IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Privacy-Preserving Authentication and Pseudonym Revocation Scheme for VANETs

JIAYU QI[1], TIANHAN GAO[2]
[1]Software College, Northeastern University, Shenyang, 110169, China (e-mail: yoonagoogoo@gmail.com)
[2]Software College, Northeastern University, Shenyang, 110169, China
Engineering Research Center of Security Technology of Complex Network System, Ministry of Education, China (e-mail: gaoth@mail.neu.edu.cn)

Corresponding author: Tianhan Gao (e-mail: gaoth@mail.neu.edu.cn).

This work was supported by the Fundamental Research Funds for the Central Universities under Grant Number: N2017002 and N2024005-1.

ABSTRACT With the development of Intelligent Transportation Systems (ITS), Vehicular Ad hoc Networks (VANETs) have become a research hotspot in recent years. However, the vehicle communication system is vulnerable, resulting in threats to the privacy of users. This paper proposes a secure and efficient identity-based anonymous authentication scheme and uses pseudonyms to enhance the privacy protection of vehicle users. By improving the existing vehicle public key infrastructure and introducing Bloom filter to compress the Certificate Revocation List (CRL), the efficient pseudonym revocation scheme is then presented under the premise of ensuring user privacy. This scheme is able to perform batch pseudonym revocation and keep the pseudonym unlinkable. The security analysis shows that the proposed scheme is able to meet the security and privacy requirements in VANETs and CRL distribution.

INDEX TERMS VANETs, privacy-preserving authentication, pseudonym revocation, CRL

I. INTRODUCTION

IN an open access environment such as Vehicular Ad hoc Networks (VANETs), the vehicle communication (VC) system is vulnerable, resulting in threats to the privacy of users. Security and privacy solutions have been proposed by technical specifications represented by IEEE WAVE 1609.2 (Security Services for Applications and Management Messages) [1], ETSI 102 (Security, Trust and Privacy Management) [2], and projects (SeVeCom [3], PRESERVE [4], CAMP [5]). A consensus was reached on the use of public key cryptography (PKC) to protect Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications [6]: a set of trust authorities (TAs) constitute the Vehicle Public-Key Infrastructure (VPKI), which provides multiple short-term certificates (pseudonyms) to legitimate vehicles. In V2V/V2I communication, the vehicle switches from one pseudonym to another to realize unlinkability. While anonymity is conditional. If the vehicle violates the law or its pseudonym certificate expires, the pseudonym and the certificate need to be revoked. Furthermore, when there are harmful behaviors in the network, it is necessary to spread the pseudonyms and certificate of the illegal vehicle to maintain communication security. In practice, Certificate Revocation List (CRL) is the most widely used revocation method for illegal vehicles in VANETs. In order to check the validity of certificates, vehicles need to obtain CRL frequently. Since the size of CRL file increases linearly with the number of revoked certificates, this method leads to a large delay and affects the real-time performance of the revocation scheme.

In the current VANETs security solutions, most researches focus on security and privacy. In [7], in order to realize identity authentication and ensure anonymity, the On Board Unit (OBU) of each vehicle needs to load a large number of anonymous public key and private key pairs in advance. However, this causes the problem of high management overhead of CRL. When the vehicle's certificate is revoked, a large number of pre-loaded certificates also need to be revoked. Some schemes try to use pseudonyms to replace certificates, while there are still problems in distributing CRL. Calandriello et al. [8] and Jung et al. [9] proposed pseudonym-based authentication schemes to keep vehicles anonymous. However, in these schemes, the distribution of CRL is heavy time consuming, which will greatly affect the availability of schemes. To reduce the size of CRL, the group

signature is adopted in [10], [11]. Whereas it is not suitable for VANETs as the high cost and delay. Wang et al. [42] proposed an efficient authentication scheme mainly utilizing symmetric encryption and message authentication code (MAC). Furthermore, vehicles need not maintain CRL. The scheme allows Key Management Centre (KMC) to manage the identity of all vehicles as the only trusted authority, and is also responsible for generating and updating the vehicle keys. KMC is a single threat model so the system is obviously not secure. To distribute the capability of identity resolution between authorities, Ali et al. [43], [44] presented an authentication framework, which can avoid pseudonyms being linked. The pseudonyms validity is set as between 10 to 50 milliseconds [44] and the vehicle interacts with Pseudonym Provider (PP) frequently. Therefore, the connectivity between them needs to be considered. Furthermore, PP sends multiple pseudonyms to the vehicle each time and they are all legitimate at the same interval, which is not security enough. In [45], Vijayakumar et al. proposed a privacy preservation and anonymous authentication scheme using anonymous certificates. In addition, it also provides a batch verification to authenticate the vehicles group by RSU. While, it is still not efficient enough because the communication overhead and message loss ratio are not considered, and vulnerable to DoS attack. Zhong et al. [46] presented an efficient conditional privacy-reserving authentication scheme utilizing hash operations with lower computational costs. It adopts a way that RSU assists OBU in message verification and also knows the OBU's identity. Moreover, it is not effective against all kinds of attacks. In recent years, in order to ensure effective anonymous authentication and revocation, RSU (Road Side Unit)-dependent authentication protocol [12] and cooperative authentication protocol [13] [14] were proposed. However, in [12], as a group manager, RSU issues a group member key to each vehicle, consequently, it can track the trajectory of the vehicle. In [13], in order to ensure privacy, each vehicle is assigned many pseudonyms. When the vehicle is revoked, CRL size will be greatly increased. whereas the cooperative authentication method proposed in [14] can only verify messages when the density of vehicles on the road is high. In addition, [14] uses the group key distribution approach to realize efficient revocation, which may cause security problems [15].

In recent vehicle revocation approaches, CRL slicing is used and each CRL slice is delivered independently [16]. CRL slices are distributed in a car-to-car manner to speed up the distribution process in high vehicle density areas [17]–[19]. However, dividing CRL into multiple fragments is vulnerable to attack. An attacker can use signature verification latency to forge CRL fragments for DoS attacks, thereby preventing the vehicle from obtaining real CRL fragments. In addition, for Vehicular Public-Key Infrastructure (VPKI) and receiving vehicles, the computational overhead increases linearly with the number of CRL fragments. To reduce the size of the transmitted CRL, a Bloom filter (BF) is proposed to compress the CRL [20]. However, the size of the CRL increases linearly with the number of revoked pseudonyms, and most of the compressed CRL may be independent of the receiving vehicle. There are also schemes to apply edge computing to the Internet of Things environment to distribute revocation information [21]. The combination of edge computing and VANETs is promising, which is still in the early research phase.

In this paper, we design a secure and efficient certificate revocation scheme for VANETs which can revoke the pseudonym effectively and provide strong privacy protection for users. The contributions are as follows: (1) A secure and efficient identity-based anonymous authentication scheme is proposed to support cross-domain vehicles. (2) The proposed scheme can effectively revoke a batch of pseudonyms without compromising the privacy of users. (3) In order to solve the problem of CRL management (e.g. distribution, update) caused by pseudonyms, Bloom filter is introduced to effectively reduce the size of CRL and decrease the management cost.

The remainder of this paper is organized as follows. In Section II, the necessary preliminaries are introduced. The system overview is presented in Section III. In Section IV, the proposed scheme is elaborated. The security analysis is given in Section V. Section VI evaluates the performance of the proposed scheme by comparing with other typical schemes in terms of anonymous authentication efficiency and pseudonym revocation efficiency. Finally, the conclusion is drawn in Section VII.

II. PRELIMINARIES

This section introduces the necessary preliminaries to support the proposed scheme.

A. BILINEAR PAIRING

Let G_1 be an additive cycle group with prime order p, and G_2 be a multiplicative group of the same order. A bilinear pairing e: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties [22].

1) Bilinearity: For any $P, Q \in G_1$, $a, b \in Z_p^*$, there are $e(aP, bQ) = e(P, Q)^{ab}$.
2) Non-degeneracy: Existing a certain $P, Q \in G_1$ satisfies $e(P, Q) = 1$.
3) Computability: An efficient algorithm can calculate $e(P, Q) \in G_2$, where $P, Q \in G_1$.

B. MATHEMATICAL PROBLEMS AND ASSUMPTIONS

The relevant problem and the assumption are given below, which are the cornerstones of the cryptosystem involved in this paper.

Definition 1: q-Strong Diffie-Hellman problem (q-SDHP) Given $(P, xP, x^2P, ..., x^qP)$ as input, finding $(c, \frac{1}{x+c}P) \in Z_p^* \times G_1$ with $x, q, c \in Z_p^*$.

Assumption 1: q-Strong Diffie-Hellman (q-SDH) assumption

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027718, IEEE Access

If no algorithm can solve the q-SDHP on G_1 with the advantage ε within time t, then the q-SDHP on G_1 is difficult, that is, the q-SDH assumption holds.

C. BLMQ SIGNATURE MECHANISM

The proposed scheme uses the BLMQ signature mechanism introduced in [23], which makes a balance between security and efficiency. Let G_1 be an additive cycle group and the prime order is q. Let G_2 be a multiplicative group of the same order. Let e: $G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing. The details of the mechanism are as follows.

1) Setup. PKG (Private Key Generator) generates public parameter $param = \{G_1, G_2, q, e, P, P_{pub}, g, H_1, H_2\}$, where $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ and $g = e(P, P)$. PKG chooses $s \in Z_q^*$ as the master key, and the public key is P_{pub}=sP.
2) Extract. Given the signer's identity ID_U, PKG computes the private key $S_U = \frac{1}{H_1(ID_U)+s} P$ for the signer.
3) Sign. If a signer wants to sign message M, the following operations will be executed.
   a) Randomly chooses $r \in Z_q^*$.
   b) Calculates $x = g^r$.
   c) Calculates $h = H_2(M, x)$, $V = (r + h) S_U$.
   d) The signature on message M is: $\sigma = (h, V)$.
4) Verify. After receiving M and σ, the verifier checks $h \equiv H_2(M, e(V, H_1(ID_U)P + P_{pub})g^{-h})$ to verify whether σ is legal.

D. BLOOM FILTER

Bloom filter was proposed by Howard Bloom to retrieve whether a given element is in the collection. Bloom filter is a kind of random data structure, whose spatial efficiency is very high.

A Bloom filter corresponds to an array of m bits, initially all set to 0. To represent a collection of n elements: $S = \{x_1, x_2, \ldots, x_n\}$, the Bloom filter maps each element to a specified range of $\{1, \ldots, m\}$ using k independent hash functions. For any given element x, the position $h_i(x)$ of the $i\text{-}th$ hash function map is set to 1, $1 \leq i \leq k$. When we want to determine whether y belongs to the set, we should first apply k times hash function to y. If the positions of $h_i(y)$ are all 1, then y can be considered as an element in S. However, Bloom filter may produce a $falsepositive$, which indicates that an element x is in S, even if it is not in S. But for many applications, this is perfectly acceptable as long as the probability of $falsepositive$ is small enough. At present, Bloom filter is often used as message passing between nodes in network applications. Moreover, Compressed Bloom filter (CBF) [24] is able to improve the performance of Bloom filter and obtain a smaller false rate while ensuring a good transmission compression rate.

III. SYSTEM OVERVIEW

This section presents an overview of the proposed system including the system framework, the system model, the trust model, the attack model, revocation information and design objectives.

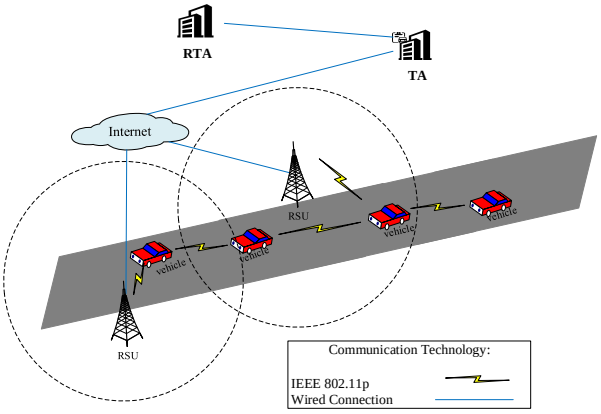


FIGURE 1. Network Architecture.

A. SYSTEM FRAMEWORK

As shown in Figure 1, the system has a four-layers architecture, including three types of entities. All infrastructures in the system are equipped with devices based on IEEE 802.11 p standard wireless communication modules and support Wireless Access in Vehicular Environment (WAVE) protocol stack. The OBU built into the vehicle can support IEEE 802.11 p standard and WAVE.

RTA and TA: RTA is the root trusted authority, as the top-layer of the system, which can authorize and issue secondary certificates to the lower-layer TA (trusted authority). The public and private keys of TAs are generated by RTA and the public parameters of TAs are further generated according to the system parameters published by RTA.

Each TA is regarded as a regional trusted authority and manages all RSUs and vehicles within its communication area. TA is responsible for the registration of RSUs and vehicles, and generates anonymous credentials for legal vehicles to apply for their pseudonyms. All RSUs generate public and private keys according to the public parameters issued by TA. TA is also responsible for the aggregation of revocation information in the region and the issuance of authoritative CRL.

RSU: RSUs are infrastructures built along the road, which are in charge of the authentication of vehicles accessing VANETs and the communication between vehicles and TA during driving. RSUs also generate pseudonyms, pseudonym certificates, as well as the corresponding public and private keys for legal vehicles according to the anonymous credentials submitted by vehicles. When a revoked pseudonym appears, RSU is responsible for distributing the pseudonym certificates revocation information.

OBU: OBU is a processing unit embedded in the vehicle, which is responsible for V2X communication, which includes both V2V and V2I. All vehicles can regularly send

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027718, IEEE Access

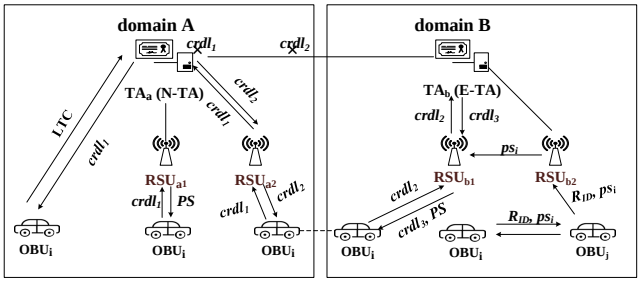


FIGURE 2. System model.

security information through OBU during driving, which is collected by RSUs. The security information includes driving speed, direction, and position of the vehicle. RSU transfers information between vehicles and TA.

TA communicates with RTA, other TAs, and RSUs in its domain through wired channels, while V2I and V2V communications are launched through wireless networks following DSRC (Dedicated Short Range Communications) protocol.

B. SYSTEM MODEL

Since vehicles are likely to cross one or even several areas on a relatively long journey, the scheme extends and enhances the current VPKI system, taking into account the cross-domain situation. There are two different domains in our system: native domains and external domains. When a vehicle leaves the domain managed by the native TA (N-TA) which it has initially registered with, the vehicle needs the external TA (E-TA) and the RSUs in the external domain to continue to provide it with services in the VANETs.

As shown in Figure 2, we figure out two domains: native domain A and external domain B. First of all, each vehicle (also called OBU later) holds an identity certificate issued offline by the vehicle administration (equivalent to CA), which is called long-term certificate (LTC). LTC is generated according to the real ID of the vehicle and contains the real identity information of the vehicle and the signature from CA. In order to access VANETs, vehicles need to complete initial registration with their N-TA. The OBU submits LTC to N-TA through the secure channel to execute initial registration and obtains the anonymous credential ($crdl$) issued and signed by N-TA. The credential can be used to apply for pseudonyms from RSU in the domain (such as RSU_{a1} or RSU_{a2} in domain A). OBU determines when to execute the pseudonym acquisition protocol based on various factors [25]. If the pseudonym request time in the vehicle's credential is about to expire, OBU sends the current $crdl$ and the new request time interval to TA in the domain to apply for a new credential to replace the current one through RSU. If the vehicle is traveling to an external domain (domain B), it does not have to register again with E-TA. OBU only needs to request E-TA for a new credential through the RSU of first access (i.e., RSU_{b1}). The new credential is signed by E-TA and can be used to apply for pseudonyms from the

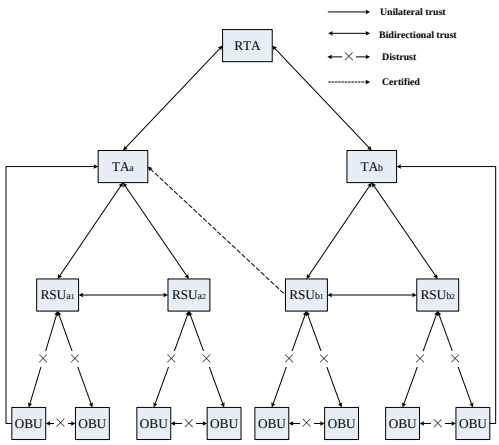


FIGURE 3. Trust Model.

RSU (such as RSU_{b2}) in domain B. In this way, even if the vehicle travels across domains, its identity information is always protected and is not exposed to E-TA and RSUs. OBU can be authenticated by a currently valid pseudonym and can interact with all RSUs in its native or external domain. CRL obtained from RSU and Online Certificate Status Protocol (OCSP) are used to publish the revocation information [26]. We assume that all vehicles registered in the system are equipped with Tamper Proof Device (TPD) to ensure that the private keys are secure enough, and that there is a misconduct detection system to trigger the revocation, such as [27]. RSU is able to initiate the process of resolving and revoking all pseudonyms of the misbehaved vehicle. When the OBU has malicious behavior in VANETs, such as spreading disloyal traffic information, other OBUs communicating with it will report its pseudonym to the nearest RSU. The RSU will further report the pseudonym together with the credential to TA.

C. TRUST MODEL

The trust model of the proposed scheme is depicted as Figure 3. It is assumed that all TAs trust RTA and pre-store the certificate of RTA, which can verify the legitimacy of vehicles. TAs communicate through secure channels and have mutual trust relations. All RSUs in the same domain trust the TA. RSUs (such as RSU_{a1} and RSU_{a2}, RSU_{b1} and RSU_{b2}) communicate through secure channels and trust each other. RSU trusts TAs of other domains conditionally. For example, RSU_{b1} needs to use the public key of TA_a e.g. domain ID of TA_a to verify the credentials signed by TA_a. There is no trust relations between OBUs and RSUs. OBUs distrust each other before authentication.

D. ATTACK MODEL

We assume that the adversary who carries out passive attack can monitor the communication channel and eavesdrop the message. While in active attack, the external adversary, i.e., unauthorized entity, tries to tamper with the message or even

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027718, IEEE Access

replace the original message in order to induce legitimate vehicles to accept forged or harmful messages without being detected. In addition, the internal adversary, i.e., malicious, affected or non-cooperative entity, may obtain and analyze messages from others to maximize abuse of VANETs.

The anonymous authentication in the proposed scheme is based on Identity Based Signature (IBS) mechanism. For the attack model of IBS schemes, it is necessary to allow the adversary to perform key extraction queries and chosen identity attack. The IBS mechanism is secure if no polynomial time attacker $\mathcal{A}$ wins the following game with at least advantage ε in time t after q_k times of key extraction queries and q_s times of signature queries, where the advantage of $\mathcal{A}$ is defined as his or her probability of winning the game. The adaptively chosen and identity attack game of IBS system consists of the following three stages, which is a game between challenger $\mathcal{C}$ and attacker $\mathcal{A}$.

1) Initialization: $\mathcal{C}$ runs the system Setup algorithm and sends the generated system parameters to $\mathcal{A}$. $\mathcal{C}$ keeps the master key s secretly.
2) Attack: $\mathcal{A}$ performs Extract query and Sign query. In an Extract query, $\mathcal{A}$ selects an identity ID, and $\mathcal{C}$ returns the private key corresponding to ID which is obtained by running Extract. In a Sign query, $\mathcal{A}$ submits an identity ID and a message m. $\mathcal{C}$ first obtains the private key by running Extract, then runs Sign to generate the signature σ and sends σ to $\mathcal{A}$.
3) Forgery: $\mathcal{A}$ outputs (ID^*, m^*, σ^*). $\mathcal{A}$ wins the game when the following three conditions are met.
   a) σ^* is a valid signature for m^* and ID^*.
   b) ID^* has not performed a Extract query.
   c) (ID^*, m^*) has not performed a Sign query.

Our attack model also takes into account honest but curious VPKI entities, such as RSU, which comply with security protocols and policies, but may collect private information of vehicles and share it with other RSU to damage users' privacy.

E. REVOCATION INFORMATION

The concept of certificate chain and the relationship between certificate and revocation information is given in IEEE 1609.2 protocol. The revocation information is issued by CRACA(Certificate Revocation Authorizing CA) or by $CRL\ signer$ directly authorized by CRACA.

In this paper, RSUs act as the role of $CRL\ signer$. As shown in Figure 4, TA is authorized by RTA and holds a CRACA certificate. TA authorizes all RSUs within its domain to act as $CRL\ signer$, enabling RSUs to issue revocation information. The pseudonym certificate of the vehicle is issued by RSU. Consequently, it is possible for vehicles to obtain the certificate revocation information directly through RSU in a timely manner rather than TA at regular intervals.

F. DESIGN OBJECTIVES

Referring to [28], the security and privacy requirements in VC system can be summarized as follows.

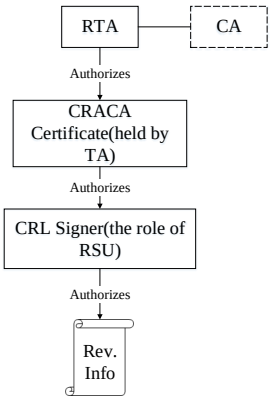


FIGURE 4. Revocation information.

Authentication and Authorization. Authentication is to verify the authenticity of an identity or other message properties. In VC system, communication and cooperation between entities need to exchange information, so users should minimize the disclosure of personal information. In anonymous authentication, in order not to expose the sender's identity and ensure confidentiality, it is necessary to be able to authenticate through anonymous certificates or credentials issued by trusted third parties.

Non-repudiation and revocation. In VC system, the reliability of messages is particularly important. Forged and illusive information may cause traffic accidents, so it is necessary to be able to hold the sender accountable, which means that the sender cannot deny having signed and sent a message. If anonymous credentials are used, only authorized entities can resolve the identity in case of disputes. At the same time, effective methods of revocation information distribution must be provided.

Anonymity and unlinkability. Anonymity requires that it is impossible to link the message to the sender according to the content of the message, and unlinkability requires that the relationship between two or more items of interest cannot be linked. The unlinkability of the sender and the message it sent is equivalent to the anonymity of the sender. The unlinkability of continuous messages from the same vehicle can avoid being tracked and protect location privacy.

According to the above requirements, the security and privacy objectives of the proposed scheme are put forward as follows.

Authentication and confidentiality. V2I and V2V authentication should be achieved without revealing the identity of the vehicle. When crossing domains, the vehicle does not need to provide the real identity to E-TA. Besides, communication between vehicles and RSUs should be encrypted.

Authorization and access control. Only legitimate vehicles can be verified and authorized by RSU and other vehicles without disclosing their real identity. Similarly, VANETs services are only available for legitimate vehicles.

Non-repudiation and revocation. All signatures in the scheme should not be denied by the signer. Once a dispute occurs and the real identity of the vehicle needs to be revealed to support traceability, the scheme should provide conditional anonymity and enable the vehicle to be revoked when misbehavior is detected.

Anonymity and unlinkability. The vehicle conceals its real identity even when crossing domains. In addition, it should be infeasible to link a pseudonym with the previous expired pseudonyms.

In terms of the effectiveness of the proposed scheme, we need to achieve the objective as follow.

Efficiency. The computational cost of the proposed scheme should be reduced to efficiently realize authentication and revocation. Therefore, the proposed scheme should to be more robust, stable and scalable.

IV. THE PROPOSED SCHEME

This section elaborates on the proposed scheme. In order to facilitate the following description, we present the symbols and the definitions involved in the proposed scheme in Table 1. It should be noted that in our scheme, $System\ Initialization$ and $Key\ Extraction$ of RTA and TAs are based on IBS mechanism. RTA is the top authority. The public and private keys of all TAs are generated according to the public parameters issued by RTA, and each TA further generates the public parameters of its domain for the RSUs. All RSUs in the domain calculate their own public and private keys in terms of the public parameters issued by TA.

The proposed scheme is composed of the following protocols and methods: initial registration protocol, pseudonyms generation and credential acquisition protocol, pseudonyms resolution and revocation protocol, LTC resolution and revocation protocol, CRL construction, consistency and resolution.

A. INITIAL REGISTRATION PROTOCOL

When the OBU holds its LTC issued offline by the vehicle administration, it can access VANETs after it completes the initial registration process with the N-TA through the secure channel. At the same time, the OBU will receive $crdl$ issued by the N-TA.

As shown in Figure 5, OBU and N-TA execute initial registration protocol as below.

1) OBU generates a pseudonym request interval $[t_s, t_e]$ according to the general fixed policy proposed in [25], i.e., each TA specifies a common fixed interval and all pseudonyms issued in its domain have a lifetime aligned to the system clock. OBU calculates the interval in terms of the fixed interval Γ_{P3} given by TA.
2) OBU registers with N-TA through a secure channel. OBU sends LTC and $[t_s, t_e]$ to N-TA.
3) N-TA encrypts OBU's real ID to generate the initial pseudonym V_{ID} of the OBU and the corresponding private key s_v according to the system parameters. After that, a "credential identifiable key" (IK_{crdl}) is created to bind the credential to the vehicle's certificate: $IK_{crdl} = h(C||t_s||t_e||Rnd_{IK_{crdl}})$, where $C = Enc\_K\{V_{ID}, exp\}$ and $Rnd_{IK_{crdl}}$ is the random number generated by N-TA for this credential, exp is the expiration of LTC. Then N-TA generates $crdl$. $crdl$ includes χ and $Sign(SK_{N-TA}, \chi)$, where $\chi \leftarrow (C, IK_{crdl}, t_s, t_e)$ and SK_{N-TA} is the private key of N-TA.
4) N-TA sends $V_{ID}, s_v, crdl, Rnd_{IK_{crdl}}$ to OBU through the secure channel.

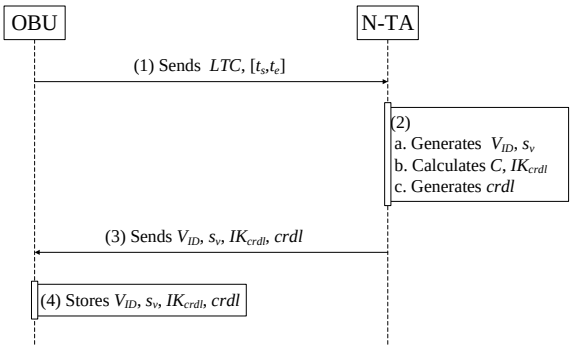


FIGURE 5. Initial registration protocol.

B. PSEUDONYMS GENERATION AND CREDENTIAL ACQUISITION PROTOCOL

When the OBU has obtained its V_{ID}, s_v and $crdl$, it will use them to interact with the RSU to obtain pseudonyms. The protocol described in this section is based on the secure V2I protocol. After the RSU completes the V2I authentication with the OBU as shown in Figure 6, the RSU and the OBU establish a secure channel.

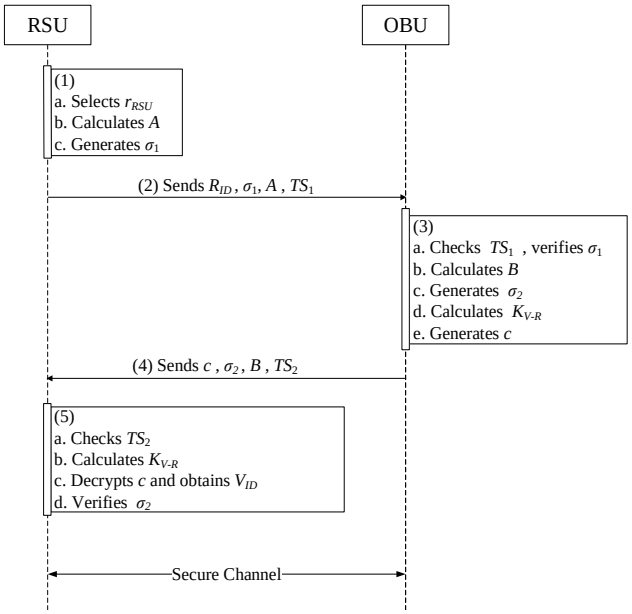


FIGURE 6. Initial V2I authentication protocol.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027718, IEEE Access

TABLE 1. Symbol and Definition

Symbol	Definition
V_{ID}	The initial pseudonym of OBU
R_{ID}	The identity of RSU
s_v	The initial private key of OBU
$crdl$	The anonymous credential of OBU
$Rnd, GenRnd()$	Random number and random number generation function
IK_A	The identifiable key of A
exp	The expiration of long-term certificate
$Enc\_K(m)$	Using the symmetric key K to encrypt message m
σ	Digital signature
t_s, t_e	The start/end timestamp
TS	The current timestamp
$nonce$	Temporary random number
$h(\cdot), h^k(\cdot)$	One-way hash function, hash function (k times)
H_i	Hash function
$\|\|$	Concatenation of messages
K_{V-R}	Shared secret key between OBU and RSU
G, p	The public primes in DH key agreement
$Sign(sk, m)$	Using the private key sk to sign message m
$Verify(pk, m)$	Using the public key pk to verify message m
$Sign\_BLMQ\_SK_A(m)$	Using the private key of entity A to sign message m through BLMQ signature mechanism
SN	Pseudonym serial number
P_v	Pseudonym of OBU
pk_v, sk_v	Pseudonym public key and private key of OBU
$Cert_v$	Pseudonym certification of OBU
Γ	Interval to issue time-aligned pseudonym
Γ_{CRL}	Interval to release CRL
τ_P	Period of validity of pseudonym

1) When OBU moves to the wireless communication range of the accessible RSU, the V2I authentication protocol will be executed. RSU generates $\{R_{ID}, \sigma_1, A, TS_1\}$, where σ_1 is the BLMQ signature and TS_1 is the timestamp. RSU randomly selects r_{RSU}, calculates $A = G^{r_{RSU}} \bmod p$, and generates the signature σ_1=$Sign\_BLMQ\_SK_{RSU}\{A, TS_1\}$.
2) RSU periodically broadcasts $\{R_{ID}, \sigma_1, A, TS_1\}$.
3) When OBU receives the broadcast message, it first checks whether TS_1 is fresh. If TS_1 is fresh, OBU continues to use R_{ID} to verify σ_1. If the verification is successful, OBU generates the signature σ_2=$Sign\_BLMQ\_SK_{s_v}\{B, TS_2\}$, where r_{OBU} is randomly selected and $B = G^{r_{OBU}} \bmod p$. Then OBU calculates the shared key K_{V-R} with RSU: $K_{V-R} = A^{r_{OBU}} \bmod p$. OBU uses K_{V-R} to generate $c = Enc\_K_{V-R}(V_{ID})$.
4) OBU sends c, σ_2, B, TS_2 to RSU.
5) After receiving the message from OBU, RSU checks if TS_2 is fresh. If TS_2 is fresh, RSU calculates the shared key $K_{V-R} = B^{r_{RSU}} \bmod p$ and uses K_{V-R} to decrypt c to obtain V_{ID} . Then RSU uses V_{ID} to verify σ_2 , if the verification is successful, OBU is regarded as a legal one, otherwise RSU will reject the access request from OBU.

If the above verification is successful, the RSU and the OBU can establish a secure channel by negotiating a shared key. The shared key is created by the Diffie-Hellman key agreement approach. Through the secure channel, the RSU sends pseudonyms, pseudonym certificates, and the corresponding public and private keys for the OBU. As shown in Figure 7, the steps of pseudonym generation protocol are as follows.

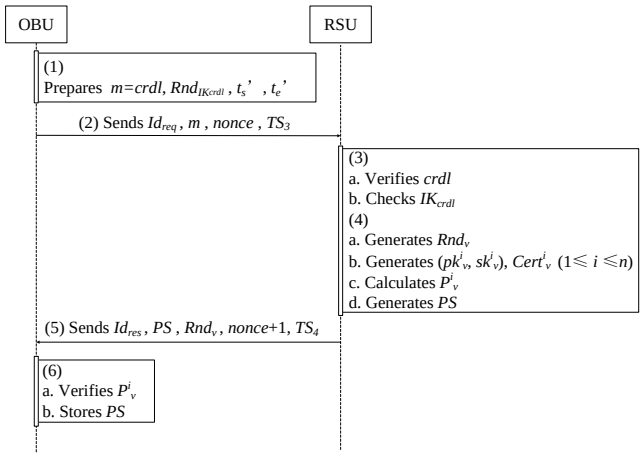


FIGURE 7. Pseudonym generation protocol.

1) OBU generates a pseudonym request message m: $m = crdl, Rnd_{IK_{crdl}}, t'_s, t'_e$, where t'_s and t'_e are the start timestamp and the end timestamp of the actual pseudonym request interval.
2) Then OBU sends $\{Id_{req}, m, nonce, TS_3\}$ to RSU through the secure channel, where $nonce$ is a random value freshly generated by OBU.
3) After receiving the request, RSU first uses the shared key with OBU to decrypt the request message and verifies the validity of $crdl$:$Verify(PK_{N-TA}, crdl)$, where PK_{N-TA} is the public key of the N-TA. Af-

ter RSU verifies that the OBU's credential is valid, it checks whether the actual period of the requested pseudonyms (i.e., $[t'_s, t'_e]$) is within the period specified in the credential (i.e., $[t_s, t_e]$) and the credential is indeed held by OBU by verifying if the equation $IK_{crdl} == h(C||t_s||t_e||Rnd_{IK_{crdl}})$ holds.

4) RSU generates random number: $Rnd_v \leftarrow GenRnd()$, several public and private key pairs(pk_v^i, sk_v^i) based on ECDSA or RSA and the corresponding public key certificates $Cert_v^i$ for OBU, where i= 1,...,n and n is the number of pseudonyms distributed each time by RSU. All the public key certificates are signed by RSU with its private key SK_{RSU}. Then RSU generates "pseudonym identifiable key"$\left(IK_{P_v^i}\right)$ to bind pseudonyms to OBU's credential: $IK_{P_v^i} = h(IK_{crdl}||pk_v^i||t_s^i||t_e^i||h^i(Rnd_v))$. RSU implicitly associates a batch of pseudonyms belonging to each OBU by calculating the pseudonym sequence number SN, i.e., when i=1, $SN^i = h(IK_{P_v^i}||h^i(Rnd_v))$, and i= 2,...,n, $SN^i = h(SN^{i-1}||h^i(Rnd_v))$. Afterwards the RSU generates pseudonyms for OBU: $P_v^i \leftarrow (SN^i, pk_i, IK_{P_v^i}, t_s^i, t_e^i)$.
5) RSU sends $\{Id_{res}, PS, Rnd_v, nonce+1, TS_4\}$ to OBU through the secure channel, where $PS = \{(P_v^1, pk_v^1, sk_v^1, Cert_v^1), ..., (P_v^n, pk_v^n, sk_v^n, Cert_v^n)\}$.
6) After receiving the response message from RSU, OBU first recovers the message with the shared key, and then verifies $IK_{P_v^i}$ by verifying whether the equation $h(IK_{crdl}||pk_v^i||t_s^i||t_e^i||h^i(Rnd_v))==IK_{P_v^i}$ holds. If the verification is successful, OBU stores PS in the TPD.

If the pseudonym request time in the credential is about to expire, the OBU sends the current $crdl$ and the new request time interval $[t_{s'}, t_{e'}]$ to TA in the domain to apply for a new credential through the RSU. After the TA validates $crdl$, a new credential is generated to replace $crdl$ that will soon be unavailable.

When the vehicle travels across domains, the OBU does not need to repeat the registration process with the E-TA. The OBU presents $crdl$ and applies for a new "native" credential $crdl'$. As shown in Figure 8, the steps are described in detail as follows.

1) OBU sends $\{Did_{N-TA}, \sigma_3, crdl, B, TS_5\}$ to the first RSU accessed after entering domain B, where Did_{N-TA} is N-TA's domain ID and σ_3=$Sign\_BLMQ\_SK_{s_v}\{crdl, B, TS_5\}, B = G^{r_{OBU}} \bmod p$.
2) After receiving the message from OBU, RSU finds the identification of other domain Did_{N-TA}. RSU temporarily saves B and then forwards the message from OBU to E-TA.
3) After getting the message, E-TA communicates with N-TA according to Did_{N-TA}. E-TA sends $\{\sigma_3, crdl, B, TS_5\}$ to the N-TA.
4) N-TA checks the validity of $crdl$ and verifies σ_3. If the verifications are both successful, N-TA returns C, t_s, t_e to the E-TA.
5) E-TA generates a new credential $crdl'$ for OBU by selecting a new $Rnd_{IK_{crdl'}}$ and using its private key SK_{E-TA} to generate the signature. E-TA then returns $crdl', Rnd_{IK_{crdl'}}$ to RSU.
6) After receiving the return message, RSU temporarily saves $crdl', Rnd_{IK_{crdl'}}$. Then it sends $\{R_{ID}, \sigma_4, A, TS_6\}$ to OBU, where σ_4=$Sign\_BLMQ\_SK_{RSU}\{A, TS_6\}, A = G^{r_{RSU}} \bmod p$. Then, RSU calculates the shared key which is used to establish the secure channel: $K_{V-R} = B^{r_{RSU}} \bmod p$.
7) When OBU receives $\{R_{ID}, \sigma_4, A, TS_6\}$, it first checks whether TS_6 is fresh. If TS_6 is fresh, OBU continues to verify σ_4. If the verification is successful, OBU calculates the shared key: $K_{V-R} = A^{r_{OBU}} \bmod p$.

After completing the above steps, the OBU and the RSU in the external domain establish a secure channel. The RSU sends the temporarily stored $crdl', Rnd_{IK_{crdl'}}$ of the OBU and the new pseudonyms, pseudonym certificates, and corresponding public and private keys to the OBU through the secure channel.

C. PSEUDONYMS RESOLUTION AND REVOCATION PROTOCOL

When OBU has malicious behavior in VANETs, such as spreading disloyal traffic information, the pseudonyms (including those not expired) of the OBU should be revoked. The process of pseudonym resolution and revocation is described in detail as follows.

1) When OBU_j receives the message m sent by OBU_i and considers m to be a false message, OBU_j generates a $report$ including the message m, the pseudonym, pseudonym certificate, and R_{ID} used to send m.
2) OBU_j sends the $report$ to the nearest RSU (RSU_n).
3) After receiving the $report$, RSU_n needs to check whether message m is a malicious message or not. If so, RSU_n broadcasts revocation information, and further transfers the $report$ to TA. If the pseudonym and certificate are generated by RSU_n, TA checks message m and the legality of OBU_i. Otherwise, RSU_n sends the $report$ to the RSU (RSU_p) that generated the pseudonym and certificate for OBU_i according to R_{ID}.
4) After getting the $report$, RSU_p double-checks message m. If m is malicious, RSU_p then updates the contents of CRL to revoke all available pseudonym certificates of OBU_i. For LTC resolution, RSU_p sends the corresponding C to TA.

D. LTC RESOLUTION AND REVOCATION PROTOCOL

When TA receives revocation information of the OBU to be revoked from any RSU in the domain, two situations should be taken into account.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027718, IEEE Access

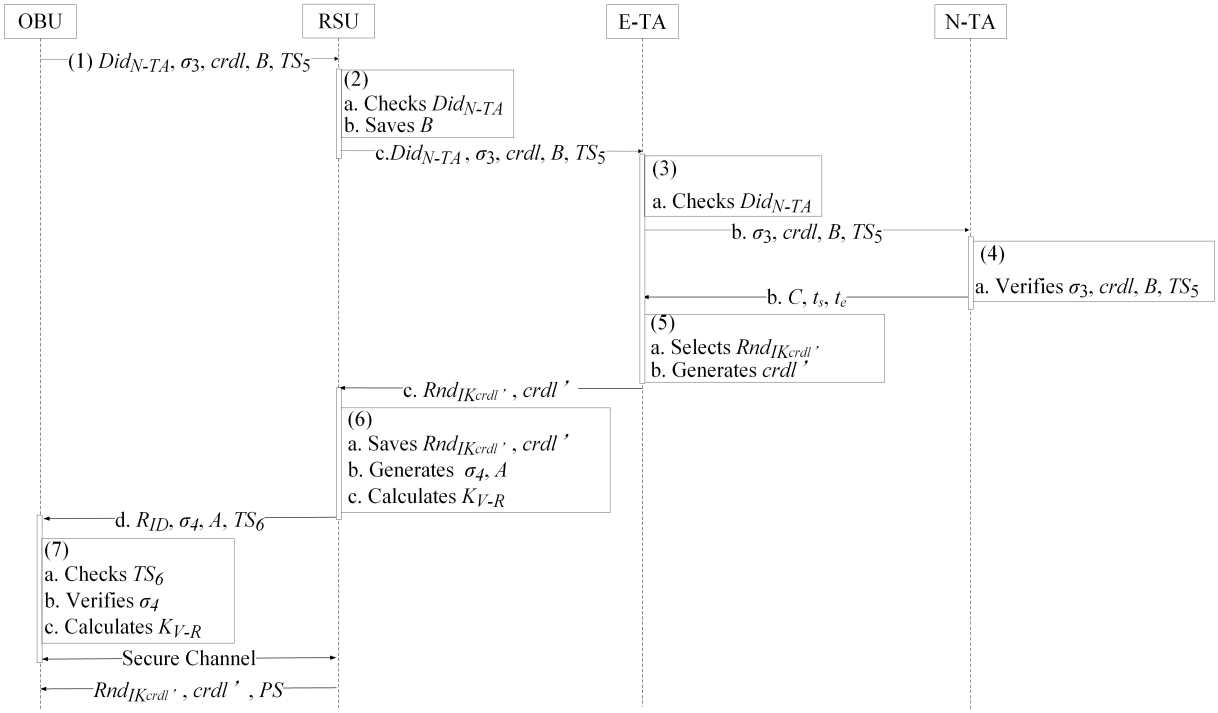


FIGURE 8. Credential acquisition protocol.

Each TA maintains a list that records the Did corresponding to C and the $crdl$ issued according to C. TA first searches the list according to C to check if Did is the native domain ID. If so, TA can directly recover the real identity of the OBU through decryption, and then revoke the LTC of the vehicle. If Did is not the native domain ID, TA needs to communicate with the TA in the domain specified by Did, informing it to resolve the real identity of the OBU and revoke the LTC.

All TAs send invalid or replaced $crdl$ to all RSUs in the domain at any time, and send revoked LTC to other TAs.

E. CRL CONSTRUCTION

When a vehicle is to be deported, the RSU executes a CRL construction process comprising the following steps.

1) RSU appends the following data to each batch of revoked pseudonyms: (i) the sequence number of the first revoked pseudonym in the implicitly associated pseudonym chain (SN^k), (ii) the hash value $(h^k_{Rnd_v})$, (iii) the number of remaining pseudonyms in the batch (x).
2) The RSU within a certain Γ_{CRL} will obtain the extended CRL with a Bloom filter.

F. CRL CONSISTENCY AND RESOLUTION

In our scheme, each RSU releases revocation information at any time to notify vehicles of any new revocation event. Vehicles can receive the latest CRL timely through RSUs. In addition, TA will collect and check extended CRL generated by all the RSUs in its domain at all times and issue integrated authoritative CRL at fixed intervals. The two CRL are consistent in contents and BF test results.

By performing the BF test, the vehicle can verify whether the pseudonym of the other is on the CRL. Upon receiving and verifying the CRL, for the operation of parsing it, each vehicle calculates the hash value x times by SN^k and $h^k_{Rnd_v}$ of the revoked pseudonym: $SN^{i+1}{=}h(SN^i||h(h^i_{Rnd_v}))$, $i = \{k, k+1, k+2, \ldots, k+x-1\}$, and calculates all revoked pseudonym sequence numbers. Reversed entries stored in local repository can be searched for in $O(log(n))$ time complexity [29]. The vehicle could locally generate a BF at a constant computational cost $(O(1))$ [18].

V. SECURITY ANALYSIS

In this section, the security analysis of the proposed scheme is mainly conducted from two aspects: satisfying the security and privacy requirements and resisting attacks.

A. SECURITY AND PRIVACY FEATURES

This subsection analyzes the security of the proposed scheme in detail to show that our scheme is capable of achieving desired design objectives as follows.

Authentication and confidentiality. The authentication scheme adopts BLMQ signature mechanism, and the security and correctness of the proposed scheme can be completely and effectively proved in V-B. The OBU and RSU that have completed authentication protocols will obtain a secure shared key for subsequent communication. The shared key is generated using a secure key sharing algorithm. Any malicious node cannot obtain the correct key, thus ensuring secure

communication. Moreover, the proposed scheme can achieve V2X authentication without exposing OBU's identity. In the first mutual authentication process between OBU and RSU, OBU presents the initial pseudonym issued by N-TA. While in the authentication process between OBUs, the new anonymous identity issued by RSU is used to avoid exposing the relevant information about the real identity. When the vehicle travels across domains, the vehicle does not need to let the TA of the external domain know its real identity. As for CRL, the authenticity and integrity of the CRL published by RSU can be verified by $CRL\ signer's$ signature.

Authorization and access control. As a Trusted Third Party (TPP), N-TA certifies and authorizes OBU, and issues $crdl$ for OBU so that OBU can request pseudonyms from any RSU by presenting $crdl$. Even if driving to an external domain, the current $crdl$ can help the OBU obtain a new available one without exposing its real identity information to entities in other domains. RSU then verifies the credential and provides pseudonyms for the OBU based on the previously established trust.

Unforgeability, non-repudiation and revocation. In our scheme, only legal OBU can obtain the pseudonym certificate and the corresponding private key to sign messages. Since all (pk_v^i, sk_v^i) and $Cert_v^i$ of OBU need to be generated by the cooperation of TA and RSU. No OBU can generate the keys and certificates on its own, nor can it forge other's signatures.

Once a dispute occurs and the LTC of the OBU needs to be revealed, our scheme enables traceability. Each TA can recover the real identity of the malicious OBU directly or through cooperation with relevant TA from its anonymous identity. See details in section IV-A, acquiring $crdl$ requires the vehicle to submit LTC containing real identity information to TA and all $crdl$ are acquired and replaced on a trusted and secure channel, and the pseudonym acquisition requires a valid $crdl$. TA and RSU compute the credential and the pseudonym identifiable key respectively to bind them to the corresponding LTC and the credential. Moreover, since the CRL with a BF is signed by RSU, no RSU can deny that it contains any pseudonym sequence number. The correctness of the CRL can also be verified by OBU through the authoritative CRL from TA. The segregation of duties between TA and RSU provides conditional anonymity and enables the vehicle to be revoked when misbehavior is detected. In addition, each request that gets a credential needs to be authenticated to prevent abuse of the mechanism by signing with the currently valid pseudonym of the vehicle.

Anonymity and unlinkability. In our scheme, pseudonym certificates are generated by RSU according to anonymous credentials. These certificates do not contain any identifiable information and cannot be linked to a particular OBU or to other pseudonym certificates. Only N-TA is able to decrypt C and recover the real identity of the OBU. Moreover, C is the encryption result of the real identity, so it reveals no identity information of the OBU to anyone except N-TA.

After OBU is connected to RSU, it obtains multiple pseudonyms issued by the RSU. In V2V authentication and communication, the unexpired pseudonyms used by OBU are not relevant to other pseudonyms, so the attacker cannot perform correlation analysis on multiple messages, i.e., given P_v^i and P_v^{i+1} , it is computationally hard to decide that they are correspondence to the same OBU without knowing SN^i and $H_{Rnd_v}^i$.

According to the proposed protocol, vehicle hides its real identity even when it crosses domains. The request interval for pseudonyms of the vehicle falls within the fixed Γ_{P3}, and the validity period of the pseudonym is aligned, so the time information cannot be used to link two consecutive pseudonyms. In addition, since hash chains are used in the pseudonym publishing process, it is not feasible to link a pseudonym with the previous expired pseudonyms. Moreover, the random number Rnd_v makes the pseudonyms in OBU's pseudonym certificates totally different, which makes it infeasible for the attacker to get the linkability between OBU's previous pseudonym certificates. For honest but inquisitive RSU, time information may be inferred from pseudonyms or the context of CRL to link pseudonym sets and track the vehicle. However, all issued pseudonyms are aligned with the clock of the RSU, so pseudonyms are not distinguishable.

B. ATTACK RESISTANCE

In the attack model of the proposed scheme, different threats are considered. Specifically, it is semantically protected against both passive and active attacks. Let a passive attacker get an encrypted and pseudonymized message during the communication. In order to find the valid key, the attacker has to solve the hard mathematical problems. The shared key is generated by the Diffie-Hellman key agreement algorithm, which is secure enough in ITS. Moreover, to further enhance security, $nonce$ is also introduced. Therefore, without the key and the $nonce$, it is impossible for an attacker to eavesdrop the communication. For an active attacker, if he or she tries to insert a bogus message or alter the contents of the message as an external adversary, the verification of signatures is able to prevent the attacks happening. Furthermore, an external adversary cannot obtain any private information either since all the communication in the proposed scheme is encrypted and authenticated. If the attacker wants to generate the key pairs in real time, he or she should have prior knowledge of the parameters as elaborated in section IV-A. On the other hand, TA issues initial pseudonym to the vehicle in a secure channel. Therefore, the internal adversary cannot obtain the real identity of the vehicle. Similarly, after obtaining $crdl$ and pseudonyms, the attacker is unaware of the valid identity of a vehicle during V2X communication. Consequently, it is impractical to launch active attacks.

As for the security of the authentication, in the proposed scheme, it mainly depends on the initial V2I authentication which is based on IBS mechanism. Reviewing III-D, there is Theorem 1.

Theorem 1: If no polynomial time attacker $\mathcal{A}$ wins the game in III-D with at least advantage ε in time t after q_k

times of key extraction queries and q_s times of signature queries, the proposed scheme is secure under adaptive chosen message and identity attacks.

Proof: Reducing the description of Theorem 1 to q-SDHP, there is Theorem 2.

Theorem 2: Under the random oracle model [30], if there exists an adaptively chosen message and identity attacker $\mathcal{A}$ wins the game in III-D with advantage $\varepsilon \geq 10(q_s+1)(q_s+q_{h_2})/2^k$ within a time t after making q_{h_i} queries to random oracles $H_i(i=1,2)$ and q_s queries to the signing oracle, then, there exists an algorithm $\mathcal{C}$ that is able to solve the q-SDHP for $q=q_{h_1}$ in an expected time

$$t' \leq 120686 q_{h_1} q_{h_2}(t+O(q_s\tau_{bp}))/(\varepsilon(1-q/2^k))+O(q^2\tau_{mul}) \quad (1)$$

where τ_{bp} and τ_{mul} denote the cost of a pairing evaluation and a scalar multiplication respectively.

It can be proved that in the mechanism of the proposed scheme, $\mathcal{C}$ can provide $\mathcal{A}$ with a perfect simulation and solve q-SDHP through interaction with $\mathcal{A}$. The mathematical proof depends on the forking lemma and is given in detail in [23]. The q-SDH assumption holds, that is, q-SDHP is difficult to solve, then there is no polynomial time attacker $\mathcal{A}$ wins the game in III-D with at least advantage ε in time t. Therefore, Theorem 1 is proved. The proposed scheme can be proved to be existentially unforgeable under adaptive chosen message and identity attacks.

Moreover, the scheme can also defend against other types of attacks.

Impersonation attack. In the initial authentication process between the OBU and the RSU, the private key for signing and the public key for verifying signature of the OBU are both calculated by N-TA, and issued to the vehicle through the secure channel, so the attacker cannot impersonate other nodes to forge signatures.

Tampering attack. According to the scheme of this paper, the messages are signed separately in the mutual authentication phase between two OBUs or between OBU and RSU. If the message is tampered, it will lead to verification failure and effectively prevent tamper attack.

Replay attack. In our scheme, OBU and RSU use in conjunction with $nonce$ and timestamp TS checking, which can effectively thwart replay attacks.

Spoofing attack. Since there is a secure channel between OBU and TA, it is impossible for an attacker to intercept LTC sent from the OBU and any available $crdl$ and key pairs from TA. Furthermore, during V2X communication, signature ensures the integrity and tamper-proof of information. Even if the attacker successfully intercepts the message, he/she cannot modify the content of the message without the knowledge of both parties.

Key stealing attack. After the mutual authentication between OBU and RSU, RSU issues multiple anonymous identities and corresponding signature keys to OBU. The keys and pseudonyms will be encrypted with the shared key K_{V-R} , which effectively prevents the keys from being stolen by attackers during key transmission.

Sybil and DoS attacks. When a vehicle requests a credential from TA, TA issues only one valid credential to the vehicle, preventing the vehicle from requesting more valid pseudonyms at the same time. In addition, the credential is implicitly bound to a specific TA (N-TA), so it cannot be used multiple times. RSU gives a pseudonym that does not overlap the validity period of the vehicle, and no vehicle can provide more than one valid pseudonym at any time, so Sybil attacks can be defended. We use a nonce (a unique string whose value is valid only for a short time) that is included in the payload to guard against DoS attacks and our scheme has an advantage for defending DDoS attacks through a significant reduction in CRL size.

Through the above analysis, the proposed scheme is able to meet the security and privacy requirements of VANETs well.

VI. PERFORMANCE ANALYSIS

In this section, the performance of the proposed scheme in terms of anonymous identity authentication efficiency and pseudonym revocation efficiency are analyzed.

A. ANONYMOUS IDENTITY AUTHENTICATION EFFICIENCY

The proposed scheme is compared with CPAS [36], ACPN [37], and PACP [38] in computational cost for the authentication efficiency analysis. The computational cost is calculated by the related network entities in the V2I and V2V authentication process. With the adoption of edge computing, RSUs typically have abundant computing resources and therefore the computing overhead of RSUs is not considered in this paper.

The following is a comparative analysis of the computing overhead of OBU under different schemes. For convenience of comparison, in our scheme, we calculate the overhead of the OBU according to RSA signature mechanism during signature and verification. In the authentication process of the schemes, the main computing operations include: bilinear pairing operation (bp), map-to-point hash operation (mtp), hash function (h), point addition (pa), point multiplication (pm), scale multiplication (mul), exponentiation in G_2 of the bilinear pairing (ep2) and RSA sign (RSA_s), RSA verification (RSA_v) and RSA encryption (RSA_e). Let T_x denote the calculation cost of operation x. Compared with the above operations, the calculation cost of T_h, T_{pa} and T_{RSA_v} can be omitted according to [31], [32], and according to [38], the computational overhead of RSA encryption is the same as that of RSA verification. In addition, by summarizing the experimental results and conclusions from [33]–[35], we can obtain the following relationships of the execution time(ms) of the operations, as in (2)-(6).

$$T_{bp} = 1.6(ms) = 3T_{RSA_s} \quad (2)$$

$$T_{mtp} = 1.5T_{RSA_s} = 0.8(ms) \quad (3)$$

$$T_{pm} = 1.5T_{RSA_s} = 0.8(ms) \quad (4)$$

$$T_{ep2} = 1.125T_{RSA_s} = 0.6(ms) \quad (5)$$

$$T_{mul} = T_{RSA_s} = 0.533(ms) \quad (6)$$

In the V2I authentication protocol of the scheme proposed in section IV-B, the OBU verifies the BLMQ signature by checking whether the equation $h_{RSU} = H_2(A||TS_1, e(V_{RSU}, H_1(R_{ID})P + P_{pub})g^{-h_{RSU}})$ is held and generates a signature. The OBU generates a BLMQ signature$\{h_{OBU}, V_{OBU}\}$, where $x = g^{r_{OBU}}, h_{OBU} = H_2(B||TS_2, x), V_{OBU} = (r_{OBU} + h_{OBU})s_v$. In addition, the OBU also needs to calculate the shared keyK_{V-R}, which is equivalent to two RSA encryption operations. Therefore, the computational cost of the proposed scheme in the V2I authentication process is:

$$CC_{ours-V2I} = T_{bp} + 2T_{pm} + 2T_{ep2} + T_{mul} + 2T_{RSA_e} \quad (7)$$

In the V2V authentication process of our scheme, since all OBUs communicate with each other using pseudonyms, the OBU needs to verify the RSU's signature on the pseudonym certificate by checking whether $\{h_{RSU}, V_{RSU}\}$ is valid. After the above verification is successful, the OBU will use the other OBU's public key to verify the signed message through one RSA verification operation. The OBU also needs to generate its RSA. From the above analysis, it can be seen that the computational cost of our scheme in the V2V certification process is:

$$CC_{ours-V2V} = T_{bp} + T_{pm} + T_{ep2} + T_{mul} + T_{RSA_s} + T_{RSA_v} \quad (8)$$

In the V2I certification process of CPAS scheme, the OBU calculates the digital signature:$U_i = r_i \cdot P \in G_1$, $h_i' = H_3(PID_i, M_i, tt_i, T_i, U_i) \in Z_q^*$ and$V_i = h_i' \cdot S_i + r_i \cdot Q'$, where $H_3 : \{0,1\}^* \rightarrow {Z_q}^*$. In addition, the OBU needs to verify the digital signature from the RSU:$h_R = H_1(ID_R, T_R)$, $h_i = H_3(ID_R, M_i, tt_i, TR, U_i^R) \in Z_q^*$ and verify whether the equation$e(V_i^R, P) = e(h_i' \cdot (P_{pub} + h_R TR), Q) \cdot e(U_i^R, Q')$. Therefore, the computational cost of CPAS scheme in V2I certification process is:

$$CC_{CPAS-V2I} = 3T_{mtp} + 3T_{bp} + 7T_{pm} \quad (9)$$

In the V2V certification process of CPAS scheme, the OBU calculates the digital signature:$h_i = H_1(PID_i, T_i)$, ${h_i}' = H_3(PID_i, M_i, tt_i, T_i, U_i) \in Z_q^*$. Then the OBU checks if the equation $e(V_i, P) = e(h_i P_{pub} + {h_i}' h_R T_i, Q) \cdot e(U_i, Q')$ holds. From the above analysis, the computational cost of the CPAS scheme in the V2V authentication process is:

$$CC_{CPAS-V2V} = 3T_{mtp} + 3T_{bp} + 5T_{pm} \quad (10)$$

In the V2I authentication process of ACPN, the OBU generates a pseudonym: $PS_v = Time \parallel E_{PK}(ID_v) \parallel HR \parallel RSU$, where ID_v is encrypted using the RSA encryption algorithm. The OBU generates a signature:$r = e(P_1, P)$, $v = h(m, r)$, $u = v \cdot S_1 D + kP_1$. The OBU then verifies the signatures by calculating $r = e(u, P) \cdot e(H(ID), -Q_T A)$ and checking whether the equation $v = h(m, r)$ is established, where $H : \{0,1\}^* \rightarrow G_1$. Therefore, the computational cost of the V2I authentication process of the ACPN scheme is:

$$CC_{ACPN-V2I} = 5T_{mtp} + 5T_{bp} + 4T_{pm} + T_{RSA_e} \quad (11)$$

In the V2V authentication process of ACPN, the OBU generates signature $\sigma = H_4(m, R)x + r$ and verifies signature (S, σ, R) by checking whether the equation $e(P_{pub}, S) = e(P \cdot H_4(m, R)R, Q_{ID})$ holds, where $H_4 : \{0,1\}^* \times G_1 \rightarrow {Z_q}^*$. It can be seen that the computational cost of the ACPN scheme in the V2V authentication process is:

$$CC_{ACPN-V2V} = 2T_{mtp} + T_{bp} + 3T_{pm} \quad (12)$$

In the V2I authentication process of the PACP scheme, the OBU generates an IBS signature and verifies the signature sent by the RSU. Since the author did not specify a specific signature algorithm, it is assumed to be the BLMQ signature. In addition, the OBU needs to perform encryption and decryption operations as follows:$\lambda_{(a,i)}^j = e(\tau_{(a,i)}^j, \sigma_j aP)$, ρ=$H_7(k, M)$, $C = \langle H_5(\rho P) \oplus (\lambda_{(a,i)}^j)k, e(P, \sigma_j aP)k, M \oplus H_6(e(\sigma_j aP, H_5(\rho P)P))\rangle$, $\Gamma_{(a,i)}^j = U \oplus VS_{(a,i)}^j$, $M' = W \oplus H_6(e(\sigma_j aP, H_5(\rho P)P)$, where $H_5 : G_1 \rightarrow \{0,1\}^*$, $H_6 : G_2 \rightarrow \{0,1\}^*$ and $H_7 : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$. Therefore, the computational cost of the PACP scheme in the V2I authentication process is:

$$CC_{PACP-V2I} = 5T_{bp} + 17T_{pm} + 2T_{ep2} + T_{mul} \quad (13)$$

In the V2V authentication process of PACP, the calculation process of the OBU is basically consistent with that in V2I. The OBU needs to generate a signature and verify the signature issued by the RSU by performing two map-to-point hash operations, two bilinear pairing operations, and one point multiplication. According to the above analysis, the computational cost of PACP scheme in the V2V certification process is:

$$CC_{PACP-V2V} = 5T_{bp} + 15T_{pm} + 2T_{ep2} + T_{mul} \quad (14)$$

The computational cost of the proposed scheme is evaluated and presented in Table 2 and Table 3, respectively. Since the time of the symmetric encryption operation (T_{enc}) is microsecond [42], it can be ignored. The computational costs of the different schemes for V2I and V2V authentication are shown in Figure 9. It should be noted that according to the previous analysis, we do not calculate the cost of T_{RSA_e} and T_{RSA_v} here. The comparative analysis shows that in the V2I and V2V authentication process, the proposed scheme owns lower computational cost than the other three schemes.

In order to further demonstrate a comprehensive comparison between our scheme and the existing schemes, a comparative analysis of the related schemes is shown in Table 4. It can be seen from the discussion in related work and the comparative analysis of performance that our scheme is more efficient than [7], [10], [14], [36]–[38], [45]. Though [42], [44], [46] also show obvious advantages in efficiency, [42]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027718, IEEE Access

Ours	Operation	Computational time(ms)
Message encryption	T_{enc}	-
Signature generation	T_{pm}+T_{ep2}+2T_{RSA_e}	1.4
Message decryption	-	-
Signature verification	T_{bp}+T_{pm}+T_{ep2}+T_{mul}	3.533

TABLE 2. Computational cost in the V2I authentication

Ours	Operation	Computational time(ms)
Message encryption	-	-
Signature generation	T_{RSA_s}	0.533
Message decryption	-	-
Signature verification	T_{bp}+T_{pm}+T_{ep2}+T_{mul}+T_{RSA_v}	3.533

TABLE 3. Computational cost in the V2V authentication

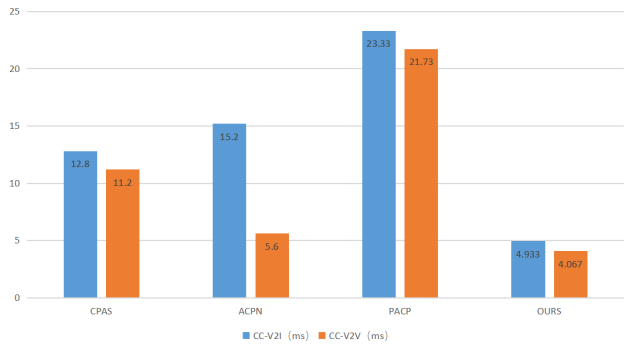


FIGURE 9. Comparision of computational cost.

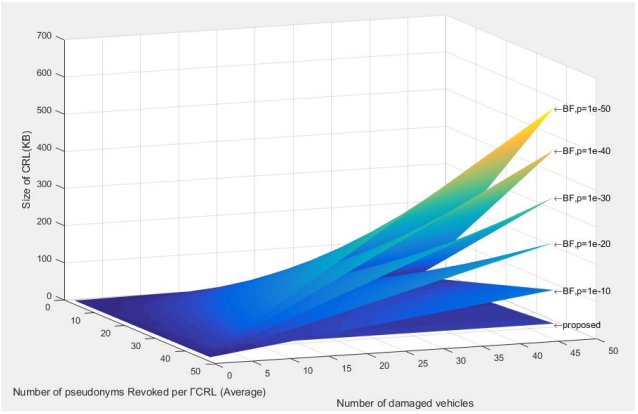


FIGURE 10. CRL size comparison.

has key escrow problem, and those three all have the threat of Sybil attack. It is worth mentioning that although [46] does not address cross-domain issues, its distributed framework can also be extended to adjust to this scenario.

B. PSEUDONYM REVOCATION EFFICIENCY

1) Distribution Efficiency of Revoked Pseudonyms

Before comparative analysis, we will first give a scenario that there are 1 million cars in VANETs. On average, each vehicle travels for four hours. Assuming Γ=30 minutes and τ_P=5 minutes, then each Γ needs 6 pseudonyms, i.e., 48 pseudonyms for each vehicle per day, and all these pseudonyms are issued in time at non-overlapping intervals [39]. Assume that one percent of these vehicles need to be expelled from the system for security reasons. Therefore, the revocation information published every day contains 480,000 entries, so the CRL size is about 14.6MB (each pseudonym has a 256-bit serial number). By implicitly binding the pseudonyms belonging to each OBU, one entry can be distributed with some additional information for a batch of revoked pseudonyms in Γ, with a total of 8 entries distributed for each revoked vehicle instead of 48 entries. Therefore, the CRL contains 80,000 entries, each with 256-bit serial number and 256-bit additional information, and the CRL size will be significantly reduced to about 4.9 MB.

2) CRL Size

Our scheme is improved on the basis of C^2RL scheme [40], which prevents vehicles from receiving a large amount of revocation information unrelated to their own travel through time alignment, and realizes batch revocation of pseudonyms while ensuring unlinkability through implicit binding of pseudonyms [47].

In the C^2RL scheme, by compressing the revocation information, the size of the CRL is given by $size = -\frac{N \times M \times \ln p}{(\ln 2)^2}$ [41], where N is the total number of damaged vehicles, M is the average number of pseudonyms revoked by each vehicle in each Γ_{CRL}, and p is the probability of false positive. As shown in Figure 10, if N is known, the size of the CRL increases linearly with M. Under the proposed scheme, it is adequate to publish only one entry to revoke all pseudonyms of the misbehaving vehicle within one Γ_{CRL} time interval. The size of the CRL in each Γ_{CRL} is given by $(256+256) \times N$, where 256 bits are used for pseudonym sequence numbers and 256 bits are used for their corresponding hash values. In addition, only when the probability of false positive increases can C^2RL scheme be comparable with the proposed scheme in the size of the CRL. For example, if M=10, the false positive probability of the C^2RL scheme should be 10^{-10} to achieve a size of the CRL equivalent to the proposed scheme. Moreover, when $p = 10^{-30}$, the size of the CRL in our scheme will be reduced by more than 2 times compared with the C^2RL scheme. Through the above comparative analysis, it can be shown that our scheme has a good performance in reducing the CRL size.

VII. CONCLUSION

This paper proposes a secure and efficient identity-based anonymous authentication scheme that can support cross-domain authentication of vehicles. Pseudonyms are adopted to strengthen the privacy protection of vehicle users. By introducing a fixed-interval pseudonym acquisition policy, all the pseudonyms issued in a domain have a lifetime aligned

TABLE 4. Comprehensive comparison

Research paper	Computational cost	Communication overhead	Key escrow	Group management	Replay attack	Sybil attack	Cross-domain
[7]	High	High	Yes	No	Yes	Yes	No
[10]	Medium	High	Yes	Yes	Yes	No	No
[14]	Medium	Medium	Yes	Yes	No	Yes	No
[36]	Medium	Medium	No	No	No	No	No
[37]	Medium	Medium	No	No	No	No	No
[38]	High	High	No	No	Yes	No	No
[42]	Low	Low	Yes	No	No	Yes	No
[44]	Low	Low	No	No	No	Yes	No
[45]	Medium	High	No	No	Yes	No	No
[46]	Low	Low	No	No	No	Yes	No
Ours	Low	Low	No	No	No	No	Yes

with the TA and RSUs, which can prevent linking of the pseudonyms. All the pseudonyms remain unlinked when the revocation event occurs, thereby improving the privacy protection strength. Bloom filter is further employed to optimize CRL. Moreover, pseudonyms are revoked in batches in terms of the pseudonym sequence number and a hash value in the CRL, which is able to enhance the performance of the scheme. Security and performance analysis demonstrate that the proposed scheme is robust and efficient.

The future work is to present a more effective pseudonym generation and changing mechanism for VANETs. The pseudonym generation mechanism will not depend on RSU or other trusted authority to issue public and private keys in advance. OBU may depend on the certificateless pseudonym scheme to generate random pseudonyms independently. Certificates or secret keys are no longer necessary, which will significantly reduce the deployment and management costs. Moreover, the performance of pseudonym revocation will be further improved by replacing CRL by employing non-interactive zero-knowledge.

VIII. ACKNOWLEDGMENT

This work was supported by the Fundamental Research Funds for the Central Universities under Grant Number: N2017002 and N2024005-1.

REFERENCES

[1] "IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages," in IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013) , vol., no., pp.1-240, 1 March 2016

[2] "ETSI TS 102 941:Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," in: Standard, European Telecommunications Standard Institute 2019, France, Feb. 2019.

[3] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," in IEEE ITST, Sophia Antipolis, Jun. 2007.

[4] "Preparing Secure Vehicle-to-X Communication Systems - PRESERVE," Accessed Date: 22-November-2019. [Online]. Available: http://www.preserve-project.eu/

[5] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A Security Credential Management System for V2V Communications," in IEEE VNC, Boston, MA, USA, pp. 1–8, Dec. 2013.

[6] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," IEEE Communications Magazine, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[7] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007.

[8] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw., New York, NY, USA, 2007, pp. 19–28.

[9] C. D. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A robust conditional privacy-preserving authentication protocol in VANET," in Security and Privacy in Mobile Information and Communication Systems (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 17. Berlin, Germany: Springer, 2009, pp. 35–45.

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

[11] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," Comput. Commun., vol. 71, pp. 50–60, Nov. 2015.

[12] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," IEEE Trans. Veh. Technol., vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[13] 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.

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

[15] H. J. Jo, I. S. Kim and D. H. Lee, "Reliable Cooperative Authentication for Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 4, pp. 1065-1079, April 2018.

[16] Papadimitratos P , Mezzour G , Hubaux J P, "Certificate Revocation List Distribution in Vehicular Communication Systems," in proceedings of the fifth ACM international workshop on Vehicular Inter-networking (VANET '08), Association for Computing Machinery, New York, NY, USA, 86–87, 10.1145/1410043.1410062.

[17] Haas J J , Hu Y C , Laberteaux K P, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in proceedings of the sixth ACM international workshop on Vehicular Inter-networking (VANET '09), Association for Computing Machinery, New York, NY, USA, 89–98, 10.1145/1614269.1614285.

[18] J. J. Haas, Y. Hu and K. P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 595-604, March 2011.

[19] Laberteaux K P , Haas J J , Hu Y C, "Security certificate revocation list distribution for VANET," pp. 88–89, Jan. 2008, 10.1145/1410043.1410063.

[20] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," in IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[21] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, Mar.-Apr. 2017.

[22] Boneh D , Franklin M, "Identity Based Encryption from the Weil Pairing," SIAM J. Comput. 32, 3 (March 2003), 586–615, 10.1137/S0097539701398521.

[23] Barreto P S L M, Libert B, Mccullagh N and Quisquater J, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from

Bilinear Maps," International Conference on Theory and Application of Cryptology and Information Security, Springer-Verlag, 2005:515-532.

[24] M. Mitzenmacher, "Compressed Bloom filters," in IEEE/ACM Transactions on Networking, vol. 10, no. 5, pp. 604-612, Oct. 2002.

[25] M. Khodaei and P. Papadimitratos, "Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems," in proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet (IoV-VoI '16). Association for Computing Machinery, New York, NY, USA, 7–12, 10.1145/2938681.2938684.

[26] K. Rabieh, M. Pan, Z. Han and V. Ford, "SRPV: A Scalable Revocation Scheme for Pseudonyms-Based Vehicular Ad Hoc Networks," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6.

[27] N. Bißmeyer, "Misbehavior Detection and Attacker Identification in Vehicular Ad-Hoc Networks," 2014.

[28] F. Schaub, Z. Ma and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," 2009 International Conference on Computational Science and Engineering, Vancouver, BC, 2009, pp. 139-145, 10.1109/CSE.2009.135.

[29] Carlos Gañán, Jose L. Muñoz, Esparza O , Jorge Mata-Díaz and Alins J, "Toward Revocation Data Handling Efficiency in VANETs," 2012, pp. 80-90.

[30] Pointcheval D, Stern J, "Security Arguments for Digital Signatures and Blind Signatures," Journal of Cryptology, 2000, 13(3):361-396.

[31] Sandip Vijay, Subhash C. Sharma, "Threshold signature cryptography scheme in wireless ad-hoc computing," Contemporary Computing, 2009, 40(7):327–335.

[32] Mohamed Abid, Songbo Song, Hassnaa Moustafa, Hossam Afifi, "Integrating identity-based cryptography in IMS service authentication," International Journal of Network Security Its Applications, 2009, 1(3).

[33] Gao T , Guo N , Yim K, "LEAS: Localized efficient authentication scheme for multi-operator wireless mesh network with identity-based proxy signature," Mathematical and Computer Modelling, 2013, 58(5-6):1427-1440.

[34] Vijayakumar P , Azees M , Deborah L J, "CPAV: Computationally Efficient Privacy Preserving Anonymous Authentication Scheme for Vehicular Ad Hoc Networks," IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2015.

[35] N. B. Gayathri, G. Thumbur, P. V. Reddy and M. Z. Ur Rahman, "Efficient Pairing-Free Certificateless Authentication Scheme With Batch Verification for Vehicular Ad-Hoc Networks," in IEEE Access, vol. 6, pp. 31808-31819, 2018.

[36] Shim KA, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Transactions on Vehicular Technology 2012, 61(4): 1874–1883.

[37] Li J , Lu H , Guizani M, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," IEEE Transactions on Parallel and Distributed Systems, 2015, 26(4):938-948.

[38] D. Huang, S. Misra, M. Verma and G. Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 3, pp. 736-746, Sept. 2011.

[39] Eckhoff David and Sommer Christoph, "Readjusting the Privacy Goals in Vehicular Ad-hoc Networks: A Safety-preserving Solution Using Non-Overlapping Time-slotted Pseudonym Pools," Computer Communications, 2018, 122, 10.1016/j.comcom.2018.03.006.

[40] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas and A. Nix, "Optimized Certificate Revocation List Distribution for Secure V2X Communications," 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, 2017, pp. 1-7.

[41] Tarkoma S , Rothenberg C E and Lagerspetz E, "Theory and Practice of Bloom Filters for Distributed Systems," IEEE Communications Surveys & Tutorials, 2012, 14(1):131-155.

[42] Wang M., Liu D., Zhu L., Xu Y. and Wang F., "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication," Computing, vol. 98, no. 7, pp. 685–708, 2016.

[43] Q. E. Ali, N. Ahmad, A. H. Malik, G. Ali, M. Asif, M. Khalid and Y. Cao, "SPATA: Strong pseudonym-based AuthenTicAtion in intelligent transport system," IEEE Access, vol. 6, pp. 79114-79128, 2018.

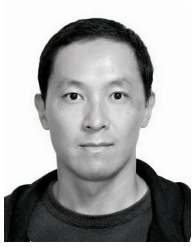
[44] Q. E. Ali, N. Ahmad, A. H. Malik, W. U. Rehman, A. U. Din and G. Ali, "ASPA: Advanced Strong Pseudonym based Authentication in Intelligent Transport System," PLOS ONE 14(8): e0221213, 2019, 10.1371/journal.pone.0221213.

[45] P. Vijayakumar, Victor Chang, L. Jegatha Deborah, Balamurugan Balusamy and P.G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," Future Generation Computer Systems, 2018, 78(PT.3):943-955, 10.1016/j.future.2016.11.024.

[46] H. Zhong, B. Huang, J. Cui, J. Li and K. Sha, "Efficient Conditional Privacy-Preserving Authentication Scheme Using Revocation Messages for VANET," 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, 2018, pp. 1-8.

[47] Mohammad Khodaei and Panos Papadimitratos, "Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs," ACM WiSec, Stockholm, Sweden, June 2018, pp. 172–183.

JIAYU QI received her master's degree in 2019 and is currently studying for her doctorate at the Software College in Northeastern University. During the master's degree period, her research direction was the next generation wireless network security. The main research content is VANETs security and privacy protection. She published a paper on anonymous authentication of VANETs in 2018. During her Ph. D., she will focus on the application of edge computation and block chain technology in VANETs security.



TIANHAN GAO received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecturer at Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at the department of Computer Science, Purdue, from February 2011 to February 2012. He obtained the doctoral tutor qualification in 2016. He is the author or co-author of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, as well as virtual reality.