J. Díaz, and J. Alins, "EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks," *Pervasive Mobile Comput.*, vol. 1, no. 1, Jan. 2014.

[45] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 13–18, 2008, pp. 1903–1911.

[46] R. Zhang *et al.*, "Interference graph-based resource-sharing schemes for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4028–4039, Oct. 2013.

[47] X. Cheng *et al.*, "Wideband channel modeling and intercarrier interference cancellation for vehicle-to-vehicle communication systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 434–448, Sep. 2013.

[48] H. Di, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Trans. Veh. Technol.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[49] K. A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

[50] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, Intell. Transp. Syst. Committee IEEE Veh. Technol. Soc. Std., IEEE Std. 1609.2-2006, Jun. 2006.

[51] M. Nowatkowski and H. Owen, "Certificate revocation list distribution in vanets using most pieces broadcast," in *Proc. IEEE SoutheastCon*, Concord, NC, USA, Mar. 18–21, 2010, pp. 238–241.

[52] J. Haas, Y. Hu, and K. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 595–604, Mar. 2011.

[53] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks," in *Proc. Global Telecommun. Conf.*, Honolulu, HI, USA, Nov. 30–Dec. 4, 2009, pp. 1–6.

[54] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533–549, Feb. 2010.

[55] C. Jung, C. Sur, Y. Park, and K. Rhee, "A robust conditional privacy-preserving authentication protocol in vanet," in *Proc. 1st Int. ICST Conf. Security Privacy Mobile Inf. Commun. Syst.*, Turin, Italy, Jun. 3–5, 2009, pp. 35–45.

[56] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "A secure and efficient revocation scheme for anonymous vehicular communications," in *Proc. IEEE ICC*, Cape Town, South Africa, May 23–27 2010, pp. 1–6.

[57] J. Chen, X. Cao, Y. Zhang, W. Xu, and Y. Sun, "Measuring the performance of movement-assisted certificate revocation list distribution in vanet," *Wireless Commun. Mobile Comput.*, vol. 11, no. 7, pp. 888–898, Jul. 2011.

[58] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. Hubaux, "Certificate revocation in vehicular networks," Tech. Rep. LCA-Report-2006-06, 2006.

[59] T. Chima, S. Yiua, L. Hui, and V. Li, "SPECS: Secure and privacy enhancing communications schemes for vanets," *Ad Hoc Netw.*, vol. 9, no. 2011, pp. 189–203, Mar. 2011.

[60] K. Laberteaux, J. Haas, and Y. Hu, "Security certificate revocation list distribution for vanet," in *Proc. VANET*, San Francisco, CA, USA, Sep. 15, 2008, pp. 88–89.

[61] W. Ming, L. Dan, Z. Lie, X. Yong, and W. Fei, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication," *Computing*, vol. 1, no. 1, Mar. 2014.

[62] L. Jie, L. Huang, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.

[63] S. Jin, Z. Chi, Z. Yan, and F. Yu, "An identity-based security system for user privacy in vehicular Ad Hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[64] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, pp. 36–63, Jan. 2001.

[65] W. Caelli, E. Dawson, and S. Rea, "PKI, elliptic curve cryptography, and digital signatures," *Comput. Security*, vol. 18, no. 1, pp. 47–66, 1999.

[66] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2182–2192, Jun. 2013.

[67] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient vanet authentication," *J. Commun. Netw.*, vol. 11, no. 6, pp. 574–588, Dec. 2009.

[68] S. Yi, L. Rong, L. Xiao, X. Sherman, and S. Jin, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[69] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Adv. Cryptol.*, vol. 2248, no. 2001, pp. 514–532, Jan. 2001.

[70] A. Enge, "Bilinear pairings on elliptic curves," HAL, Lyon, France, 2012.

[71] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Eurocrypto LNCS*, 2004, pp. 213–229.
[72] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The tesla broadcast authentication protocol," in *Proc. RSA CryptoBytes*, 2005, vol. 5, pp. 2–13.
[73] P. Ning, A. Liu, and W. Du, "Mitigating dos attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sens. Netw.*, vol. 4, no. 1, pp. 1–6, Jan. 2008.
[74] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in vanets," in *Proc. IEEE Int. Conf. Netw. Commun.*, Avignon, France, Oct. 12–14, 2008, pp. 508–513.
[75] K. Plößl and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular Ad Hoc networks," *Comput. Standards Interfaces*, vol. 30, no. 2008, pp. 390–397, Jan. 2008.
[76] M. Bellare, J. A. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Espoo, Finland, May 31–Jun. 4, 1998, pp. 236–250.
[77] H. Zhu, X. Lin, R. Lu, P. Ho, and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in *Proc. IEEE ICC*, Beijing, China, May 19–23, 2008, pp. 1436–1440.
[78] S. Zhang, J. Tao, and Y. Yuan, "Anonymous authentication-oriented vehicular privacy protection technology research in vanet," in *Proc. IEEE ICECE*, Yichang, China, Sep. 16–18, 2011, pp. 4365–4368.
[79] W. Qian, J. Ferrer, and Úrsula, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.
[80] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in vanets," in *Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens.,Mesh Ad Hoc Commun. Netw.*, Rome, Italy, Jun. 22–26, 2009, pp. 1–9.
[81] K. Sampigethaya *et al.*, "Caravan: providing location privacy for vanet," in *Proc. ESCAR*, Cologne, Germany, Nov. 2005, pp. 1–15.
[82] C. Tsai, C. Lin, and M. Hwang, "A new strong-password authentication scheme using one-way hash functions," *Int. J. Comput. Syst. Sci.*, vol. 45, no. 4, pp. 623–626, Jun. 2006.
[83] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for vanet," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
[84] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in vanets," *J. Netw. Comput. Appl.*, vol. 36, no. 2013, pp. 1599–1609, Feb. 2013.
[85] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. Bhaskar, "Pseudonym based mechanism for sustaining privacy in vanets," in *Proc. IEEE Int. Conf. Comput. Intell., Commun. Syst. Netw.*, Indore, India, Jul. 23–25, 2009, pp. 420–425.
[86] T. Little and A. Agarwal, "An information propagation scheme for vanets," in *Proc. IEEE Int. Conf. Intell. Transp. Syst.*, Sep. 13–15, 2005, pp. 155–160.
[87] P. Barreto, B. Libert, N. McCullagh, and J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. 11th Int. Conf. Theory Appl. Cryptology Inf. Security*, Chennai, India, Dec. 4–8, 2005, pp. 515–532.
[88] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A practical pseudonym changing scheme for location privacy in vanets," in *Proc. IEEE VNC*, Tokyo, Japan, Oct. 28–30, 2009, pp. 1–8.
[89] V. S. Chaurasia and Bhasker, "Message broadcast in vanets using group signature," in *Proc. IEEE Int. Conf. Wireless Commun. Sens. Netw.*, Allahabad, India, Dec. 2008, pp. 131–136.
[90] J. Chou and Y. Chen, "A secure anonymous communication scheme in vehicular ad hoc networks from pairings," *IACR Cryptology ePrint Archive*, vol. 2010, no. 28, pp. 1–30, Jan. 2010.
[91] C. Gañán, J. Muñoz, O. Esparza, J. Díaz, and J. Alins, "PPREM: Privacy preserving revocation mechanism for vehicular Ad Hoc networks," *Comput. Standards Interfaces*, vol. 36, no. 2014, pp. 513–523, Aug. 2013.
[92] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms-ideal and real," in *Proc. IEEE Veh. Technol. Conf.*, Dublin, Ireland, Apr. 22–25, 2007, pp. 2521–2525.
[93] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, Philadelphia, PA, USA, Oct. 1, 2004, pp. 29–37.
[94] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," in *Proc. MobiHoc*, Montreal, QC, Canada, Sep. 9–14, 2007, pp. 164–171.
[95] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for DTN protocol evaluation," in *Proc. SIMUTools*, Rome, Italy, Jun. 2009, pp. 1–10.
[96] D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner, "Sumo (simulation of urban mobility); an open-source traffic simulation," in *Proc. 4th MESM*, Sharjah, UAE, Sep. 2002, pp. 183–187.
[97] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *J. Cryptology*, 2000, pp. 446–465.
[98] X. Lin, C. Zhang, X. Sun, P.-H. Ho, and X. Shen, "Performance enhancement for secure vehicular communications," in *Proc. IEEE GLOBECOM*, Washington, DC, USA, Nov. 26–30, 2007, pp. 480–485.
[99] H. Moustafa, G. Bourden, and Y. Gourhan, "Providing authentication and access control in vehicular network environment," in *Proc. Int. Inf. Security Conf.*, Karlstad, Sweden, May 22–24 2008, pp. 62–73.
[100] D. Rivas, J. Ordinas, M. Zapata, and J. Pozo, "Security on vanets: Privacy, misbehaving nodes, false information, and secure data aggregation," *J. Netw. Comput. Appl.*, vol. 34, no. 2011, pp. 1942–1955, Jul. 2011.
[101] L. Rong, L. Xiao, L. Xiaoh, and S. Xue, "A dynamic privacy-preserving key management scheme for location-based services in vanets," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.
[102] L. Rong, L. Xiao, H. Luan, L. Xiaoh, and S. Xue, "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.
[103] D. Silva, T. Kosa, S. Marsh, and K. Khatib, "Examining privacy in vehicular ad-hoc networks," in *Proc. DIVANet*, Paphos, Cyprus, Oct. 2012, pp. 105–109.
[104] A. Slagell, R. Bonilla, and W. Yurcik, "A survey of pki components and scalability issues," in *Proc. IEEE Int. Conf. Perform., Comput., Commun.*, Phoenix, AZ, USA, Apr. 10–12, 2006, p. 484.
[105] B. Yua, C. Xua, and B. Xiao, "Detecting sybil attacks in vanets," *J. Parallel Distrib. Comput.*, vol. 73, no. 2013, pp. 746–756, Feb. 2013.
[106] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 13–18, 2008, pp. 816–824.
[107] R. Zhang *et al.*, "A unified tdma-based scheduling protocol for vehicle-to-infrastructure communications," in *Proc. IEEE Int. Conf. WCSP*, Hangzhou, China, Oct. 24–26, 2013, pp. 1–6.
[108] Z. Zhao, X. Cheng, M. Wen, L. Yang, and B. Jiao, "Constructed data pilot-assisted channel estimators for mobile environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 947–957, Apr. 2014.
[109] Car 2 car communication consortium. [Online]. Available: http://www.car-to-car.org/
[110] Inemanet framework for omnet++. [Online]. Available: http://github.com/inetmanet/inetmanet/tree/master
[111] Inet framework extension. [Online]. Available: https://github.com/inetmanet/
[112] The website of ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns/
[113] Objective modular network testbed inc++ (omnet++). [Online]. Available: www.omnetpp.org
[114] Omnet++. [Online]. Available: http://www.omnetpp.org/

Fengzhong Qu (S'07–M'10–SM'15) received the B.S. and M.S. degrees in electrical engineering from Zhejiang University, Hangzhou, China, in 2002 and 2005, respectively, and the Ph.D. degree from the University of Florida, Gainesville, FL, USA, in 2009. From 2009 to 2010, he was an Adjunct Research Scholar with the Department of Electrical and Computer Engineering, University of Florida. Since 2011, he has been with the Ocean College, Zhejiang University, where he is currently an Associate Professor and an Associate Chair with the Institute of Marine Information Science and Engineering. His current research interests include intelligent transportation wireless communications and networking, underwater acoustic communications and networking, and seafloor observatories.

Zhihui Wu received the B.S. degree in automation from Nanjing University of Post and Telecommunication, Nanjing, China, in 2014. She is currently working toward the M.S. degree in naval architecture and ocean engineering with Zhejiang University, Hangzhou, China. Her research interests include wireless communication and underwater acoustic communication.

Fei-Yue Wang (S'87–M'89–SM'94–F'03) received the Ph.D. degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1990. In 1990, he joined the University of Arizona and became a Professor and Director of the Robotics and Automation Laboratory and Program in Advanced Research for Complex Systems. In 1999, he founded the Intelligent Control and Systems Engineering Center, Chinese Academy of Sciences (CAS), Beijing, China, under the support of the Outstanding Oversea Chinese Talents Program. In 2002, he was appointed as the Director of the CAS Key Laboratory for Complex Systems and Intelligence Science. From 2006 to 2010, he was the Vice President for Research, Education, and Academic Exchanges with the Institute of Automation, CAS. Since 2005, he has been the Dean of the School of Software Engineering, Xian Jiaotong University. In 2011, he became the Director of the State Key Laboratory of Management and Control for Complex Systems, and launches the Qingdao Academy of Intelligent Industries in 2014. Currently, he has been a researcher, educator, and practitioner of intelligent and complex systems over three decades. He has served as General or Program Chair of more than 20 IEEE, INFORMS, ACM, ASME conferences since 1997. He was the Founding Editor-in-Chief of *International Journal of Intelligent Control and Systems* from 1995 to 2000, *Series on Intelligent Control and Intelligent Automation* from 1996 to 2004, and *IEEE Intelligent Transportation Systems Magazine*, and was the Editor-in-Chief of *IEEE Intelligent Systems Magazine*. He has served as the Editor-in-Chief of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS since 1999. He was the President of IEEE ITS Society from 2005 to 2007, the Chinese Association for Science and Technology (CAST, USA) in 2005, and the American Zhu Kezhen Education Foundation from 2007 to 2008. Since 2008, he has been the Vice President and Secretary General of Chinese Association of Automation. He is a member of Sigma Xi and an elected Fellow of INCOSE, IFAC, ASME, and AAAS.

Woong Cho (S'06–M'08) received the B.S. degree in electronics engineering from the University of Ulsan, Ulsan, Korea, in 1997; the M.S. degree in electronic communications engineering from Hanyang University, Seoul, South Korea, in 1999; the M.S. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 2003; and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2007. From February 2008 to February 2012, he was a Senior Research Engineer with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea. He is currently with the Department of Computer System Engineering, Jungwon University, Goesan, South Korea. His research interests include cooperative/relay networks, vehicular communications, and signal processing for wireless communications.