Hindawi
Security and Communication Networks
Volume 2019, Article ID 4752612, 11 pages
https://doi.org/10.1155/2019/4752612

Research Article

A Practical Authentication Framework for VANETs

Baosheng Wang, Yi Wang, and Rongmao Chen

School of Computer, National University of Defence Technology, 410073, China

Correspondence should be addressed to Rongmao Chen; chromao@nudt.edu.cn

Received 14 March 2019; Revised 29 April 2019; Accepted 7 May 2019; Published 20 May 2019

Guest Editor: Fagen Li

In vehicular ad hoc networks (VANETs), conditional privacy preserving authentication (CPPA) scheme is widely deployed to solve security and privacy issues. Existing CPPA schemes usually require ideal tamper-proof devices (TPDs) on vehicles which, however, might be infeasible or do not exist in reality due to high security requirements. To address this problem, we propose a practical framework of CPPA scheme that supports more realistic TPDs which are less secure correspondingly. We demonstrate that this framework also manages to achieve nonframeability in addition to other security objectives including nonrepudiation, conditional privacy preserving, and unlinkability. Moreover, performance analysis shows that our framework has better efficiency in authentication. All these features make our framework practical for VANETs.

1. Introduction

As one form of mobile ad hoc network in the domain of vehicles, vehicular ad hoc network (VANET) is a promising solution for improving road safety and driving experience. Generally, a VANET is composed of roadside units (RSUs) and vehicles equipped with electronic components such as wheel rotation sensors, radars, and on-broad units (OBUs). Various sensors on vehicle provide continuous monitoring of driving information, such as speed, direction, and position. OBUs enable vehicles to communicate with not only each other but also RSUs via Dedicated Short Range Communications (DSRC) technique. Thus, there are plenty of potential applications on VANETs which can be categorized into safety-related, such as collision avoidance and automatic driving, and other applications, such as traffic navigation and infotainment.

For the security of VANET and its applications, especially safety-related applications, it is crucial to authenticate transmitted messages and identities of their senders; otherwise any unauthorized vehicle could disseminate bogus messages easily or conduct other malicious behaviours without being caught, which might cause great damages to urban transportation systems and even endanger the lives of drivers and pedestrians. To authenticate itself to other entities, vehicle might have to prove the possession of secret information which is usually saved in tamper-proof device (TPD) on vehicle. In addition to storage of secret data, TPD also provides computation service where secret information is involved. For instance, the simplest way to achieve authentication is using digital signature. Every vehicle is assigned to a public/private key pair, and TPD is responsible for storing private keys and generating signatures. Many authentication schemes [1–8] are designed under the assumption of using ideal TPD that can never be compromised by adversary to securely store secrets and to perform related calculations. However, this assumption might be too strong to be realistic in practice. Specifically, in VANET conditions, TPD might mistake normal shocks of vehicle caused by uneven road surface for malicious tampering and erase all the secrets [9]. Moreover, it is possible for adversary to collect sufficient information about secrets in TPD through side-channel attacks such as electromagnetic radiation [10] and power consumption analysis [11].

To address this problem, we loosen the security requirements on ideal TPD and consider a more realistic TPD for practical use. Comparing to ideal TPD, realistic TPD is less sensitive to vehicle shocks but might be compromised by sophisticated hardware tampering. To cope with such hardware tampering as well as aforementioned side-channel attacks, we assume that realistic TPD offers temporary storage of secrets and erases them regularly before adversary obtains

substantial information about them. In this work, we propose an efficient framework of CPPA scheme based on identity-based cryptography (IBC) that only requires realistic TPD.

Our framework also aims at achieving nonframeability [12]. That is, trusted authority (TA) that serves particular region as certification authority and RSUs cannot forge messages to frame an innocent vehicle. TA in existing works (e.g., [6, 13]) usually holds all the secrets of vehicles, so it is quite simple for unrestricted TA to impersonate any vehicle and forge its signature. In our framework, the key used for authentication is independently generated by vehicle itself and stored in TPD. TA that does not possess the authentication key of vehicle cannot impersonate vehicle and successfully authenticate itself to RSU. Meanwhile, RSU's master key which is used to generate the signatures of messages sent by vehicles in our framework is unknown to TA. Thus, TA also cannot forge the signature of vehicle. Besides, RSU cannot forge it either as the pseudo-identity generation also requires vehicle's authentication key.

We design our framework with an objective of improving the efficiency of mutual authentication between vehicle and RSU. Since the location and identity of RSU are relatively fixed, RSU-to-vehicle (R2V) authentication is rather trivial and can be efficiently achieved by periodically broadcasting signed messages. However, vehicle-to-RSU (V2R) authentication in existing works (e.g., [13, 14]) needs the cooperation of TA. In contrast, V2R authentication in our framework does not require real-time interactions between RSUs and TA. Precisely, TA maintains a dynamic list that contains authentication-related information of vehicles, and every RSU is asked to store a latest copy of this list in the background. This list enables RSUs to complete the anonymous authentication of vehicles by themselves, which reduces the workload of TA and promotes the efficiency of authentication. Generally, the main contributions of our work are as follows.

(i) We propose an efficient IBC-based framework of CPPA scheme to solve security and privacy issues in VANETs. Due to the support of realistic TPD, our framework is a practical authentication solution in reality.

(ii) Our framework has achieved nonframeability. The authentication of vehicle and the generation of a valid signature both require vehicle's self-chosen authentication key, which prevents TA and RSUs from framing an innocent vehicle.

(iii) In our framework, we design a mechanism to improve the efficiency of authentication. The overall workload of authentication is distributed to every RSU. Instead of participating in the process of authentication directly, TA just needs to maintain the latest information list for RSUs.

(iv) We give a specific analysis of our framework in terms of security and performance. We prove that this framework has achieved all the security objectives in Section 3. Theoretical analysis on performance indicates that this framework provides excellent authentication efficiency.

The rest of the paper is organized as follows. Section 2 summarizes the related work on authentication schemes for VANETs. Section 3 introduces the architecture of VANETs and our design goals. Preliminary background of cryptographic primitives is provided in Section 4. In Section 5, we present our framework of CPPA scheme. Sections 6 and 7 give the comprehensive security analysis and performance evaluation of our framework, respectively. Section 8 concludes the paper.

2. Related Work

A number of related studies have been reported on authentication issue in VANETs, and their proposed authentication schemes can be categorized into following four types.

Schemes based on Public Key Infrastructure (PKI) [9, 15]. PKI issues a bunch of public/private key pairs and public key certificates to vehicles. Before sending a message, vehicle has to attach a digital signature and a certificate to it, which might increase the communication overhead significantly. To achieve identity privacy and conditional anonymity, anonymous public keys are required for PKI and vehicles. The management of certificates including revocation could be a heavy burden to PKI.

Schemes based on symmetric cryptosystem [12, 16, 17]. Message authentication code (MAC) can be adopted to authenticate message and the verification of the message can be completed in extremely short time. However, the process of message authentication might need the aid of RSUs, and vehicle cannot authenticate received message independently. TESLA [18] is an efficient broadcast authentication protocol based on MAC and loose time synchronization between network nodes. Based on TESLA and the prediction of vehicle direction, it is possible to achieve instant verification of beacon messages sent by vehicles. Unfortunately, this protocol allows adversary to trace the trajectory of vehicle.

Schemes based on group signature [1, 4, 19–22]: group signature naturally provides privacy to group members because every member signs message on behalf the group. The group manager owns the master key of group and is able to learn the real identities of group members, which satisfies the requirement of conditional privacy preservation. However, the verification of group signature usually costs more time than that of traditional signature. Also, revoking compromised group members properly is still a problem.

Schemes based on IBC [2, 6, 7, 13, 14, 23–25]. In identity-based signature (IBS) scheme, the identity of vehicle could be used as the public key, and the corresponding private key is generated by the private key generator (PKG) using master key. Comparing to PKI, it avoids the management of certificates. To achieve conditional privacy, vehicles communicate with other entities using pseudo-identities that are retrievable to authorities. Unfortunately, due to bilinear pairing operations, the time efficiency of IBS schemes is relatively lower than other traditional signature schemes.

To improve the performance, batch verification is adopted to verify multiple signatures at the same time. Moreover, efficient one-time IBS [6, 13], identity-based online/offline signature (IBOOS) [7], and IBS without bilinear pairing [6] also are used in authentication schemes.

3. Background

3.1. Network Architecture. A VANET commonly consists of vehicles, RSUs, and TA, as shown in Figure 1.

TA plays the role of administrator in VANET and manages the authentication of network nodes including vehicles and RSUs. To join the VANET, all the nodes must register themselves at TA in advance. Due to the mobility of vehicles, we consider a frequently changing group of vehicles that requires TA to provide real-time registration service via secure network infrastructure. In contrast, the locations and total number of RSUs usually stay unchanged for a relatively long period of time. The registration of RSUs can be finished during initialization phase. Also, TA maintains a list of registered vehicles and has responsibility for revealing real identities of misbehaving vehicles and revoking licenses of these vehicles in time.

RSUs as roadside infrastructure are scattered all over the region of TA. Communication between RSU and TA relies on wired channel while RSU communicates with vehicles via wireless channel using DSRC protocol. RSUs forward messages not only between TA and vehicles but also from one vehicle to another. A RSU and vehicles enrolled by it form a subgroup of VANET. Vehicles that newly enter the transmission range of RSU have to be authenticated by RSU.

Every vehicle is equipped with OBU to communicate with other entities in VANET and support DSRC protocol. Realistic TPD is also embedded in vehicle. It provides temporary storage of secret information and related computation service, which is more feasible than ideal TPD that never discloses any secrets. Therefore, secrets stored in TPD needs to be updated regularly with the assistance of TA.

3.2. Design Goals. As a framework of CPPA scheme, our framework should satisfy basic requirements: authentication, nonrepudiation, identity privacy preserving, and conditional traceability.

(i) *Authentication*: there are two kinds of authentication: message and entity authentication. Message authentication is confirming that received messages are generated by valid vehicles and unmodified during transmission. Entity authentication, also called mutual authentication, requires that two entities into a session are able to identify each other.

(ii) *Nonrepudiation*: this property refers to a situation where a receiver is able to prove to a third party that sender cannot deny its responsibility for generating messages. It prevents adversary from forging messages in other identities.

(iii) *Identity privacy preserving*: vehicles on the roads are required to frequently broadcast messages including position, speed, direction, and driving status. Identity privacy preservation means that nobody could discover the binding between messages and real identities of vehicles.

(iv) *Conditional traceability*: in certain circumstances (e.g., traffic accidents), the real identities of vehicles should be retrievable. Conditional traceability enables TA only to recover the real identities of vehicles from saved messages.

Considering the particular scenario of VANET, we also attempt to achieve other meaningful properties at the same time.

(i) *Nonframeability*: this property requires no entities in VANETs including TA and RSUs could frame an innocent vehicle or accuse an honest vehicle for having misbehaved. To achieve this security goal, we assume that TA does not collude with RSUs.

(ii) *Ideal TPD freeness*: under the premise of ensuring system security, this property proposed by Zhang et al. [13] permits the usage of realistic TPD or one with sufficient security level embedded in vehicle, instead of ideal one which can never be compromised by adversary.

(iii) *Unlinkability*: let m_1 and m_2 be two messages sent by one vehicle; this property means that one cannot determine whether m_1 and m_2 originate from the same vehicle or not. Unlinkability prevents adversary from tracking vehicles and profiling drivers.

(iv) *Message confidentiality*: in particular applications, messages should be transmitted to receivers in encrypted form and cannot be decoded by unauthorized entities.

(v) *Attack resistance*: this property requires that proposed framework can withstand common attacks, such as replay attack, impersonation attack, modification attack, and side-channel attack.

4. Preliminaries

4.1. Cryptographic Schemes. A symmetric encryption scheme consists of three algorithms which are described as follows.

(i) KeyGen(1^n): this algorithm takes as input security parameter 1^n and outputs key $K \in \mathcal{K}$, where $\mathcal{K}$ is the key space.

(ii) Enc(K, m): this algorithm takes as input key K and message m and outputs ciphertext c.

(iii) Dec(K, c): this algorithm takes as input key K and ciphertext c and outputs message m.

An identity-based signature (IBS) scheme is composed of four algorithms which are described as follows.

(i) Setup(1^n): this algorithm takes as input security parameter 1^n and generates the public parameters PP and master key $msk \in \mathcal{MK}$ for private key generator (PKG). Note that msk is kept secret.

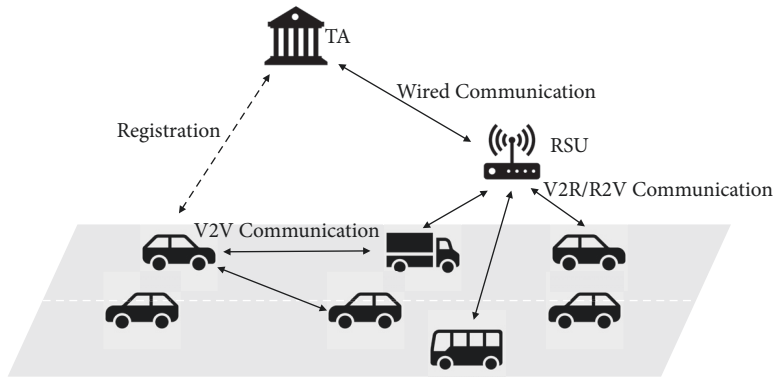

Figure 1: The network architecture of VANET.

(ii) Extract(msk, ID): this algorithm takes as input master key msk and an identity and outputs a private key $sk_{ID} \in \mathcal{SK}$.

(iii) Sign(sk_{ID}, m): this algorithm takes as input private key sk_{ID} and message m and generates a signature $Sign$ of message m.

(iv) Verify($PP, ID, m, Sign$): this algorithm outputs "accept" if $Sign$ is valid signature of message m and outputs "reject" otherwise.

An identity-based online/offline signature (IBOOS) scheme is an IBS scheme where the process of generating signature can be divided into offline and online phases:

(i) $\text{Sign}_{\text{off}}(PP)$: based on public parameters PP, this algorithm generates an offline signature $\overline{Sign}$.

(ii) $\text{Sign}_{\text{on}}(sk_{ID}, \overline{Sign}, m)$: based on private key sk_{ID}, offline signature $\overline{Sign}$, and message m, this algorithm generates a signature $Sign$ of message m.

An one-time identity-based signature (OT-IBS) scheme is an IBS scheme with one-time private key sk_{ID}. Similar to signing key in one-time signature scheme, every private key in OT-IBS can be used only once.

4.2. Cryptographic Hardness Assumption. Computational Diffie-Hellman (CDH) assumption: let $\mathbb{G}$ be a group with prime order p and $g \in \mathbb{G}$ is a random generator of $\mathbb{G}$, and $\mathcal{A}$ is a probabilistic polynomial-time (PPT) algorithm that takes as input a tuple (g, g^a, g^b) and outputs g^c. We define the CDH-advantage of $\mathcal{A}$ to be $Adv_{\mathcal{A}}^{CDH}(n) = \Pr[\mathcal{A}(g, g^a, g^b) = g^{ab}]$. The CDH assumption is that there is no PPT algorithm $\mathcal{A}$ that can compute g^{ab} with nonnegligible CDH-advantage.

5. Proposed Framework of CPPA Scheme

5.1. Overview. In initialization phase of our framework, TA generates parameters for the whole system. RSUs and vehicles are allowed to join VANET after registration. For vehicle that drives into a new RSU region, it also needs to conduct mutual authentication with RSU. To conceal the real identity of vehicle from RSU, V2R authentication needs the assistance of a list maintained by TA that consists of authentication-related information of vehicles. If this authentication succeeds, vehicle would receive the master key of RSU and be able to sign messages in pseudo-identities. Only TA can recover the real identity of vehicle from its pseudo-identities. There also is an efficient and secure mechanism of updating secrets (i.e., authentication key of vehicle and master key of RSU) in TPD before adversary has collected sufficient information via side-channel attacks. Notations used in our framework are defined as follows.

(i) $\mathcal{IBS}$ = (Setup, Extract, Sign, Verify): an IBS scheme that supports batch verification of multiple signatures.

(ii) $\mathcal{SE}$ = (KeyGen, Enc, Dec): a symmetric encryption scheme with message space $\{0,1\}^*$ and key space $\mathcal{K}$.

(iii) $\mathbb{G}_1, \mathbb{G}_2$: two cyclic groups with prime order q.

(iv) g_1, g_2: two generators of $\mathbb{G}_1, \mathbb{G}_2$.

(v) H_1, H_2, H_3, H_4: four hash functions $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \longrightarrow \mathcal{K}$, $H_3 : \{0,1\}^* \longrightarrow \{0,1\}^\ell$, and $H_4 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$.

(vi) ID_{U_i}/ID_{V_j}: real identity of RSU U_i or vehicle V_j.

(vii) PID_{V_j}: pseudo-identity of vehicle V_j.

5.2. System Initialization. In initialization phase, TA generates parameters for the whole system and all the RSUs and vehicles have to register themselves to TA before joining the VANET. Precisely, the system is initialized as follows.

TA Setup: TA runs algorithm Setup to generate public parameters PP_s and system master key msk_s. TA also generates two cyclic groups $\mathbb{G}_1, \mathbb{G}_2$with prime order q and picks generators $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$. Then it picks $x, y, z \in \mathbb{Z}_q^*$ and computes $X = g_1^x, Y = g_1^y, Z = g_1^z$ which are used to generate pseudo-identities for vehicle. Hash functions $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \longrightarrow \mathcal{K}$, $H_3 : \{0,1\}^* \longrightarrow \{0,1\}^\ell$, and $H_4 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$ are chosen by TA. The system public parameters are $PP = (PP_s, q, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, X, Y, Z, H_1, H_2, H_3, H_4)$. TA also maintains a private list $\mathcal{L}$ to record authentication

information of registered vehicles as well as list $\mathscr{L}_{pub}$ that is only accessible to registered RSUs. The details of these lists are described later.

RSU Setup: since TA is the only party that owns msk_s in current system, RSU U_i with identity ID_{U_i} obtains its private key $sk_{U_i} \longleftarrow \text{Extract}(msk_s, ID_{U_i})$ from TA. Besides, each RSU U_i has to generate their own public parameters PP_{U_i} and master key msk_{U_i} by running algorithm Setup. For the sake of system security, we require RSU to update its public parameters and master key regularly and share its latest public parameters among all the registered RSUs.

Vehicle Setup: vehicle should register itself to local TA via secure network infrastructure as soon as it enters a new TA region. TPD on vehicle is initialized to preload system public parameters PP and all the identities of registered RSUs. Let V_j be a vehicle with identity ID_{V_j}. Supposing that V_j randomly picks $a'_j \in \mathbb{Z}_q^*$ at time t_j, then its authentication key is $a_j = H_4(a'_j, t_j) \in \mathbb{Z}_q^*$. Vehicle V_j computes $H_j = H_1(ID_{V_j}, a_j)$, $A_j = g_1^{a_j}$ and submits (ID_{V_j}, H_j, A_j) to TA. Then, TA picks $r_j \in \mathbb{Z}_q^*$ and generates challenge $R_j \longleftarrow g_1^{r_j}$ and dynamic password $P_j = A_j^{r_j}$ for V_j. Authentication key a_j and challenge R_j are saved in TPD on vehicle V_j. Meanwhile, TA inserts tuple $\{ID_{V_j}, H_j, A_j, r_j, P_j, T_j\}$ into list $\mathscr{L}$ and tuple $\{A_j, P_j, T_j\}$ into list $\mathscr{L}_{pub}$, where T_j is the expiration date of these two tuples. When tuples in both lists have expired, TA forces corresponding vehicles to update their authentication keys.

5.3. Mutual Authentication. Mutual authentication between vehicle V_j and RSU U_i happens when vehicle V_j is in the transmission range of RSU U_i but does not possess its latest master key. The whole process consists of two stages.

R2V authentication: RSU U_i broadcasts message $(ID_{U_i}, PP_{U_i}, R_i, E_i, t_i, \sigma_{U_i})$ periodically to authenticate itself to newly entered vehicles, where timestamp t_i provides freshness, challenge $R_i = g_1^{r_i}$ that changes along with t_i is used to authenticate vehicle in next stage, element $E_i = g_2^{e_i}$ is used to negotiate symmetric keys with vehicles (both $r_i, e_i \in \mathbb{Z}_q^*$ are picked by RSU U_i and kept secret), and $\sigma_{U_i} \longleftarrow \text{Sign}(sk_{U_i}, M_{R2V})$ is the signature of $M_{R2V} = (ID_{U_i}, E_i, t_i) \in \{0,1\}^*$. After receiving the broadcast message, vehicle V_j first checks whether identity ID_{U_i} has been preloaded into TPD at setup stage or not. If not, vehicle V_j aborts this authentication; otherwise, it verifies signature σ_{U_i} by running $\text{Verify}(PP_s, ID_{U_i}, M_{R2V}, \sigma_{U_i})$. If algorithm Verify outputs "reject", vehicle V_j aborts; otherwise, this authentication succeeds.

V2R authentication: to authenticate itself to RSU U_i, vehicle V_j has to recover its dynamic password P_j in list $\mathscr{L}$ and answer the challenge R_i of RSU U_i with authenticate key a_j.

(1) Vehicle V_j computes $P_j = R_j^{a_j}$ and $P_i = R_i^{a_j}$. Then, it picks $f_j \in \mathbb{Z}_q^*$ and computes $F_j = g_2^{f_j}$ and $K = H_2(E_i^{f_j})$. Key K is used to encrypt $M_{VR} = (P_j, H_3(ID_{U_i}, P_j, P_i, F_j, t_j))$ with algorithm Enc, where t_j is the timestamp. Let $C_j = \text{Enc}(K, M_{VR})$ be the ciphertext of M_{VR}, vehicle V_j replies to RSU U_i with message $(ID_{U_i}, F_j, t_j, C_j)$.

(2) RSU U_i first computes symmetric key $K = H_2(F_j^{e_i})$ and decrypts C_j with K. Supposing that $M'_{VR} = (P'_j, P'_i, H'_{VR})$ is the output of $\text{Dec}(K, C_j)$, if $H'_{VR} \neq H_3(ID_{U_i}, P'_j, P'_i, F_j, t_j)$, RSU U_i aborts; otherwise, RSU U_i searches list $\mathscr{L}_{pub}$ for tuple $\{A', P', T'\}$, where $P' = P'_j$. If such tuple does not exists or has expired, or more than one tuple is found in list $\mathscr{L}_{pub}$, RSU U_i aborts; otherwise, it computes $P''_i = (A')^{r_i}$. If $P''_i = P'_i$, then vehicle V_j manages to authenticate itself to RSU U_i without revealing its real identity.

(3) RSU U_i sends its master key msk_{U_i} to vehicle V_j in ciphertext format $(ID_{U_i}, \widetilde{T}_i, \widetilde{t}_i, \widetilde{C}_i)$, where $\widetilde{T}_i$ is the expiry time of msk_{U_i}, $\widetilde{t}_i$ is a timestamp, and $\widetilde{C}_i = \text{Enc}(K, M_{RV})$, $M_{RV} = (msk_{U_i}, H_3(ID_{U_i}, msk_{U_i}, \widetilde{T}_i, \widetilde{t}_i))$.

(4) Vehicle V_j decrypts C_i and gets $M'_{RV} = (msk'_{U_i}, H'_{RV})$. If $H'_{RV} \neq H_3(ID_{U_i}, msk'_{U_i}, \widetilde{T}_i, \widetilde{t}_i)$, vehicle V_j aborts; otherwise, it stores master key msk'_{U_i} into TPD. Note that this master key will be erased automatically at time $\widetilde{T}'_i$.

5.4. Pseudo-Identity Generation. In terms of privacy preservation, instead of real identities of vehicles, pseudo-identities are generated by TPD to hide the real-world identities of vehicles. Considering a vehicle V_j with real identity ID_{V_j} in the transmission range of RSU U_i, we define its pseudo-identity as $PID_{V_j} = (S, \Pi_0, \Pi_1) = (g_1^s, H_1(ID_{V_j}, a_j)X^s, Y^s Z^{\theta s})$, where $s \in \mathbb{Z}_q^*$ is randomly picked by TPD and $\theta = H_4(g_1^s, H_1(ID_{V_j}, a_j)X^s)$.

We remark that the computation of pseudo-identity of vehicle V_j can be viewed as encrypting $H_1(ID_{V_j}, a_j)$ using Cramer-Shoup encryption scheme (CS scheme) [26] which is secure against adaptive chosen-ciphertext attack (CCA2 secure). The main advantage of such pseudo-identity is that TA could trace the real identity of vehicle by decrypting pseudo-identity. Besides, the nonmalleability of CS scheme does not allow anyone to derive a new and valid pseudo-identity from given one. Using CS scheme might be time-consuming for devices on vehicle, while this problem can be overcame by preparing sufficient pseudo-identities offline in storage device as the on-board storage capacity of vehicle could be extensive.

5.5. Message Signing and Verification. When vehicle V_j locates in the region of RSU U_i, before signing message, it first generates the private key psk_{V_j} of its pseudo-identity PID_{V_j} with master key msk_{U_i} and then signs message m with psk_{V_j} and broadcasts $(PID_{V_j}, ID_{U_i}, m, t_j, \sigma_{V_j})$ to RSUs or vehicles

around, where t_j is a timestamp and $\sigma_{V_j} \longleftarrow \text{Sign}(psk_{V_j}, M)$, $M = (PID_{V_j}, m, t_j)$.

Message m can be verified by running $\text{Verify}(PP_{U_i}, PID_{V_j}, M, \sigma_{V_j})$. However, for verifier that is not in the region of RSU U_i, it has to request the public parameters PP_{U_i} of U_i from nearby RSU. Since IBS scheme $\mathcal{IBS}$ supports the batch verification of multiple signatures, the verifier is able to take advantage of this property to improve the performance of message verification.

5.6. Vehicle Tracing. Pseudo-identity protects the privacy of vehicles on the one hand and facilitates some malicious vehicles to disseminate bogus information on the other. Thus, it is of importance to track down the real identities of misbehaving vehicles which can only be done by TA. Particularly, let PID_{V_j} be one pseudo-identity of malicious vehicle V_j, TA parses PID_{V_j} into (S, Π_0, Π_1) and computes $\theta = H_4(S, \Pi_0)$, $\Pi_1' = S^{y+\theta z}$. If $\Pi_1' \neq \Pi_1$, then this pseudo-identity is invalid; otherwise TA computes $H = \Pi_0 / S^x$. If there exists one valid tuple $\{ID_{V_j}, H_j, A_j, r_j, P_j, T_j\}$ in list $\mathcal{L}$ with $H_j = H$, then TA succeeds to find out the real identity ID_{V_j} of vehicle V_j.

5.7. Secret Parameters Update. There are two secret parameters in TPD that need to be updated regularly: authentication key and RSU's master key. Note that RSU's master key is updated along with V2R authentication. Here, we focus on authentication key update.

(1) Assuming that tuple $\{ID_{V_j}, H_j, A_j, r_j, P_j, T_j\}$ reaches the expiration date T_j, TA generates a pseudo-identity $PID_A = (A_j, H_j A_j^x, A_j^{y+\theta z})$ for vehicle V_j, where $\theta = H_4(A_j, H_j A_j^x)$. Then, TA picks $\hat{r}, r^*, e \in \mathbb{Z}_q^*$ and computes $\widehat{R} = g_1^{\hat{r}}$, $R^* = g_1^{r^*}$, $E = g_2^e$ where challenge $\widehat{R}$ is a test for target vehicle V_j, R^* is a new challenge for V_j and E is used to negotiate key. TA then computes signature $\sigma_A \longleftarrow \text{Sign}(psk_A, M_{TA})$, where $psk_A = \text{Extract}(msk_s, PID_A)$ and $M_{TA} = (PID_A, \widehat{R}, R^*, \widehat{t})$ and broadcasts (M_{TA}, σ_A), where $\widehat{t}$ is a timestamp.

(2) Vehicle V with real identity ID_V and authentication key a that receives this message of TA would check whether $PID_A = (g_1^a, H_1(ID_V, a)X^a, Y^a Z^{\theta a})$, where $\theta = H_4(g_1^a, H_1(ID_V, a)X^a)$. Only V_j that possesses a_j can recognize this pseudo-identity. Then, V_j prepares to update authentication key. It runs $\text{Verify}(PP_s, PID_A, M_{TA}, \sigma_A)$. If signature σ_A is valid and timestamp $\widehat{t}$ is fresh, vehicle V_j picks $a', f \in \mathbb{Z}_q^*$ and computes $a^* = H_4(a', t_j)$, $A^* = g_1^{a^*}$, $H^* = H_1(ID_{V_j}, a^*)$, $F = g_2^f$, $K' = H_2(E^f)$, and $\widehat{P} = \widehat{R}^{a_j}$. Then, vehicle V_j sends message (ID_{TA}, F, t_j, C_j) to TA, where t_j is the timestamp, $C_j = \text{Enc}(K', M_U)$, and $M_U = (A^*, \widehat{P}, H_3(ID_{TA}, A^*, \widehat{P}, t_j))$.

(3) TA recovers $K' = H_2(F^e)$ to decrypt C_j and obtains $M_U' = (A', H', \widehat{P}', H_U')$. If $H_U' \neq H_3(ID_{TA}, A', \widehat{P}', t_j)$, TA aborts; otherwise, it computes $P' = A_j^{\hat{r}}$. If $\widehat{P}' \neq P'$, TA aborts; otherwise, vehicle V_j passes the test of TA; then TA computes $P^* = (A')^{r^*}$ and updates $\{ID_{V_j}, A_j, H_j, r_j, P_j, T_j\}$ with $\{ID_{V_j}, A', H', r^*, P^*, T^*\}$ in list $\mathcal{L}$, where T^* is the expiration time. Also, in list $\mathcal{L}_{pub}$, tuple $\{A_j, P_j, T_j\}$ is updated with $\{A', P^*, T^*\}$. TA picks $\overline{r} \in \mathbb{Z}_q^*$, computes $\overline{R} = g_1^{\overline{r}}$, $\overline{P} = (A')^{\overline{r}}$, and broadcasts $(PID_A, \overline{R}, \overline{P}, \overline{t}, \sigma_A')$, where $\overline{t}$ is a timestamp, $\sigma_A' \longleftarrow \text{Sign}(psk_A, \overline{M}_{TA})$ is the signature of $\overline{M}_{TA} = (PID_A, \overline{P}, \overline{t})$.

(4) Vehicle V_j checks the integrity and validity of message. If signature σ_A' is valid and timestamp $\overline{t}$ is fresh, vehicle V_j computes $\overline{P}' = \overline{R}^{a^*}$. If $\overline{P} \neq \overline{P}'$, vehicle V_j aborts; otherwise, current authentication key a_j and challenge R_j in TPD are replaced with a^* and R^*.

We remark that the centralized update of authentication key might incur DoS attack against TA. Fortunately, there are several effective ways to cope with such attack. First, TA in reality can provide the update service in parallel mode. That is, multiple servers are deployed to interact with vehicles simultaneously which can alleviate the burden on each server and accelerate the overall efficiency. Besides, since TA is the initiator of update procedure, it is able to adaptively adjust the interval of update according to practical situation without compromising the security of whole system. Also, if TA does not receive the reply of one vehicle within a period of time, it would abort the update process with this vehicle and refuse to interact with it temporarily.

6. Security Analysis

This section gives a comprehensive security analysis of our framework. We show that our framework has achieved all the security objectives mentioned in Section 3.

Authentication: one can notice that message authentication is guaranteed by IBS scheme immediately, so we mainly analyze the mutual authentication between vehicle and RSU. In R2V authentication, the generation of signature of broadcasted message needs RSU's private key which is provided by TA. If received signature can be successfully verified with the identity of RSU, vehicle is convinced that current RSU is the sender of messages from the unforgeability of IBS scheme. In V2R authentication, for vehicle V_j, it proves to RSU that it can recover the dynamic password $P_j = A_j^{r_j}$ of tuple $\{A_j, P_j, T_j\}$ in list $\mathcal{L}_{pub}$ and answer the dynamic password $P_i = A_j^{r_i}$ which is corresponding to new challenge $R_i = g_1^{r_i}$ generated by RSU. We claim that given A_j and R_i, other entities that do not possess the authentication key a_j or r_i picked by RSU cannot compute the correct P_i if CDH problem is hard. Therefore, vehicles that send correct dynamic password pair (P_j, P_i) can authenticate themselves

to RSU. Since tuple $\{A_j, P_j, T_j\}$ and P_i are independent of the real identity of V_j, the whole process of authentication does not leak any information about vehicle's identity.

Nonrepudiation: the pseudo-identity of vehicle, corresponding to private key and signature of message broadcasted by vehicle are all generated in TPD. Since pseudo-identity, signature, and timestamp are key components of message, a vehicle cannot deny its behavior of generating message via TPD at certain time. Moreover, the generation of pseudo-identity requires authentication key a_j which is only accessible to vehicle itself. Due to the nonmalleability of CS scheme, we note that one cannot derive a new valid pseudo-identity from given one.

Identity privacy preserving: the pseudo-identity of vehicle V_j is a ciphertext of $H_1(ID_{V_j}, a_j)$ in CS scheme. From the security of this encryption scheme, pseudo-identity does not leak any information about vehicle's real identity. Moreover, the mutual authentication between vehicle and RSU does not leak real identity as well.

Conditional Traceability: the process of tracing vehicle has been described in Section 5 already. Only TA that possesses the private key x, y, z is able to verify the validity of pseudo-identity, recover $H_j = H_1(ID_{V_j}, a_j)$, and find the real identity ID_{V_j} in private list $\mathscr{L}$.

Nonframeability: since vehicle's authentication key is only accessible to itself, TA cannot authenticate itself to RSU as a valid vehicle and obtain the RSU's master key, let alone generating the private keys of pseudo-identities and forging the signatures of vehicles. On the other hand, although RSU owns master key, it cannot generate vehicle's new pseudo-identities and valid signatures as the authentication key is required and collected pseudo-identities do not provide any useful information for pseudo-identity generation. Moreover, although RSU could collect a set of pseudo-identities of vehicles, due to unlinkability, it is impossible for RSU to distinguish certain vehicle's pseudo-identities and to forge serial signatures of this vehicle. TA is also able to detect the reuse of pseudo-identities by decrypting them and querying recovered hash values in maintained list. If TA does not find them in list, then there exists the abuse of pseudo-identities.

Ideal TPD freshness: one can note that secrets in TPD are vehicle's authentication key and RSU's master key. TA is responsible for the update of vehicle's authentication key and RSU would regularly update its master key. Thus, realistic TPD is secure enough to store these secrets and ideal TPD is not needed.

Unlinkability: in our framework, all messages of vehicle are signed with different pseudo-identities which are independent from each other. It is impossible to distinguish whether two random messages are sent by one vehicle or not. Thus, our framework satisfies unlinkability.

Message confidentiality: in V2R authentication, RSU sends its master key in ciphertext form to vehicles that complete current authentication. The master key of RSU is encrypted using symmetric encryption scheme and the negotiation of symmetric key follows the method of Diffie-Hellman key exchange. Thus, transmission of RSU's master key is confidential and secure. Similarly, the same symmetric encryption scheme and key exchange method are applied in transmitting new authentication information of vehicle during updating secret parameters.

Attacks resistance: In proposed framework, we assume that the whole system is initialized in a secure environment, but mutual authentication, message signing and verification, and secret parameter update might suffer various attacks from adversary. We now demonstrate that our framework is resistant to following attacks.

(i) Replay attack: every transmitted message is marked with timestamp. The receiver of message would check the freshness of message via timestamp and discard replayed messages.

(ii) Impersonation attack: in mutual authentication, adversary might try to imitate a valid RSU U_i and gain the trust of vehicles. However, the private key of RSU U_i is generated in initialization phase and securely kept by RSU U_i. Adversary cannot access to this private key. Thus, the signature of its message cannot be verified with the identity of U_i. In secret parameters update, if adversary (e.g., registered vehicles or RSUs) wants to impersonate the TA and send update instruction to vehicle V_j, it has to compute the special pseudo-identity PID_A of V_j with public parameters X, Y, Z. The hardness of computing $PID_A = (A_j, H_j A_j^x, A_j^{y+\theta z})$ with A_j and X, Y, Z can be reduced to CDH assumption. One update instruction is targeted at only one vehicle, but other irrelevant vehicles might also receive this instruction. If a malicious vehicle intends to imitate the target one V_j, it has to answer the challenge $\widehat{R}$ of TA with dynamic password $\widehat{P}$. Given $\widehat{R}$ and A_j, it is still hard to compute $\widehat{P} = \widehat{R}^{a_j} = A_j^{\widehat{r}}$ according to CDH assumption. Thus, our framework could withstand impersonation attack.

(iii) Modification attack: for signed message, making any modifications could result in the failure of verification from the correctness of IBS scheme. For encrypted message, the plaintext and its hash value are concatenated and encrypted together. If ciphertext is modified arbitrarily, the underlying plaintext cannot be verified with its hash value.

(iv) Side-channel attack: this attack is mainly for vehicle's TPD which stores sensitive data including authentication key and master key of RSU. It is worth mentioning that the real identity of vehicle is not stored in TPD. In our protocol, these secret parameters are updated frequently such that adversary cannot obtain sufficient data through side-channel analysis. Moreover, new secret parameters are independent of the old ones, so the leakage of old parameters does not benefit the guessing of new ones.

Remarks: it is worth mentioning that Sybil attack is inevitable and ubiquitous in most of cryptographic schemes and thus the detection of such attack has been extensively studied

Table 1: Notations of different execution time.

Notation	Description
T_m	Average execution time of multiplication operation on group $\mathbb{G}_1$ or $\mathbb{G}_2$.
T_a	Execution time of addition operation on group $\mathbb{G}_1$ or $\mathbb{G}_2$.
T_p	Execution time of bilinear pairing operation $e(\cdot,\cdot)$.
T_{pm}	Average execution time of multiplication operation on group $\mathbb{G}$.
T_{pa}	Execution time of addition operation on group $\mathbb{G}$.
T_h	Average execution time of general hash operation.
$T_{sign}^{\mathcal{IBS}}$	Execution time of signing message using $\mathcal{IBS}$ scheme.
$T_{vrfy}^{\mathcal{IBS}}$	Execution time of verifying signature using $\mathcal{IBS}$ scheme.
T_{aes}	Execution time of AES encryption / decryption.
T_{query}	Execution time of searching list.

[27]. Our framework is vulnerable to Sybil attack as any authenticated vehicle is accessible to the master key of RSU and can imitate other vehicles at the same time by forging their messages. However, we claim that it is possible to detect such attack by authorities in proposed framework. Precisely, misbehaving vehicle cannot imitate other vehicles as it does not know their authentication keys and cannot generate correct pseudo-identities. Collected pseudo-identities also do not help in computing new ones from the nonmalleability of CS scheme. Besides, the reuse of collected pseudo-identities can be detected by TA. Consequently, only pseudo-identities of misbehaving vehicle itself can be generated to conduct Sybil attack. The TA is able to detect such attack easily by revealing its real identity from pseudo-identities.

7. Performance Analysis

In this section, we evaluate both the computation and communication costs of authentication in our framework and make a comparison with existing works. To achieve 80-bit security, elliptic curve groups $\mathbb{G}_1, \mathbb{G}_2$ with 160-bit prime order q, IBS scheme $\mathcal{IBS}$, and symmetric encryption scheme AES with 80-bit security are used in our protocol. In pairing-based IBS scheme $\mathcal{IBS}$, we use bilinear pairing e: $\mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$ to realize 80-bit security level, where $\mathbb{G}$ is an additive group with 160-bit prime order p on supersingular elliptic curve with embedding degree 2. The sizes of elements in $\mathbb{G}_1$ and $\mathbb{G}$ are 320 bits and 1024 bits. For the convenience of discussion, notations of execution time are defined in Table 1.

According to [6], bilinear pairing operation that takes $T_p \approx 4ms$ is the most time-consuming operation. Other bilinear pairing-related operations cost more time than corresponding operations in ECC. That is, $T_{pm} \approx 3.9T_m = 1.7ms$ and $T_{pa} \approx 3.9T_a$. The execution time of multiplication operation T_m/T_{pm} is approximately 240 times greater than T_a/T_{pa}. In comparison to above execution time, T_h, T_{aes}, and T_{query} could be negligible.

7.1. Comparison of Different IBS Schemes. IBOOS and OT-IBS schemes usually might be more efficient than traditional IBS schemes. In IBOOS scheme, time-consuming operations can be completed in offline stage, and the actual signing time is determined by online stage. The structure of OT-IBS scheme is commonly much simpler than that of traditional IBS scheme because of the one-time usage of private key. Moreover, IBS schemes that support batch verification could amortize time-consuming operation over a bundle of signatures. Therefore, for better performance, we only investigate existing IBOOS and OT-IBS schemes that support batch verification.

Table 2 shows the comparison of signing time T_{sign}, verification time T_{vrfy}, and signature size. One can note that bilinear pairing-based IBS schemes XMS and ZWD are less efficient than ECC-based IBS schemes in both verification time and signature size. Schemes LBZ and HZS have same verification time. However, the signing time of LBZ is correlated with the bit length n of message, so it might be greater than that of HZS for long messages. Moreover, scheme HZS enjoys the shortest signature among these schemes. Thus, in following discussion, we adopt scheme HZS as the IBS scheme in our framework.

7.2. Authentication Efficiency. When evaluating an authentication protocol, we are most concerned about the time and communication costs of authentication. In our framework, vehicle that just enters a new RSU region has to complete the mutual authentication with RSU in time; otherwise it cannot communicate with other entities. Thus, we consider the overhead of mutual authentication from the perspective of vehicle. Since RSU broadcasts messages periodically, it is reasonable to assume that vehicle receives these messages as soon as it drives into the region of RSU. The computational overhead of R2V authentication is mainly determined by $T_{vrfy}^{HZS} = 3T_m + 2T_a$. Before replying to RSU, vehicle has to spend time $T_{gen}^{v} = 3T_m + 2T_h + T_{aes}$ to generate message $(ID_{U_i}, F_j, t_j, C_j)$. In AES, the size of ciphertext is the same as plaintext, so ciphertext C_j is 320∗2+160=800-bit long. Suppose that the size of identity of RSU ID_{U_i} is 160 bits, timestamps are 20 bits, and the length of message $(ID_{U_i}, F_j, t_j, C_j)$ is 160+320+20+800=1300 bits. Then, RSU spends time $T_{proc}^{r} = 2T_m + 3T_h + 2T_{aes} + T_{query}$ to process the message from vehicle and prepare master key for it if authentication succeeds, where T_{query} is the execution time of searching list $\mathcal{L}_{pub}$. The length of message $(ID_{U_i}, \widetilde{T}_i, \widetilde{t}_i, \widetilde{C}_i)$ sent by RSU is 160+20+20+(160+160)=520 bits. Vehicle needs

Table 2: Efficiency of different IBS schemes.

Signature Type	Scheme	Signing Time T_{sign}	Verification Time T_{vrfy}	Signature Size (bits)
IBOOS	XMS [28]	negligible	$2T_p + 2T_{pm} + T_{pa}$	$2\lvert\mathbb{G}\rvert + \lvert p\rvert \approx 2208$
	LBZ [29]	nT_a	$3T_m + 2T_a$	$2\lvert\mathbb{G}_1\rvert + \lvert q\rvert \approx 800$
OT-IBS	HZS [6]	T_m	$3T_m + 2T_a$	$\lvert\mathbb{G}_1\rvert + \lvert q\rvert \approx 480$
	ZWD [13]	$T_{pm} + T_{pa}$	$2T_p + T_{pm} + T_{pa}$	$\lvert\mathbb{G}\rvert + \lvert p\rvert \approx 1184$

Table 3: Comparison of mutual authentication efficiency.

Mutual Authentication	Computation Overhead	Communication Overhead (bits)
Li et al.[7]	$9T_m + 726T_a \approx 2886T_a$	3200
Zhang et al.[13]	$2T_p + 6T_{pm} + T_{pa} \approx 10300T_a$	3268
Our framework	$8T_m + 2T_a \approx 1920T_a$	1820

time $T^v_{dec} = T_{aes} + T_h$ to decrypt it and check the master key of RSU. Therefore, the overall computation overhead of mutual authentication is $T_{v\longleftrightarrow r} = T^{HZS}_{vrfy} + T^v_{gen} + T^r_{proc} + T^v_{dec} = 8T_m + 2T_a + 6T_h + 4T_{aes} + T_{query} \approx 8T_m + 2T_a$, and the communication overhead is 1300+520=1820 bits.

Similarly, we also analyze the efficiency of mutual authentication in existing works. In [7], LBZ scheme is used to sign messages during mutual authentication. Suppose that the sizes of code HR of vehicle's home region, nonce nc, and join request $join$ are 20 bits and ciphertext E_{pk} of vehicle's real identity is 320 bits; then the length of vehicle's pseudo-identity $T\|E_{pk}\|HR\|ID_U$ is 20+320+20+160=520 bits. Then message $(ID, PS, t, join, Sign(PS, t))$ sent by vehicle is 160+520+20+20+800=1520 bits. The offline signature of LBZ scheme actually could be preloaded by vehicle, so the message $(ID, t, PS, ID_r, nc, Sign(ID_r, t))$ returned from RSU is 160+20+520+160+20+800=1680 bits. The total communication overhead is 3200 bits. The computation overhead is $3T^{LBZ}_{vrfy} + T^{LBZ}_{sign} + T'^{LBZ}_{sign} = 3 * (3T_m + 2T_a) + 540T_a + 180T_a$, where T^{LBZ}_{sign} is correlated to the length of input.

In [13], the computational overhead of protocol is $T^{ZWD}_{vrfy} + T^v_{gen} + T^r_{proc} + T^v_{dec} = 2T_p + 6T_{pm} + T_{pa} + 6T_h + 4T_{aes} + T_{query} \approx 2T_p + 6T_{pm} + T_{pa}$. Suppose that the length of authentication key λ is 160 bits, element $F \in \mathbb{G}$ is 1024 bits, then message (F, ID, C, t) sent by vehicle is 1024+160+(160+20)+20=1384 bits, where $C = \mathrm{Enc}(\lambda, t)$. RSU returns message (H, C') which is 160+(20+160+160)=500 bits long to vehicle. Since RSU has to forward message sent by vehicle to TA, then the communication overhead is 1384∗2+500=3268 bits.

Table 3 shows the comparison of computation and communication overhead of mutual authentication between vehicle and RSU, where computation overhead is represented as the multiples of T_a. The improvement on computation is $(2886T_a - 1920T_a)/2886T_a \approx 33.5\%$ over [7] and $(10300T_a - 1920T_a)/10300T_a \approx 81.4\%$ over [13]. In communication overhead, there are $(3200 - 1820)/3200 \approx 43.1\%$ and $(3268 - 1820)/3268 \approx 44.3\%$ improvements over [7] and [13], respectively.

7.3. Secret Parameters Update Efficiency. At the beginning of update secret parameters, TA has to compute 3∗320=960-bit long pseudo-identity PID_A first, which costs time $2T_m + T_a$ and then challenges $\widehat{R}, R^*$, element E, and signature $Sign_A$. The overall broadcast message is 960+320+320+320+20+480=2420 bits long and TA spends time $(2T_m + T_a) + 3T_m + T_m = 6T_m + T_a$ to generate it.

We assume that vehicle V_j has computed its PID_A in advance and could recognize the update instruction from TA immediately after receiving the broadcast message. Vehicle V_j first verifies the signature, picks new authentication key, and then responds TA with new authentication information (ID, F, t, C) which is 160+320+20+(320+160+320+160)=1460-bit long. This process would take $T^{HZS}_{vrfy} + 4T_m + 3T_h + T_{aes} \approx 7T_m + 2T_a$.

After receiving the authentication information from vehicle V_j, TA needs to spend time $T_{aes} + T_m$ to check its integrity. If received information is complete and valid, TA has to prove to V_j that it possesses the latest information of V_j by broadcasting message $(PID_A, \overline{R}, \overline{P}, t, Sign)$whose length is 960+320+320+20+480=2100 bits. The time of generating message is $2T_m + T^{HZS}_{sign} = 3T_m$.

Finally, vehicle V_j takes $T^{HZS}_{vrfy} + T_m = 4T_m + 2T_a$ to verify the message sent by TA, and the procedure of secret parameters update is finished. Overall, the time cost on the vehicle side is $(7T_m + 2T_a) + (4T_m + 2T_a) = 11T_m + 4T_a$, and $(6T_m + T_a) + 3T_m = 9T_m + T_a$ on the TA side. The communication costs are 1460 bits and 2420+2100=4520 bits for vehicle and TA, respectively.

8. Conclusions

In this paper, we propose a practical framework of CPPA scheme that does not rely on ideal TPD and supports realistic TPD. This feature makes our framework more suitable for practical use. In addition to traditional security requirements, such as nonrepudiation and conditional privacy preservation, our framework also achieves nonframeability that prevents TA and RSUs from framing innocent vehicles. Performance analysis shows that our framework outperforms existing schemes in terms of mutual authentication.

Data Availability

The data of execution time supporting the findings of this study are from previously reported studies, which have been cited.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Key R&D Program of China under grants 2017YFB0802300, the National Natural Science Foundation of China [61702541, 61872087], the Young Elite Scientists Sponsorship Program by CAST [2017QNRC001], and the Science Research Plan Program by NUDT [ZK17-03-46].

References

[1] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[2] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 246–250, IEEE, Phoenix, Ariz, USA, April 2008.

[3] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: a robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, 2009.

[4] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[5] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.

[6] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[7] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[8] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.

[9] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[10] J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Proceedings of the International Conference on Research in Smart Cards*, pp. 200–210, Springer, Berlin, Germany, 2001.

[11] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the Annual International Cryptology Conference*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397, Springer, Berlin, Germany, 1999.

[12] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008.

[13] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016.

[14] S.-J. Horng, S.-F. Tzeng, Y. Pan et al., "B-SPECS+: batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 1229–1237, IEEE, April 2008.

[16] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: prediction-based authentication for vehicle-to-vehicle communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 71–83, 2016.

[17] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2526–2536, 2018.

[18] A. Perrig, R. Canetti, D. J. Tygar et al., "The TESLA broadcast authentication protocol," *Rsa Cryptobytes*, vol. 5, no. 2, pp. 2–13, 2002.

[19] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009*, pp. 1–9, IEEE, Italy, June 2009.

[20] Q. Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010.

[21] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

[22] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

[23] K.-A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[24] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.

[25] J. Liu, Y. Yu, Y. Zhao et al., "An efficient privacy preserving batch authentication scheme with deterable function for VANETs," in *Proceedings of the International Conference on Network and System Security*, pp. 288–303, Cham, Swizerland, 2018.

[26] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, L. R. Knudsen, Ed., vol. 2332 of *Lecture Notes in Computer Science*, pp. 45–64, Springer, Berlin, Germany, 2002.

[27] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[28] S. Xu, Y. Mu, and W. Susilo, "Efficient authentication scheme for routing in mobile ad hoc networks," in *Proceedings of the International Conference on Embedded and Ubiquitous Computing*, vol. 3823 of *Lecture Notes in Computer Science*, pp. 854–863, Springer, Berlin, Germany, 2005.

[29] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287–296, 2010.