IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received May 6, 2020, accepted May 22, 2020, date of publication May 26, 2020, date of current version June 8, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2997840*

# AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs

**YANJI JIANG[1], SHAOCHENG GE[2], AND XUELI SHEN[1]**
[1]Software College, Liaoning Technical University, Huludao 125000, China
[2]College of Safety and Emergency Management Engineering, Taiyuan University of Technology, Taiyuan 030000, China

Corresponding author: Yanji Jiang (jyjvip@126.com)

This work was supported by the National Natural Science Foundation of China under Grant 51274116.

**ABSTRACT** As special ad-hoc networks, vehicular ad-hoc networks (VANETs) support vehicles to communicate with each other via opportunistic wireless links. In order to protect privacy of drivers, vehicles registered in VANETs are required to authenticate and communicate with surrounding vehicles or roadside infrastructure anonymously. However, due to high-speed driving and wireless environment, it is vital to propose a privacy protection scheme that is able to balance security and efficiency. Consequently, this paper proposes an anonymous authentication scheme in VANETs (AAAS). Specifically, we add region trust authority to provide more efficient anonymous authentication service for vehicles. Subsequently, group signature mechanism is adopted to achieve anonymity and conditional privacy. Moreover, security and performance analysis show that AAAS has higher security and efficiency.

**INDEX TERMS** VANETs, group signature, anonymous authentication, SVO.

## I. INTRODUCTION

With the rapid development of wireless communication technology, intelligent transportation systems (ITSs) plays a crucial role in improving transportation safethy and enhancing producivity [1]. Recently, as providing stable communication services for vehicles, VANETs have extensive attention in ITSs. Generally, driving vehicles with OBU should inform surrounding vehicles and roside infrastures of their position, direction and velocity [2]. Meanwhile, as collectors, vehicles can integrate and analyze received information, so as to avoid congested road and prevent accidents. However, due to the wireless network communication environment, it's easy for attackers to intercept, tamper and replay the transmitted messages, which gives a risk to security and reliability of VANETs [3]. According to [4], authentication is considered to be the most reliable mechanism to ensure the legitimacy of entities in VANETs. Before data exchange, the legality of each 4̂extcolorredsender's identity must be verified, which can effectively prevent the security threat caused by adversaries attacks. Since adversaries can collect safety information broadcast by vehicle, it is likely for adversaries to obtain trajectory of vehicle and violate the personal privacy of the driver over time [5]. Thus, vehicles have to broadcast security messages anonymously to prevent being tracked. Consequently, proposing a secure and efficient anonymous authentication and communication scheme has become an important factor in the rapid popularization of VANETs.

Recently, many anonymous authentication schemes have been proposed to ensure the security in vehicle to infrastructure (V2I) communication. Symmetric cryptography, asymmetric cryptography, and group signature, are thought as main mechanisms to achieve anonymous authentication in VANETs.

For schemes based on symmetric cryptography, in [6], an authority called ombudsman (OM) issues a unique identity and a seed value to each vehicle. Each vehicle and OM can calculate a set of pseudonymous handles depending on seed values. Meanwhile, roadside units (RSUs) can provide the service of generating short-term pseudonyms for vehicles according to the handle. However, as all messages generated by vehicles using short-term pseudonym can only be verified by RSUs, receiver has to send these messages to RSU for verification, which increases delay and extra communication overhead. In [7], a prediction-based authentication for vehicle-to-vehicle communications (PBA) is designed by using symmetric cryptography mechanism. PBA adopts vehicle position prediction mechanism to integrate location prediction result into and generate beacon messages in advance to guarantee efficiency of signature verification. Besides,in

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran.

order to reduce storage cost, PBA requests vehicles to use local keys and construct new temporary signatures. However, PBA is based on the accurate prediction of vehicle position, without considering how to achieve mutual authentication if the vehicle position prediction fails. In addition, symmetric cryptography is less flexible than asymmetric cryptography when it comes to the realization of authentication capabilities.

Pseudonym issue and authentication process of the schemes based on asymmetric cryptography mechanism are similar to the PKI mechanisms. In [8], Trust authority (TA) issues public key, private key, activation key and vehicle license to vehicle. And each vehicle is able to generate anonymous certificate based on message from TA that is easily verified by other vehicles. In addition, the scheme proposes an effective mechanism to enable RSU to achieve batch authentication of multiple vehicles when vehicle sender enters the area covered by a RSU and requests network service from the RSU. However, according to [9], for the purpose of privacy protection, vehicles are required to change pseudonyms and certifies frequently. In this step, vehicles must communicate with TA, which leads to high computational overhead and communication costs. Moreover, Hardly can it guarantee the high-speed vehicles to receive new certificates in time. Reference [10] proposes an efficient anonymous authentication (EAAP), which enable vehicles to generate pseudonyms independently. In EAAP, vehicle can use authorization key (AK) obtained from TA to generate anonymous certificates, which improves communication cost of changing anonymous certificates in the traditional scheme. Nevertheless, in order to protect the privacy of vehicles, vehicles are required to generate anonymous certificates frequently while communicating with other entities to request services. According to [11], due to the limited vehicle computing and storage capacities, EAAP has to meet the huge challenge in performance. To reduce computation cost in authentication, [12] proposes an identity (ID)-based signature (IBS) scheme (CPAS) to support anonymous authentication. Instead of Map To Point function, CPAS uses general hash functions to keep a balance between privacy security and operation. Furthermore, CPAS supports batch verification to improve efficiency of RSU authentication. Unfortunately, CPAS does not propose an effective revocation mechanism for illegal vehicles. Once vehicles are compromised, the threats facing VANETs cannot be ignored. In LIAP [13], Wang and Yao presented a local identity-based anonymous authentication protocol. Not only does the scheme has low computational cost but also it supports the batch signature verification. However, RSU is requested to distribute certificates to vehicles's identity and maintain vehicle identity, the scheme will confront a huge challenge, without sufficient computation and storage capacity.

In anonymous authentication scheme based on group signature, VANETs are composed of multiple groups, and each group manager is thought to be trustworthy. Generally, group members can generate signatures without revealing their real identity. In [14], anonymous certificate is cancelled and RSUs are considered as group leaders to provide anonymous authentication service for vehicles, which is able to effectively improve the transmission and communication costs caused by certificate issuance and revocation. However, [14] could not meet the security requirements of distributed resolution authority. Since RSUs has already saved privacy information of vehicles, once a RSU compromises, each vehicle privacy is at risk of being exposed. Reference [15] proposes a secure vehicular network communication schemes (GIGS) through combining group signatures and identity-based signature. GIGS adopts group signature and reduces vehicle information storage overhead. Apart from that, GIGS uses identity-based signature to release public key and certificate management pressure. However, once there are illegal vehicles in the network, the scheme does not provide an effective mechanism for illegal vehicles revocation. [16] adds regional group manager to support vehicles update their identifies and group secret keys periodically. In credential revocation, which decreases TA revocation cost significantly. Nevertheless, in anonymous authentication, a large number of point multiplication and bilinear pairing are executed, which makes the scheme inefficient. Ring signature, as a special group signature, is used in the scheme [17] for vehicle anonymous authentication. In [17], vehicles can generate ring signature independently without the help of RSUs or TA. In addition, identities of all members can be changed quickly without consent or messaging. However, the scheme does not mention how to disclose each illegal vehicle identity and trajectory, which is unable to solve the credential revocation of illegal vehicles. Reference [18] adopts a batch group signature scheme to achieve effcient message signature verifcation and propose group session key (GSK)-based revocation strategy (GSSA) to achieve fast vehicle revocation check. In terms of computation time cost, message delay and loss rate, GSSA is efficient. What is more, GSSA is able to resist to impersonation attacks, tracking attacks, sybil attacks, and replay attacks. However, due to lack of challenge value in signature, GSSA does not recognize the trustworthiness of the sender's message content, which causes vehicle could not verify the legal of the response from RSU.

To solve above problems, we propose an anonymous authentication scheme based on group signature in VANETs (AAAS). AAAS consists of four phases: system initialization, initial registration, initial V2I authentication, and handover V2I authentication.The main features of the proposed paper are as follows.

- AAAS adds region trust authority (RTA) as group manager to provide anonymous authentication and communication services for vehicles, which can effectively improve the computation and communication costs of TA and relieve the pressure of RSU with low computation and storage capacity.
- Pseudonym mechanism and group signature mechansim are integrated into the scheme to satisfy distrubuted resolution. Single authority cannot directly resolve the real identity, which effectively reduces the

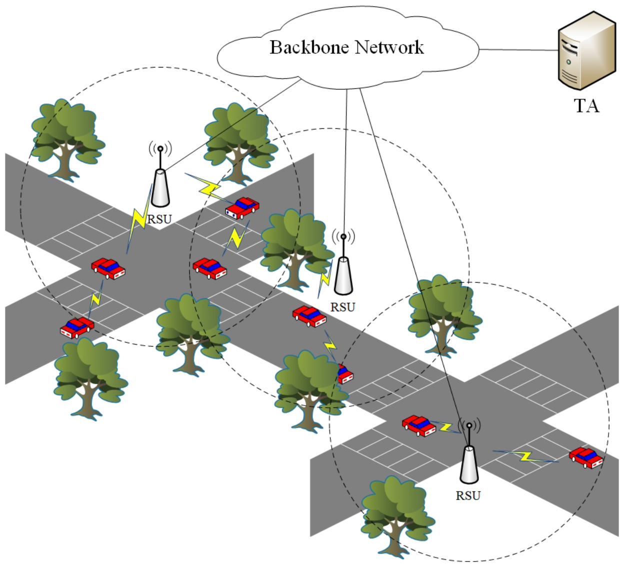



**FIGURE 1.** VANETs architecture.

risk of vehicle privacy exposure once an authority is compromised.
- Security and performance analysis show that AAAS can maintain a balance between efficiency and security well.

The rest of this paper is organized as follows. In Section II, we outline necessary preliminaries. The proposed scheme is elaborated in section III, followed by security proof and analysis in section IV. Section V evaluates the performance of the proposed scheme through communication overhead, computation cost, and signaling cost. Finally, we draw our conclusion and future work in section VI.

## II. PRELIMINARIES

### A. VANETs

As a vital part of intelligent transportation system (ITS), vehicular ad-hoc networks (VANETs) are able to use wireless communication technologies to support continuous and stable network communication service [19]. As shown in Figure 1, VANETs consist of three important entities: trust authority (TA), roadside units (RSUs), and vehicles equipped with on board units (OBUs) [20]. TA is usually regarded as a trust third party, which is trusted by all entities in VANETs. Security and reliability of TA are the basis for establishing a mutual trust relationship among other entities in VANETs. RSUs deployed on both sides of the road have high storage and computation capacity. RSUs can provide safety-related services, efficiency-related services, and entertainment-related services for vehicles through wireless communication. OBUs, installed in vehicles, can support the information exchange with RSUs or other OBUs to obtain required services.

### B. BILINEAR PAIRING

Let $G_1$ be an additive group of prime order $q$, generated by $P$, and let $G_T$ be a multiplicative group with the same $q$. A bilinear pairing is a map:

$$e : G_1 \times G_1 \rightarrowtail G_T$$

The pairing $e$ satisfies the following properties [21]:

1) Bilinearity: For any $P, Q \in G_1, a, b \in \mathrm{Z}_\mathrm{q}^*$, $e(aP, bQ) = e(P, Q)^{ab}$.
2) Non-degeneracy: Existing $P, Q \in G_1$ satisfies $e(P, Q) = 1$.
3) Computability: There is an efficient algorithm to compute $e(P, Q)$, where $P, Q \in \mathrm{G}_1$.

### C. IDENTITY-BASED GROUP SIGNATURE

Group signature is considered as a special signature mechanism, in which authorized members can sign on behalf of the underlying group [22]. For a given group signature, any unauthorized entity can use group public key to verify whether the signature is legal, but it is impossible for any other verifier except for group manager to reveal the signer's identity. Consequently, group signature mechanism can be effectively used in anonymous authentication in VANETs [23]. However, in traditional group signature schemes, any verifier has to determine the validity of the group public key certificate before verifying the group signature, which may influence the efficiency and stability of communication for high-speed vehicles. In addition, due to limited computing and storage capacity of vehicles, the overhead of storing certificates for vehicles is also not negligible. Consequently, identity-based group signature is adopted in the proposed scheme, where publicly group mamanger identifier can be used as the public group key component [24]. To reduce the burden of public key certificate management, verifier only needs to know the identity of the group manager to compute the group public key.

The earliest identity-based group signature mechanism was proposed by Park *et al.* [25]. However, due to its high computation cost and low efficiency, it is difficult to be used in anonymous authentication in VANETs. Han *et al.* proposed a novel identity-based group signature scheme [26], which makes a balance between the security and effciency. In the perposed scheme, [26] is used in anonymous authentication and communication in VANETs. The details of the scheme are as follows.

1) Setup. Let $G_1$ and $G_T$ be two cyclic groups generated by $P$, whose order is prime $q$, where $G_1$ is additive group and $G_T$ is multiplicative group. The group manager (GM) chooses two cryptographic hash functions: $H_1 : \{0, 1\}^* \rightarrow G_1$, $H_2 : \{0, 1\}^* \times G_1 \rightarrow G_1$ and constructs a bilinear function $e$: $\mathrm{G}_1 \times \mathrm{G}_1 \rightarrow G_T$. Then, GM generates $a \in Z_q^*$ as the secret key of GM and sets $P_{pub} = aP$ as the public key of group.
2) Extract. When a new member $U_i$ wants to be an authorized member of the group, the member is requested to sent its identity $f_i$ to GM through the secure tunnel. GM computes $Q_{f_i} = H_1(f_i)$, $sk_i = aQ_{f_i}$ and sends $sk_i$ to $U_i$. After receiving $sk_i$, $U_i$ chooses a secret key $b_i$ as its

personal private key. Support $b_i f_i \equiv 1 \; mod \varphi(n)$. Now. $U_i$ is considered as a member of the group. Its private key is $\{b_i, sk_i\}$ and public key is $f_i$.

3) Sign. For given a message $M$, signer chooses $x \in Z_q^*$ and computes $A = xP$, $B = x^{-1} sk_i + H_2(m, A) b_i$. The group signature on message $M$ is $\{A, B, f_i\}$.
4) Verify. After receiving $M$ and group signature $\{A, B, f_i\}$, verifier carries out the followings to verify the group signature.
   a) Compute $\alpha = e(f_i P_{pub}, f_i)$, $\beta = e(A, f_i B)$, and $\gamma = e(A, H_2(M, A))$ respectively.
   b) Check $\beta == \alpha\gamma$ to verify whether the group signature $\{A, B, f_i\}$ legal.

   If the equality holds, then $\{A, B, f_i\}$ is thought as a valid group signature; Otherwise, the signature is rejected.

## III. THE PROPOSED SCHEMES

In this section, AAAS network architecture, trust model, system initialization, initial registeration, V2I initial authentication, and V2I handover authentication are described. We adopt identity based on signature mechanism (CC signatute [27]), Diffie-Hellman key exchange mechanism [28], and AES cipher mechanism [29] to support anonymous authenticaion and communication. Before introducing AAAS, a few of relevant abbreviations and descriptions used frequently are illustrated in Table 1.

### A. NETWORK ARCHITECTURE

Figure 2 shows the network architecture of the proposed scheme, which includes four types of entities, name, trusted authority (TA), region trusted authority (RTA), RSU, and vehicle.

- TA: As a trusted third-party entity, TA generates system parameters, issues private keys for RTA, and computes pseudonyms and private keys for vehicles. In addition, TA also maintains an identity list of vehicles and provides services for illegal vehicle revocation.
- RTA: In order to alleviate TA computation and communication pressure, in AAAS network architecture, RTA is added to manage all RSUs in each area and provides anonymous authentication and communication services for vehicles.
- RSUs: RSUs are usually deployed on both sides of the road to provide related safety services and entertainment services for legal vehivles on the road through wireless communications.
- Vehicles: For obtaining network service provided by VANETs, each vehicle equipped with OBU is able to to exchange information with surrounding RSUs and vehicles, so as to enjoy better driving experience for drivers.

### B. TRUST MODEL

The trust model of the proposed scheme is described in Figure 3. TA is trusted by all entities in VANETs. Other entities

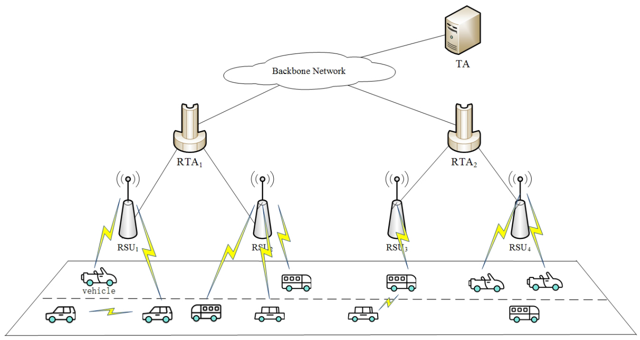



**FIGURE 2. Network architecture.**

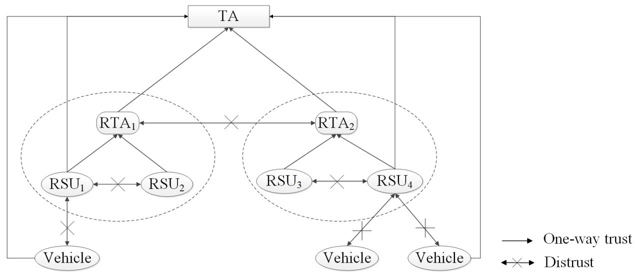



**FIGURE 3. Trust model.**

need to submit true identities to apply for registration. Keeping security and reliability of TA is the basis to establish trust relationship among other entities in VANETs. RTA is requested to register with TA to establish trust relationship with TA. Meanwhile, RTA is trusted by all RSUs in the assigned areas, but there is no trust relationship between RTAs. RSU trusts TA and RTA in its area but not vehicles. Besides, RSU does not trust other RSUs. All vehicles trust TA, but vehicles do not trust other vehicles and RSUs. The purpose of the proposed scheme is to establish the trust relationship between vehicles and RSUs anonymously.

### C. SYSTEM INITIALIZATION

In terms of the network architecture and trust model, system initialization is executed as follows.

- TA selects two cyclic groups $G_1$ and $G_T$ generated by $P$, whose order is a prime $q$, where $G_1$ is an additive group and $G_T$ a multiplicative group.
- TA chooses a bilinear pairing $e : G_1 \times G_1 \rightarrow G_T$ and three hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$, $H_2 : \{0, 1\}^* \times G_1 \rightarrow G_1$, $H_3 : \{0, 1\}^l \times Z_q^* \rightarrow \{0, 1\}^l$.
- TA generates a master key $s \in Z_q^*$ and computes public key $PK_{TA} = sP$.
- TA publishes the parameter $param = \{G_1, G_T, e, q, P, PK_{TA}, H_1, H_2, H_3\}$ and stores $s$.

### D. INITIAL REGISTERATION PROTOCOL

#### 1) VEHICLE REGISTERATION PROTOCOL

1) Vehicle first randomly picks a secret key $a \in Z_q^*$, challenge value $N_1$, and computes key-agreement

**TABLE 1. Abbreviations and descriptions.**

| Abbreviation | Description |
|---|---|
| $ID_A$ | The true identity of entity A |
| $PS_A$ | The pseudonym of entity A |
| $PK_A/SK_A$ | The public key/privacy key of entity A |
| $K_{A-B}$ | The shared key between entity A and entity B |
| $C_{A-B}$ | The ciphertext generated by entity A to entity B |
| $Sign_A$ | A's signature |
| $TS$ | The current timestamp |
| $N$ | Random number |
| $Exp_A$ | pseudonym expiration of entity A |
| $Enc\_PK_A\{M\}$ | Using $PK_A$ to encrypt message $M$ |
| $Sign\_SK_A\{M\}$ | Using the $SK_A$ to sign message $M$ |
| $Sign\_group\_SK_A\{M\}$ | Using $SK_A$ to sign message $M$ through group signature mechanism |
| $Enc\_K_{A-B}\{M\}$ | Using symmetric key $K_{A-B}$ to encrypt message $M$ |
| $\|\|$ | Connection operations between message |
| $Z_q^*$ | Set of prime numbers |
| $ab$ | Point multiplication operation |

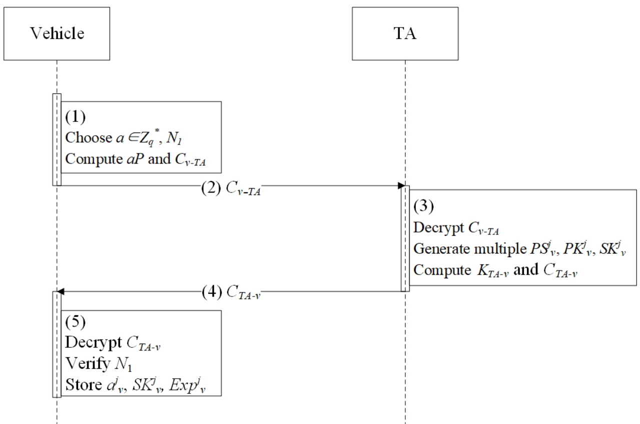



**FIGURE 4. Vehicle registeration protocol.**

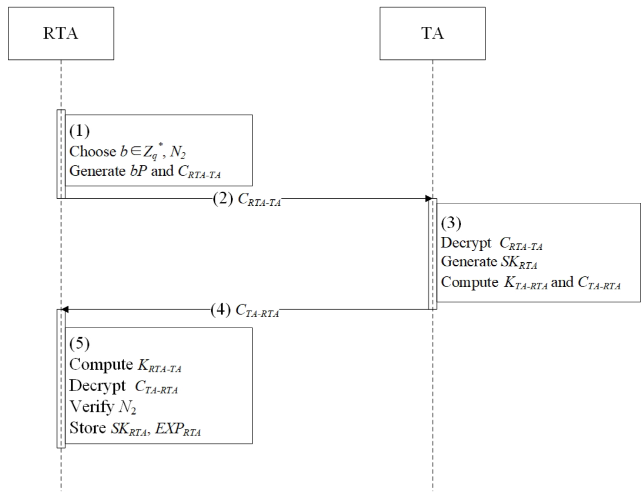



**FIGURE 5. RTA registration protocol.**

parameter $aP$, then vehicle uses the public key of TA to encrypt $< ID_v, aP, N_1 >$ and gets $C_{v-TA} = Enc\_PK_{TA}\{ID_v, aP, N_1\}$.

2) Vehicle sends the ciphertext $C_{v-TA}$ to TA.
3) When obtianing the ciphertext from vehicle, TA uses master key $s$ to decrypt $C_{v-TA}$ and gets $ID_v$, $aP$, and $N_1$. TA selects multiple random numbers $d_v^j \in Z_q^*$ to compute vehicle's pseudonyms $PS_v^j = H_3(ID_v, d_v^j)$ and corresponding public keys $PK_v^j = H_1(PS_v^j||Exp_v^j)$ and private keys $SK_v^j = sPK_v^j$, where $Exp_v^j$ is the expiration of $d_v^j$, $1 < j < n$, $n$ is the total number of each vehicle obtaining pseudonym. Then TA computes the session key with vehicle $K_{TA-v} = saP$ and encrypts $< d_v^j, SK_v^j, Exp_v^j, N_1 >$ to get $C_{TA-v} = Enc\_K_{TA-v}\{d_v^j, SK_v^j, Exp_v^j, N_1\}$. Finally, TA stores $< ID_v, d_v^j, SK_v^j, Exp_v^j >$.
4) TA sends $C_{TA-v}$ to vehicle.
5) After receiving $C_{TA-v}$ from TA, vehicle computes the session key with TA $K_{v-TA} = aPK_{TA}$ and decrypts $C_{TA-v}$ to get $< d_v^j, SK_v^j, Exp_v^j, N_1 >$. Vehicle verifies $N_1$, if the verification is successful, vehicle stores $< d_v^j, SK_v^j, Exp_v^j >$. Otherwise, vechicle needs to reapply for registration.

## 2) RTA REGISTRATION PROTOCOL

1) RTA selects a random number $b \in Z_q^*$ as its secret key and computes key-agreement parameter $bP$. RTA then computes ciphertext $C_{RTA-TA} = Enc\_PK_{TA}\{ID_{RTA}, bP, N_2\}$, where $N_2$ is a challenge value.
2) RTA sends $C_{RTA-TA}$ to TA.
3) Upon receiving the ciphertext, TA first decrypts $C_{RTA-TA}$ to get $< ID_{RTA}, bP, N_2 >$. TA computes the private key of RTA: $SK_{RTA} = sPK_{RTA}$, where $PK_{RTA} = H_1(ID_{RTA}||Exp_{RTA})$ is the public key of RTA, $Exp_{RTA}$ is the expiration of $SK_{RTA}$. Finally, TA computes the session key with RTA $K_{TA-RTA} = sbP$ and encrypts $< SK_{RTA}, Exp_{RTA}, N_2 >$ to get $C_{TA-RTA} = Enc\_K_{TA-RTA}\{SK_{RTA}, Exp_{RTA}, N_2\}$.
4) TA sends $C_{TA-RTA}$ to RTA.
5) When getting the ciphertext from TA, RTA computes the session key with TA $K_{TA-RTA} = bPK_{TA}$ to encrypt $C_{TA-RTA}$ and gets $< SK_{RTA}, Exp_{RTA}, N_2 >$. RTA confirms the validity of $N_2$. If it is not valid, then RTA stores $< SK_{RTA}, Exp_{RTA} >$. Otherwise, RTA registration is failed.

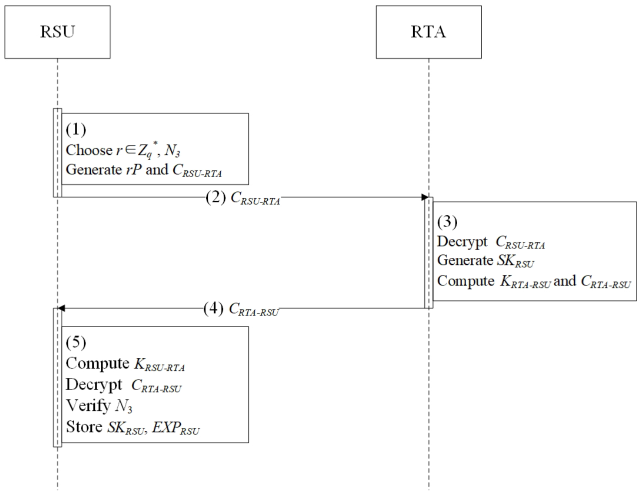



**FIGURE 6.** RSU registration protocol.

### 3) RSU REGISTRATION PROTOCOL

In order to reduce the computation and communication pressure of TA, All RSUs are required to submit their registration applications to RTA in their area. Before RSU registration protocol is executed, RTA first chooses $SK'_{RTA} = b$ and $PK'_{RTA} = bP$ as group public/private key that are valid only in its area. Then RTA uses $SK_{RTA}$ to sign $PK'_{RTA}$ and gets $Sign_{RTA} = Sign\_SK_{RTA}\{ID_{RTA}, Exp_{RTA}, PK'_{RTA}\} = \{V_{RTA}, W_{RTA}\}$, where $V_{RTA} = r_{RTA}PK_{RTA}$, $W_{RTA} = (r_{RTA} + H_2(M, V_{RTA}))$, $M = ID_{RTA}||Exp_{RTA}||PK'_{RTA}$, $r_{RTA} \in Z_q^*$ is random number. Finally, RTA broadcasts messages $ID_{RTA}$, $Exp_{RTA}$, $PK'_{RTA}$ and $Sign_{RTA}$ to RSUs in its area. When receiving the message from RTA, RSU computes the public key of RTA: $PK_{RTA} = H_1(ID_{RTA}||Exp_{RTA})$, then RSU verifies $Sign_{RTA}$, if $Sign_{RTA}$ is legal, RSU stores $ID_{RTA}$, $Exp_{RTA}$, $PK'_{RTA}$, and $Sign_{RTA}$ and executes registration protocol. Figure 6 shows the details.

1) Each RSU generates a secret key $r \in Z_q^*$ randomly and calculate $rP$ as key-agreement parameter with RTA. After that, RSU generates ciphertext $C_{RSU-RTA} = Enc\_PK'_{RTA}\{ID_{RSU}, rP, N_3\}$, where $N_3$ is a random number as a challenge value.
2) RSU sends $C_{RSU-RTA}$ to RTA.
3) RTA decrypts $C_{RSU-RTA}$ and gets $< ID_{RSU}, rP, N_3 >$. Then RTA generates RSU's private key $SK_{RSU} = bPK_{RSU}$, where $PK_{RSU} = H_1(ID_{RSU})$. After that, RTA computes the session key $K_{RTA-RSU} = brP$ and $C_{RTA-RSU} = Enc\_K_{RTA-RSU}\{SK_{RSU}, Exp_{RSU}, N_3+1\}$, where $Exp_{RSU}$ is the expiration of $SK_{RSU}$.
4) RTA sends $C_{RTA-RSU}$ to RSU.
5) RSU computes the session key with RTA $K_{RTA-RSU} = bPK'_{RTA}$ and encrypts $C_{RTA-RSU}$ to get $SK_{RSU}$, $Exp_{RSU}$, $N_3 + 1$. If $N_3 + 1$ is valid, RSU stores $SK_{RSU}$, $Exp_{RSU}$. Otherwise, RSU is requested to re-apply for registration.

### E. V2I INITIAL AUTHENTICATION PROTOCOL

V2I initial authentication refers to the process that vehicle performs mutual authentication with RSU ($RSU_1$) when entering the coverage of $RSU_1$ for the first time. The details are shown as Figure 7.

1) $RSU_1$ broadcasts $ID_{RSU_1}$, $Exp_{RTA}$, $Exp_{RSU_1}$, $TS_1$, $N_4$, $ID_{RTA}$, $PK'_{RTA}$, $Sign_{RSU_1}$, and $Sign_{RTA}$ regularly, where $Sign_{RSU_1} = Sign\_SK_{RSU_1}\{ID_{RSU_1}, ID_{RTA}, Exp_{RSU_1}, TS_1, N_4\} = \{V_{RSU_1}, W_{RSU_1}\}$, $V_{RSU_1} = r_{RSU_1}PK_{RSU_1}$, $W_{RSU_1} = (r_{RSU_1}+H_2(M, V_{RSU_1}))SK_{RSU_1}$, $r_{RSU_1} \in Z_q^*$ is random number, $M = ID_{RSU_1}||ID_{RTA}||Exp_{RSU_1}||TS_1||N_4$, $N_4$ is challenge value.
2) When receiving the message from $RSU_1$, vehicle first computes $PK_{RTA} = H_1(ID_{RTA}||Exp_{RTA})$, and verifies $Sign_{RTA}$, if $Sign_{RTA}$ is illegal, then the authentication is failed, otherwise $PK'_{RTA}$ is considered valid. Then vehicle continues to check the freshness of $TS_1$ and verify the validity of signature $Sign_{RSU_1}$. If the validation is successful, RTA and $RSU_1$ are thought as legal entities. Vehicle chooses $r_v \in Z_q^*$ and computes the session key with $RSU_1$: $K_{v-RSU_1} = r_vV_{RSU_1}$ and the session key with $RTA$: $K_{v-RTA} = r_vV_{RTA}$ respectively. Finally, vehicle chooses $PS_v^j$ and generates signature $Sign_v = Sign\_SK_v^j\{PS_v^j, Exp_v^j, TS_2, N_5, N_6\} = \{V_v, W_v\}$, ciphertext $C_{v-RSU_1} = Enc\_K_{v-RSU_1}\{N_4\}$, and $C_{v-RTA} = Enc\_K_{v-RTA}\{N_6\}$, where $V_v = r_vPK_v^j$, $W_v = (r + H_2(M, V))SK_v^j$, $M = PS_v^j||Exp_v^j||TS_2||N_5||N_6$, $N_5$ and $N_6$ are challenge values.
3) vehicle sends $PS_v^j$, $Exp_v^j$, $TS_2$, $N_5$, $N_6$, $Sign_v$, $C_{v-RSU_1}$, and $C_{v-RTA}$ to $RSU_1$.
4) Once the message from vehicle is received, $RSU_1$ verifies $Exp_v^j$, $TS_2$, and $Sign_v$ respectively. If all the verifications are successful, $RSU_1$ regards vehicle as a legal node and generates the session key with vehicle $K_{RSU_1-v} = r_{RSU_1}V_v$ to decrypt $K_{v-RSU_1}$ and checks $N_4$. Finally $RSU_1$ computes $C_{RSU_1-v} = Enc\_C_{v-RSU_1}\{N_5\}$.
5) $RSU_1$ sends $PS_v^j$, $Exp_v^j$, $N_6$, and $C_{v-RTA}$ to RTA.
6) When receiving the message from $RSU_1$, RTA first computes the session key with vehicle $K_{RTA-v} = r_{RTA}V_v$ and decrypts $C_{v-RTA}$ to obtain $N_6$. If $N_6$ is legal, RTA generates multiple group identities $f_v^i$, and group private keys $SK_{f_v^i} = \{b_i, sk_i\}$ for vehicle. Finally, RTA encrypts $f_v^i$, $SK_{f_v^i}$, and $N_5$ to get $C_{RTA-v} = Enc\_K_{RTA-v}\{f_v^i, SK_{f_v^i}, Exp_{f_v^i}, N_6\}$, where $Exp_{f_v^i}$ is the expiration of $f_v^i$.
7) RTA sends $C_{RTA-v}$ to $RSU_1$.
8) $RSU_1$ sends $C_{RSU_1-v}$ and $C_{RTA-v}$ to vehicle.
9) Vehicle decrypts $C_{RSU_1-v}$ and verifies $N_5$, if $N_5$ is legal, then the secure channel between vehicle and $RSU_1$ is built. Then $C_{RTA-v}$ is decrypted to get $f_v^i$, $SK_{f_v^i}$, $Exp_{f_v^i}$, and $N_6$. If $N_6$ is legal, the vehicle is identified as a group member of RTA, vehicle saves $f_v^i$, $SK_{f_v^i}$, and $Exp_{f_v^i}$.

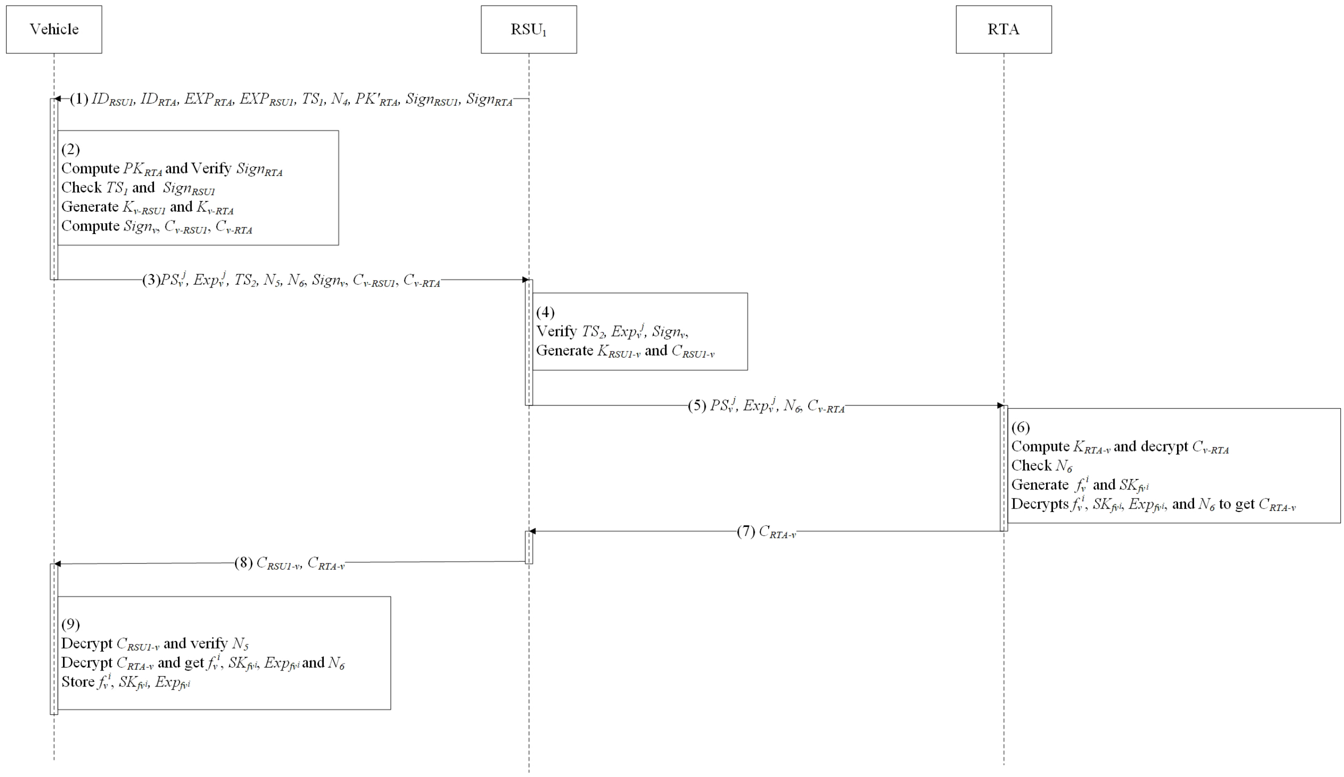



**FIGURE 7.** **V2I initial authentication protocol.**

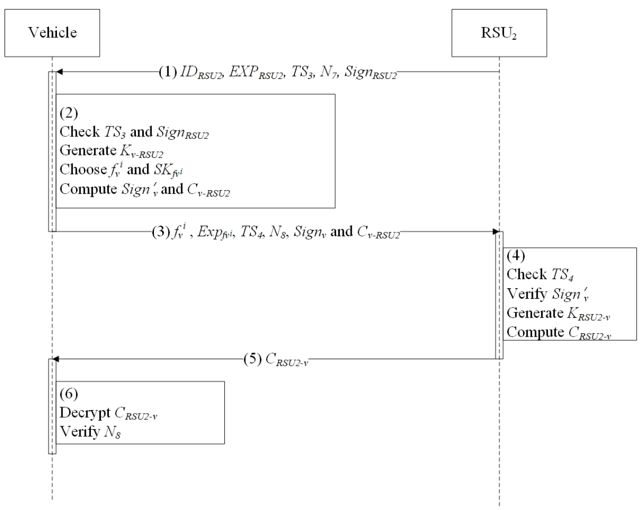



**FIGURE 8.** **V2I handover authentication protocol.**

### *F. V2I HANDOVER AUTHENTICATION PROTOCOL*

When vehicle leaves RSU$_1$ and enters the area covered by RSU$_2$ signal. V2I handover authentication is required to execute. The details are shown as following.

1) RSU$_2$ broadcasts $ID_{RSU_2}$, $Exp_{RSU_2}$, $TS_3$, $N_7$, $Sign_{RSU_2}$, regularly, where $Sign_{RSU_2} = Sign\_SK_{RSU_2}\{ID_{RSU_2}, Exp_{RSU_2}, TS_3, N_7\} = \{V_{RSU_2}, W_{RSU_2}\}$, $V_{RSU_2} = r_{RSU_2} PK_{RSU_2}$, $W_{RSU_2} = (r_{RSU_2} + H_2(M, V_{RSU_2}))SK_{RSU_2}$, $r_{RSU_2} \in Z_q^*$ is random number, $M = ID_{RSU_2}||Exp_{RSU_2}||TS_3||N_7$.
2) Once the message from RSU$_2$ is received, vehicle verifies whether $TS_3$ is fresh. If $TS_3$ is not fresh, the authentication is failed. Otherwise, vehicle continues to verify $Sign_{RSU_2}$. If the verification is successful, vehicle generates the shared key with RSU$_2$: $K_{v-RSU_2} = r_v V_{RSU_2}$. Vehicle selects its pseudonym $f_v^i$ and private key $SK_{f_v^i}$ to signs $< f_v^i, Exp_{f_v^i}, TS_4, N_8 >$: $Sign'_v = Sign\_group\_SK_{f_v^i}\{f_v^i, Exp_{f_v^i}, TS_4, N_8\} = \{V'_v, W'_v\}$, where $V'_v = r_v P$, $W'_v = r_v^{-1} sk_i + H_1(M, V'_v)b_i$, $M = f_v^i||Exp_{f_v^i}||TS_4||N_8$, $r_v \in Z_q^*$ is random number. Finally, vehicle encrypts $N_7$ to get $C_{v-RSU_2} = Enc\_K_{v-RSU_2}\{N_7\}$.
3) vehicle sends $f_v^i$, $Exp_{f_v^i}$, $TS_4$, $N_8$, $Sign'_v$, and $C_{v-RSU_2}$ to RSU$_2$.
4) RSU$_2$ first verifies the freshness of $TS_4$. Then $Sign'_v$ is verified through computing the public key of vehicle $PK_{f_v^i} = H_1(f_v^i||Exp_{f_v^i})$. If the verification is successful, the vehicle $f_v^i$ is considered as a legal vehicle. Otherwise, RSU$_2$ refuses the request from vehicle communication. Finally, RSU $_2$ generates the session key with vehicle: $K_{RSU_2-v} = r_{RSU_2} V'_v$ to verify $N_7$ and computes $C_{RSU_2-v} = Enc\_K_{RSU_2-v}\{N_8\}$.
5) RSU$_2$ sends $C_{RSU_2-v}$ to vehicle.
6) vehicle uses $K_{v-RSU_2} = r_v V_{RSU_2}$ to decrypt $C_{RSU_2-v}$. If $N_8$ is legal, then the trust relationship is established between vehicle and RSU$_2$, otherwise, handover authentication fails.

## IV. SECURITY PROOF AND ANALYSIS

In this section, security proof and analysis for AAAS are presented. We first use SVO logic to provide a formal security

**TABLE 2.** Notation and description in SVO.

| Notation | Description |
|---|---|
| $\vdash \varphi$ | $\varphi$ is a theorem |
| $\mathrm{PK}_\sigma(P, K)$ | $K$ is the public signature verification key for $P$ |
| $\mathrm{PK}_\delta(P, K)$ | $K$ is the public key-agreement key for $P$ |
| $\mathrm{SV}(X, K, Y)$ | $K$ can verify if $X$ is Y'signature |
| $\mathrm{F}(\mathrm{K_p}, \mathrm{K_q})$ | F is a key-agreement function |
| fresh($X$) | $X$ is fresh |
| $\{X\}K$ | The ciphertext encrypted by $K$ |
| $[X]K$ | The message signed by $K$ |

proof. Afterwards, we also give further security analysis to prove AAAS satisfies the security requirements in [30].

### A. SVO LOGIC

Recently, an increasing number of researchers use formal analysis method to evaluate security of their protocols and schemes. Among all proposed formal security analysis methods, SVO logic [31], as an important BAN-like logic, owns the advantages of BAN logic, GNY logic, and AT logic. Besides, SVO logic redefines some concepts in formal semantic and owns very simple inference rules or axioms. Now, SVO logic has become a widely used formal analysis method. In most cases, since vehicles and RSUs perform V2I handover authentication protocol, formal security proof in AAAS handover authentication is provided in this section. Relevant notations and descriptions are given as Table 2.

#### 1) INITIAL RULES

SVO has two inference rules:

Modus Ponens: From $\varphi$ and $\varphi \supset \psi$ infer $\psi$.
Necessitation: From $\vdash \varphi$ infer $\vdash P$ believes $\varphi$.

#### 2) SVO AXIOM SCHEMATA

For any principal $P$, $Q$ and formulae $\varphi$, $\psi$, the following axiom schemates are introduced.

(1) Believing
Ax1:$P$ believes $\varphi \wedge P$ believes $(\varphi \supset \psi) \supset P$ believes $\psi$
Ax2:$P$ believes $\varphi \supset P$ believes ($P$ believes $\varphi$)
(2) Source Association
Ax3:$SharedKey(K, P, Q) \wedge R$ received $\{X^Q\}_K \supset Q$ said $X \wedge Q$ sees $K$
Ax4:$(PK_\sigma(Q, K) \wedge R$ received $[X]K \wedge SV(X, K, Y)) \supset Q$ said $Y$
(3) Key Agreement
Ax5:$((PK_\delta(P, K_p) \wedge (PK_\delta(Q, K_q)) \supset SharedKey(F(K_p, K_q), P, Q)$
(4) Receiving
Ax6:$P$ received $(X_1, \cdots, X_n) \supset P$ receives $X_i$
Ax7:($P$ received $\{X\}_K \wedge P$ sees $K^{-1}) \supset P$ has X
(5) Seeing
Ax8:$P$ received $X \supset P$ sees $X$
Ax9:$P$ sees $(X_1, \cdots, X_n) \supset P$ sees $X_i$
Ax10:($P$ sees $X_1 \wedge \cdots \wedge P$ sees $X_n) \supset$ ($P$ sees $F(X_1, \cdots, X_n)$)
(6) Comprehending
Ax11:$P$ believes ($P$ sees $F(X)) \supset P$ believes ($P$ sees $X$)
Ax12:($P$ received $F(X) \wedge P$ believes $P$ sees $X) \supset P$ believes $P$ received $F(X)$
(7) Saying
Ax13:$P$ said $(X_1, \cdots, X_n) \supset (P$ said $X_i \wedge P$ sees $X_i)$
Ax14:$P$ says $(X_1, \cdots, X_n) \supset (P$ says $X_i \wedge P$ said $(X_1, \cdots, X_n))$
(8) Jurisdiction
Ax15:($P$ controls $\varphi \wedge P$ says $\varphi) \supset \varphi$
(9) Freshness
Ax16:$fresh(X_i) \supset fresh(X_1, \cdots, X_n)$
Ax17:$fresh(X_1, \cdots, X_n) \supset (F(X_1, \cdots, X_n))$
(10) Nonce-Verification
Ax18:($fresh(X) \wedge P$ said $X) \supset P$ says $X$
(11) Symmetric goodness of shared keys
Ax19:$SharedKey(K, P, Q) \equiv SharedKey(K, Q, P)$
(12) Having
Ax20:$P$ has $K \supset P$ sees $K$

#### 3) FORMAL DESCRIPTION

① Goals

In handover authentication protocol, the following SVO goals are given according to the security requirements of AAAS.

G1: Vehicle believes $\mathrm{RSU_2}$ says $(ID_{RSU_2}, Exp_{RSU_2}, TS_3, N_7)$
$\mathrm{RSU_2}$ believes vehicle says $(f_v^i, Exp_{f_v^i}, TS_4, N_8)$
G2: vehicle believes $\mathrm{RSU_2}$ says $N_8$
$\mathrm{RSU_2}$ believes vehicle says $N_7$
G3: Vehicle believes sharedkey($K_{v-RSU_2}-$, vehicle, $\mathrm{RSU_2}$)
$\mathrm{RSU_2}$ believes sharedkey($K_{RSU_2-v}-$, $\mathrm{RSU_2}$, vehicle)
G4: Vehicle believes sharedkey($K_{v-RSU_2}+$, vehicle, $\mathrm{RSU_2}$)
$\mathrm{RSU_2}$ believes sharedkey($K_{RSU_2-v}+$, $\mathrm{RSU_2}$, vehicle)
G5: Vehicle believes $fresh(K_{v-RSU_2})$
$\mathrm{RSU_2}$ believes $fresh(K_{RSU_2-v})$

(2) Assumptions

P1: Vehicle believes $fresh(TS_3)$
$\mathrm{RSU_2}$ believes $fresh(TS_4)$
P2: Vehicle believes vehicle received $(([ID_{RSU_2}, Exp_{RSU_2}, TS_3, N_7]SK_{RSU_2}) \supset PK_\delta(\mathrm{RSU_2}, r_{RSU_2}P))$
$\mathrm{RSU_2}$ believes $\mathrm{RSU_2}$ received $(([f_v^i, Exp_{f_v^i}, TS_4, N_8]SK_{vehicle}) \supset PK_\delta(vehicle, r_{f_v^i}P))$
P3: Vehicle believes vehicle received $\{\mathrm{N_8}\}\mathrm{K_{RSU_2-v}}$
$\mathrm{RSU_2}$ believes $\mathrm{RSU_2}$ received $\{\mathrm{N_7}\}\mathrm{K_{v-RSU_2}}$
P4: Vehicle believes $PK_\sigma(\mathrm{RSU_2}, r_{RSU_2}P)$
$\mathrm{RSU_2}$ believes $PK_\sigma$(vehicle, $r_{f_v^i}P$)
P5: Vehcle believes $\mathrm{SV}([ID_{RSU_2}, Exp_{RSU_2}, TS_3, N_7]SK_{RSU_2}, PK_{RSU_2}, (ID_{RSU_2}, Exp_{RSU_2}, TS_3, N_7))$
$\mathrm{RSU_2}$ believes $\mathrm{SV}([f_v^i, Exp_{f_v^i}, TS_4, N_8]SK_{f_v^i}, PK_{f_v^i}, (f_v^i, Exp_{f_v^i}, TS_4, N_8))$
P6: Vehicle believes $((\mathrm{RSU_2}$ says $(ID_{RSU_2}, Exp_{RSU_2}, TS_3, N_7) \supset PK_\delta(\mathrm{RSU_2}, r_{RSU_2}P))$
$\mathrm{RSU_2}$ believes ((vehicle says$(f_v^i, Exp_{f_v^i}, TS_4, N_8)) \supset PK_\delta(vehicle, r_{f_v^i}P))$
P7: Vehicle believes $\mathrm{PK}_\delta$(vehicle, $r_{f_v^i}P$)
$\mathrm{RSU_2}$ believes $\mathrm{PK}_\delta(\mathrm{RSU_2}, r_{RSU_2}P)$

P8: Vehicle believes (vehicle sees $PK_\delta$(vehicle, $r_{f_v^i}P$))
RSU$_2$ believes (RSU$_2$ sees $PK_\delta(RSU_2$, $\mathrm{r}_{\mathrm{RSU}_2}P$))
P9: ¬ (vehicle said $\{\mathrm{N}_8\}\mathrm{K}_{\mathrm{v-RSU}_2}$)
¬ (RSU$_2$ said $\{\mathrm{N}_7\}\mathrm{K}_{\mathrm{RSU}_2-\mathrm{v}}$)
P10: $\mathrm{OBU_i}$ believes fresh($\mathrm{N}_7$)
$\mathrm{OBU_j}$ believes fresh($\mathrm{N}_8$)

(3) Security proof

From P2, P4, P5, Ax4, we can get:

S1: Vehicle believes RSU$_2$ said ($ID_{RSU_2}$, $Exp_{RSU_2}$, $TS_3$, $N_7$)
RSU$_2$ believes vehicle said ($f_v^i$, $Exp_{f_v^i}$, $TS_4$, $N_8$)

From S1, P1, Ax19, we can get:

S2: Vehicle believes RSU$_2$ says ($ID_{RSU_2}$, $Exp_{RSU_2}$, $TS_3$, $N_7$)
RSU$_2$ believes vehicle says ($f_v^i$, $Exp_{f_v^i}$, $TS_4$, $N_8$)
(G$_1$ **is proved**)

From S2, P6, Ax1 and Necessitation, we can get:

S3: Vehicle believes $PK_\delta$(RSU$_2$, $r_{RSU_2}P$))
RSU$_2$ believes $PK_\delta$(vehicle, $r_{f_v^i}P$))

From S3, P7, Ax5, we can get:

S4: Vehicle believes sharedkey($K_{v-RSU_2}$, vehicle, RSU$_2$)
RSU$_2$ believes sharedkey($K_{RSU_2-v}$, RSU$_2$, vehicle)
where $K_{v-RSU_2} = F(r_{f_v^i}, r_{RSU_2}P)$,
$K_{RSU_2-v} = F(r_{RSU_2}, r_{f_v^i}P)$

From P2, Ax1, Ax8, we can get:

S5: Vehicle believes (vehicle sees $PK_\delta$(RSU$_2$, $r_{RSU_2}P$))
RSU$_2$ believes (RSU$_2$ sees $PK_\delta(vehicle, r_{f_v^i}P)$)

From S5, P8, Ax5, we can get:

S6: Vehicle believes vehicle sees sharedkey($K_{v-RSU_2}$, vehicle, RSU$_2$)
RSU$_2$ believes RSU$_2$ sees sharedkey($K_{RSU_2-v}$, RSU$_2$, vehicle)
where $K_{v-RSU_2} = F(r_{f_v^i}, r_{RSU_2}P)$,
$K_{RSU_2-v} = F(r_{RSU_2}, r_{f_v^i}P)$

From S4, S6, the definition of SharedKey(K-, A, B), we can get:

S7: Vehicle believes sharedkey($K_{v-RSU_2}-$, vehicle, RSU$_2$)
RSU$_2$ believes sharedkey($K_{RSU_2-v}-$, RSU$_2$, vehicle)
(G$_3$ **is proved**)

From P1, P2, S4, Ax16, Ax17, we can get:

S8: Vehicle believes fresh($K_{v-RSU_2}$)
RSU$_2$ believes fresh($K_{RSU_2-v}$)
(G$_5$ **is proved**)

From P2, P9, S8 and the definition of confirm$_p(X)$, we can get:

S9: $confirm_{vehicle}(K_{v-RSU_2})$
$confirm_{RSU_2}(K_{RSU_2-v})$

From S7, S9, and the definition of SharedKey(K+, A, B), we can get:

S10: Vehicle believes sharedkey($K_{v-RSU_2}+$, vehicle, RSU$_2$)
RSU$_2$ believes sharedkey($K_{RSU_2-v}+$, RSU$_2$, vehicle)
(G$_4$ **is proved**)

From P3, S4, Ax3, we can get:

S11: vehicle believes RSU$_2$ said $N_8$
RSU$_2$ believes vehicle said $N_7$

From S11, P10, and Ax19, we can get:

S12: vehicle believes RSU$_2$ says $N_8$
RSU$_2$ believes vehicle says $N_7$
(G$_2$ **is proved**)

### B. FURTHER SECURITY AND PRIVACY ANALYSIS

According to the security and privacy requirements of VANETs, we further analyze the security of the proposed scheme in the following aspects [30].

#### 1) SECURITY ANALYSIS

##### a: AUTHENTICATION

In VANETs, Authentication is the process of checking the authenticity and accuracy of certain claims, e.g., identity, privileges and authority. In the proposed scheme, all vehicles are required to perform mutual authentication protocol before getting network services from surrounding vehicles and RSUs. Depending on the group signature mechanism and identity based on signature, vehicles and RSUs can confirm the legitimacy of their identities. Besides, through Diffie-Hellman key exchange mechanism and challenge value,vehicles and RSUs can confirm that the information is transmitted correctly and a safe communication tunnel is built.

##### b: ACCOUNTABILITY

In some scenarios, when some vehicles commit illegal acts, e. g. broadcasting a forged warning message, there exists the serious risk of unnecessary traffic jams and accidents. In this situation, law enforcement agencies needs to have capacity to accurately identify the real identity of illegal vehicles and hold them accountable. In addition, accountability means non-repudiation, that is, sender cannot repudiate the message that has been sent. In the proposed scheme, each vehicle sends CC signature or group signature to prove the legitimacy of its identity. Receiver cannot know the true identity of sender, but once the vehicle has performed illegal acts, RTA and TA can resolve the real identity of the signer according to the content of the signature. Signer can not deny its signature, which meets accountability well.

##### c: RESTRICTED CREDENTIAL USAGE

Usage of a legal credential is required to to be limited by time and parallel use. In AAAS, as identity based signature is adopted, the identity of the vehicle is identified as a credential for authentication and accountability. In addition, since uncontrolled identity and signature of the vehicle may lead to abuse, and the attacker may use these credentials to launch a Sybil attack, AAAS adds expiration and timestamp into the signer's public key and signatures respectively to control service time of credential and prevents the signature used as credentials from being reused.

##### d: CREDENTIAL REVOCATION

As vehicles may be sold or broken, and theirs OBU could be compromised, it is crucial to exclude malfunctioning or misbehaving vehicles from the VANETs. Consequently, law enforcement agencies must be able to revoke their pseudonyms. AAAS implements vehicle credential revocation through cooperation mechanism between RTA and TA.

When a vehicle is considered illegal, its signatures, pseudonyms and expirations are required to be sent to RTA. When receiving these messages, RTA is able to find pseudonym of illegal vehicles issued by TA. TA can reveal the true identity of illegal vehicle and distribute credential revocation List (CRL) to achieve credential revocation.

#### 2) PRIVACY REQUIREMENT

##### a: MINIMUM DISCLOSURE

Minimal disclosure means that messages revealed by receivers should be kept to minimum in communication. In the mutual authentication of the proposed scheme, all messages sent need to be adaptive to authentication requirements and additional messages are not allowed to be added to authentication messages.

##### b: ANONYMITY AND UNLINKABILITY

It is the basis of protecting vehicle privacy to ensure vehicle communication anonymously. Based on the group signature mechanism, in AAAS, the verification of the vehicle's identity is realized by verifying the identity issued by TA and RTA. Verifier only needs to determine that the verified vehicle is approved by TA or RTA, and do not need to know the real identity of vehicle. Besides, as attackers cannot obtain the real identity of the vehicle through monitored messages, anonymous communication can also meet the privacy requirements of unlinkability in VANETs. In addition, multiple pseudonyms issued by TA and RTA also provide support for the vehicle to change pseudonyms regularly.

##### c: DISTRIBUTED RESOLUTION AUTHORITY

In order to protect the security of the vehicle's true identity, the capacity to resolve the identity of the vehicle should be distributed among multiple authorities, no authority can directly resolve the real identity of the vehicle by itself. In the proposed scheme, TA and RTA have to cooperate for the resolution of vehicle real identity. Specifically, RTA queries the pseudonym $a_v^i$ issued by TA for the vehicle through the public pseudonym $f_v^i$ of the vehicle, and TA is able to obtain the real identity of the vehicle through $a_v^i$.

##### d: PERFECT FORWARD PRIVACY

In VANETs, the resolution of a vehicle credentials should not decrease unlinkability of other credentials of the vehicle. In AAAS, all broadcasted pseudonyms and certificates only indicate the legitimacy of their identity. More concretely, a Vehicle anonymous credential does not contain information about other credentials of the vehicle. Consequently, attackers can not obtain any information about other credentials of the vehicle.

**TABLE 3. Symbol, description, and execution time.**

| Symbol | Description | Execution time(ms) |
|---|---|---|
| $\mathrm{T_{mtp}}$ | The execution time of hash-to-point | 21.94 |
| $\mathrm{T_{bp}}$ | The execution time of bilinear pairing | 6.05 |
| $\mathrm{T_{pm}}$ | The execution time of point multiplication | 9.79 |
| $\mathrm{T_{pe}}$ | The execution time of point exponentiation | 9.82 |

## V. PERFORMANCE ANALYSIS

In this section, AAAS is compared with CPAS [12], EDKM [16], LIAP [13], and GSSA [18] in anonymous authentication. We give the details from 3 aspects: communication overhead, computation cost, and signaling cost.

### A. COMPUTATIONAL COST

Computational cost is defined as the total amount of computation in authentication protocol. In order to analyze and compare the computational costs of above schemes, we need to consider operations that consume a lot of computing resources. As the processing time of bilinear pairing and point multiplication operation are thousands times of point addition operation or hash function, we ignore the cost of such low computation operations.

In order to obtain the execution times of cryptographic operations, a Type A pairing uses JAVA Pairing-based Cryptography (JPBC) library [35] is adopted. We have executed the benchmark on the hardware platform with Intel(R) Core(TM) i7-6700HQ CPU running at 2.6 GHz with 2GB of RAM. Debian 9.4 was the operating system. JPBC is a Java porting of the PBC Library written in C, which provides a full ecosystem of interfaces and classes to simplify the use of bilinear maps and supports both exponentiation and pairing preprocessing. The experiment uses bilinear map $e : G_1 \times G_1 \rightarrowtail G_T$, $G_1$ and $G_T$ represent additive group and multiplicative group with *order* $q$ respectively, which generated by $P$. The curve uses an equation $y^2 = x^3 + x \ mod \ p$ with an embedding degree $d = 2$, prime number $p = 512$ bits, and Solinas prime number $q = 160$ bits. The experiment results are shown in Table 3.

For anonymous authentication in CPAS, vehicle first chooses $r \in Z_q^*$ and computes $U = rP \in G_1$, $h' = H_2(PID, M, TS, T, U)$, and $V = h'S + rQ'$, where $PID$ is vehicle pseudonym ID, $M$ is a traffic-related message, $TS$ is current timestamp, $S$ is vehicle private key issued by private key generator (PKG), $T$ and $Q'$ are sysmtem parameter. Then vehicle signs $M$ and $TS$ to get: $\tau =< T, U, V >$. Finally $< PID, M, TS, \tau >$ are sent to RSU. When receiving the message from vehicle, RSU is required to compute $h = H_2(PID, T)$ and $h' = H_1(PID, M, TS, T, U)$. After that, RSU checks $e(V, P) == e(hP_{pub} + h'hT, Q)e(U, Q')$ to verify whether $\tau$ is legal. Consequently, computational cost of CPAS contains seven point multiplication operations, three bilinear map operations, and map-to-point hash function operation in $G_1$.

In EDKM, for signing message $M$, vehicle needs to compute $U = H_1(r||M)$, $V = H_1(rg||M)$, $T_1 = \alpha U$,

$T_2 = \alpha V + A$, and $\delta = \alpha x$, where $r$ and $\alpha$ are random numbers selected by the vehicle, $g$ is parameter generated by TA, $x$ and $A$ are vehicle group keys. Then vehicle chooses random numbers $r_\alpha$, $r_x$, $r_\delta \in Z_q^*$ and computes $R_1 = r_\alpha U$, $R_2 = e(T_2, P_1)^{r_x} e(V_i, P_2)^{-r_\alpha} e(V_i, P_1)^{-r_\delta}$, $R_3 = r_x T_1 - r_\delta U$, $c = H_2(M||r||T_1||T_2||R_1||R_2||R_3)$, $s_\alpha = r_\alpha + c\alpha$, $s_x = r_x + cx_i$, and $s_\delta = r_\delta + c\delta$. Here, message signature is $\sigma = (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$. When geting $M$ and $\sigma$, RSU computes $U = H_1(r||M)$, $V_j = H_1(rg||M)$, $\tilde{R_1} = s_\alpha U - cT_1$. $\tilde{R_2} = e(T_2, P_1)^{s_x}\ e(V_j, P_2)^{-s_\alpha}\ e(V_j, P_1)^{-s_\delta}$ $(\mathrm{e}(T_2, P_2)/e(PK^1_{RM_j}, PK^1_{RM_j}))^c$. $\tilde{R_3} = s_x T_1 - s_\delta U$. If $c == H_2(M||r_2||T_1||T_2||\tilde{R_1}\ ||\tilde{R_2}||\tilde{R_3})$ holds, then vehicle is thought as legal vehicle. Therefore, EDKM computational cost includes nineteen point multiplication operations, seven point exponentiation operations, eight bilinear map operations, and four map-to-point hash function operation in $G_1$.

In LIAP, vehicle first selects a random number $k_i \in Z_q^*$ to compute $PID_i^1 = k_i P$, $PID_i^2 = RID_i \oplus H(k_i PK_{CA})$, $PSK_i^1 = m_i^1 PID_i^1$, and $PSK_i^2 = m_i^2 H(PID_i^1, PID_i^2)$, where $RID_i$ is the real identity of vehicle, $PID_i = (PID_i^1, PID_i^2)$ is the anonymous identity of vehicle, and $PSK_i = (PSK_i^1, PSK_i^2)$ is the corresponding private key. Then the signature of message $M$ is $\sigma_i = PSK_i^1 + h(M)PSK_i^2$. Finally, vehicle sends $PID_i, M$, $PK_{RSU}$, and $\sigma_i$ to RSU. When the message is received, RSU checkverifies the equation $e(\sigma_1, P) == e(PID_i^1, RPK_i^1) \times e(h(M)H(PID_i^1||PID_i^2), RPK_i^2)$, if the equation holds, RSU accepts the signature and vehicle is considered as a legal vehicle. Otherwise, RSU accepts it. Therefore, LIAP communicational cost comprises of six point multiplication operations, three bilinear map operations, and three map-to-point hash function operation in $G_1$.

In GSSA, vehicle first chooses a variable $t \in Z_q^*$, and computes $\sigma_1 = C_1 g_1^t$, $\sigma_2 = C_2(h_1 \cdot Y)^{-t}$, $\sigma_3 = (\sigma_1)^y$, $\sigma_4 = H_2(M)^y$, and $\sigma_5 = H_1(M||\sigma_1||\sigma_2||\sigma_3||\sigma_4||H_1(GSM_j||TS))$, where $C_1$ and $C_2$ are parameters issued by group manager RSU, $g_1$ is generators of $G_1$, $h_1 \in G_1$, $Y$ is the public key of vehicle, and $M$ is a plaintext containing information such as message sequence number, position, speed etc. Then vehicle sends its signature $\sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ and $M$ to RSU. When receiving $\sigma$ and $M$, RSU checks whether $\sigma_4$ and $\sigma_5$ is legal. Then, RSU uses the system parameters $g_2$, $h_2$, $U_2$ and the group public key $A$ to check $e(\sigma_2, g_2)e(\sigma_1, h_2)e(\sigma_3, U_2) = A$, if the equality holds, vehicle is considered as a legal. Consequently, the computational cost of GSSA consists of five point multiplication operations, three bilinear map operations, four point exponentiation operations, and two map-to-point hash function operation in $G_1$.

In AAAS, vehicle is required to sign msssage $< f_v^i, Exp_{f_v^i}, TS_4, N_8 >$ for authentication. vehicle computes its signature $\sigma = \{V_v', W_v'\}$, where $V_v' = r_v p$, $W_v' = r_v^{-1} sk_i + H_2(f_v^i||Exp_{f_v^i}||TS_4||N_8, V_v')b_i$, and $r_v \in Z_q^*$ is a random number selected by vehicle. Then vehicle sends $f_v^i$, $Exp_{f_v^i}$, $TS_4$, $N_8$, and $\sigma$ to RSU. When receiving the message from vehicle, RSU checks $e(f_v^i P_{pub}, f_v^i)e(V_v', H_2((f_v^i||Exp_{f_v^i}||TS_4||N_8, V_v')) == e(V_v', f_v^i W_v')$ to verify whether sign is legal. AAAS communicational cost includes six point multiplication operations three bilinear map operations, and two map-to-point hash function operation in $G_1$.

**TABLE 4. Comparison of computational costs of schemes.**

| Scheme | Computational cost | Execution time(ms) |
|---|---|---|
| CPAS [12] | $7T_{pm} + 3T_{bp} + T_{mtp}$ | 108.62 |
| EDKM [16] | $19T_{pm} + 7T_{pe} + 8T_{bp} + 4T_{mtp}$ | 390.91 |
| LIAP [13] | $6T_{pm} + 3T_{bp} + 3T_{mtp}$ | 142.71 |
| GSSA [18] | $3T_{bp} + 5T_{pm} + 2T_{pe} + 2T_{mtp}$ | 130.62 |
| AAAS | $6T_{pm} + 3T_{bp} + 2T_{mtp}$ | 120.77 |

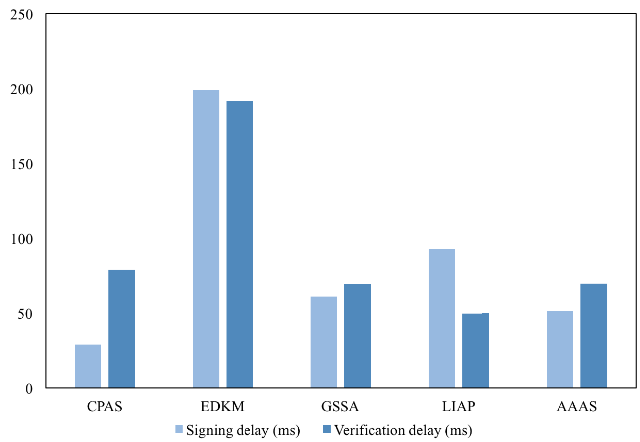



**FIGURE 9. Comparison of computational costs.**

The comparison of computational costs is presented in Table 4 and Figure 9.

From Table 4 and Figure 9, we can observe that CPAS has a lower computational cost compared with AAAS. However, CAPS does not consider how to establish a session key, which is vital to guarantee secure communication between vehicle and RSU. Besides, since the signature of vehicle does not contain challenge value, it is difficult for the vehicle to determine whether RSU receives the message sent by the vehicle.

### B. COMMUNICATION COST

Communication cost refers to the total size of message transmitted. According to [32], [33], for type A pairing with respect to 80 bit security level, the size of $p$ is equal to 64 bytes, A point on the group of points $E(F_q)$ consists of $x$ and $y$ coordinates. This means that the size of each element in $G_1$ is $64 * 2 = 128$ bytes whilst that of each element in $G_2$ is $20 * 2 = 40$ bytes. In addition, the size for a general hash function in $Z_q^*$, a expiration, and a timestamp are considered to be 20 bytes, 4 bytes, and 4 bytes, respectively. As the basic configuration information is the same for above schemes, we ignore the size of message and only take into account the size of the signature on the message with the corresponding pseudo-identity.

In CPAS, vehicle broadcast $\tau =< T, U, V >$ with timestamp $TS$, pseudonym $PID$ to RSU, where $T, U, V \in$

**TABLE 5. Comparison of communication cost of schemes.**

| Scheme | message-signature | communication cost (byte) |
|---|---|---|
| CPAS [12] | $3\|G_1\| + \|TS\| + \|PID\|$ | 392 |
| EDKM [16] | $5\|G_1\| + 2\|Z_q^*\|$ | 680 |
| LIAP [13] | $4\|G_1\| + \|TS\|$ | 516 |
| GSSA [18] | $4\|G_1\| + \|Z_q^*\| + \|TS\|$ | 536 |
| AAAS | $2\|G_1\|+\|Z_q^*\|+\|TS\|+\|EXP\|$ | 304 |

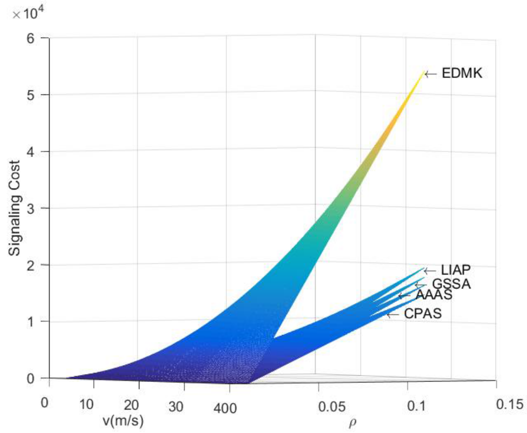



**FIGURE 10. Signaling cost.**

$G_1$. This results in communication cost of CPAS is $128 * 3 + 4 + 4 = 392$ bytes. Vehicle in EDKM sends signature $\sigma = (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$ for authentication, where $r, c \in Z_q^*$, $T_1$, $T_2$, $s_\alpha$, $s_x$, $s_\delta \in G_1$. Thus, the communication cost of EDGK is: $128 * 5 + 20 * 2 = 680$ bytes. In LIAP, vehicle is request to sends its pseudo-identity $PID_i = (PID_i^1, PID_i^2) \in G_1$, the public key $PK_{RSU} \in G_1$, timestamp $TS$, and its signture $\sigma \in G_1$ to the RSU. Thus, the total communication cost of LIAP is $128 * 4 + 4 = 516$ bytes. In GSSA, vehicle is required to send message $\sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ and $M$ to RSU, where $\sigma_1 = C_1 g_1^t$, $\sigma_2 = C_2(h_1 \cdot Y)^{-t}$, $\sigma_3(\sigma_1)^y$, $\sigma_4 = H_2(M)^y \in G_1$, and $\sigma_5 = H_1(M||\sigma_1||\sigma_2||\sigma_3||\sigma_4||H_1(GSM_j||TS)) \in Z_q^*$. Therefore, the total communication cost of GSSA in authentication is $128 * 4 + 20 + 4 = 536$ bytes. In AAAS, vehicle needs to sends signature $\sigma = \{V_v', W_v'\}$, $V_v', W_v' \in G_1$, $N_8 \in Z_q^*$ with pseudo-identity $f_v^i$, expriation $Exp_{f_v^i}$, timestamp $TS_4$, and challenge value $N_8$ to RSU. Thus, the total communication cost of AAAS is $20+4+4+20+128 \times 2 = 304$ bytes. The result in communication cost of scheme is shown in table 5.

### C. SIGNALING COST

In this section, we adopt fluid-flow model to evaluate signaling cost in authentication. We assume that subnets in VANETs are circular and of same size. Crossing rate(R) and signaling cost (SC) are defined as:

$$R = \frac{\rho v L}{\pi} \tag{1}$$

$$SC = HL \times R \tag{2}$$

where $\rho$, $v$, $L$ refer to vehicle density, vehicle average velocity, and permeters of a subnet. $HL$ means authentication delay, which includes communication overhead and transmission delay. Acording to [34], We sets $L = 100\ m$, $\rho = 0.1 \sim 0.01(1/m^2)$, $v = 0 \sim 40(m/s)$, the wireless bandwidth is 6 Mbps. The result is shown in Figure 10.

Vehicle density and velocity have a great influence on the signaling overhead. The signaling overhead increases rapidly as the vehicle density and velocityincreases. According to Figure 10, we can see that AAAS owns lower signaling cost than EDKM, LIAP, and GSSA due to low computational cost and communication cost. AAAS and CPAS have similar signaling cost, but AAAS has higher performance due to lower communication cost. Besides, the computational overhead of the session key in CPAS is also not negligible.

## VI. CONCLUSION

This paper proposes an anonymous authentication scheme based on group signature in VANETs. Region trust authority as group manager is added to support vehicles to perform anonymous authentication as the group members. Pseudonym mechanism and identity based on signature mechanism are adopted, which reduces the costs caused by the storage and verification of pseudonym certificates. Moreover, security and performance analysis demonstrate that the proposed scheme is robust and efficient.

In the future, we will propose a V2V authentication scheme based on AAAS, and simulate the proposed scheme to obtain more accurate performance results.

## REFERENCES

[1] C. N. E. Anagnostopoulos, I. E. Anagnostopoulos, V. Loumos, and E. Kayafas, "A license plate-recognition algorithm for intelligent transportation system applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 3, pp. 377–392, Sep. 2006.

[2] D. Rossi, R. Fracchia, and M. Meo, "VANETs: Why use beaconing at all?" in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 2745–2751.

[3] J. Feng, N. Liu, J. Cao, Y. Zhang, and G. Lu, "Securing traffic-related messages exchange against inside-and-outside collusive attack in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9979–9992, Dec. 2019.

[4] T. Gao, X. Deng, Q. Li, M. Collotta, and I. You, "APPAS: A privacy-preserving authentication scheme based on pseudonym ring in VSNs," *IEEE Access*, vol. 7, pp. 69936–69946, 2019.

[5] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.

[6] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proc. 1st ACM Int. Workshop Qual. Service Secur. Wireless Mobile Netw. (Q2SWinet)*, Oct. 2005, pp. 79–87.

[7] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 71–83, Jan. 2016.

[8] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 943–955, Jan. 2018.

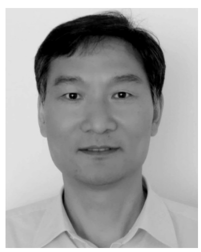
[9] *IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*, IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), Mar. 2016, pp. 1–240.

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

[11] T. Gao, Y. Li, N. Guo, and I. You, "An anonymous access authentication scheme for vehicular ad hoc networks under edge computing," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 2, pp. 1–16, Feb. 2018.
[12] K.-A. Shim, "$\mathcal{CPAS}$: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.
[13] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.
[14] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.
[15] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[16] Y. Sun, Z. Feng, Q. Hu, and J. Su, "An efficient distributed key management scheme for group-signature based anonymous authentication in VANET," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 79–86, Jan. 2012.
[17] B. K. Chaurasia and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," in *Transactions on Computational Science XIII* (Lecture Notes in Computer Science), vol. 6750. Berlin, Germany: Springer, 2011, pp. 147–156.
[18] C. Zhang, X. Xue, L. Feng, X. Zeng, and J. Ma, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access*, vol. 7, pp. 178310–178320, 2019.
[19] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.
[20] *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*, IEEE Standard 1609.0-2019 (Revision of IEEE Std 1609.0-2013)-Redline, Apr. 2019, pp. 1–219.
[21] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology*, vol. 32, no. 3. Philadelphia, PA, USA, Aug. 2001, pp. 213–229.
[22] J. Y. Hwang, L. Chen, H. S. Cho, and D. Nyang, "Short dynamic group signature scheme supporting controllable linkability," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1109–1124, Jun. 2015.
[23] 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.
[24] S. Parvin, S. Han, Z. U. Rehman, A. Al Faruque, and F. K. Hussain, "A new identity-based group signature scheme based on knapsack ECC," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Palermo, Italy, Jul. 2012, pp. 73–80.
[25] S. Park, S. Kim, and D. Won, "ID-based group signature," *Electron. Lett.*, vol. 33, no. 19, pp. 1616–1617, Sep. 1997.
[26] S. Han, J. Wang, and W. Liu, "An efficient identity-based group signature scheme over elliptic curves," in *Universal Multiservice Networks* (Lecture Notes in Computer Science), vol. 3262. Berlin, Germany: Springer, 2004.
[27] J. C. Choon and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 2567. Berlin, Germany: Springer, 2003.
[28] P. Bhattacharya, M. Debbabi, and H. Otrok, "Improving the Diffie-Hellman secure key exchange," in *Proc. Int. Conf. Wireless Netw., Commun. Mobile Comput.*, Maui, HI, USA, Jun. 2005, pp. 193–197.
[29] Federal Information Processing Standards Publication (FIPS) 197. (Nov. 26, 2001). *Specification for the Advanced Encryption Standard (AES)*. [Online]. Available: http://www.nist.gov/aes
[30] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.
[31] P. F. Syverson and P. C. van Oorschot, "On unifying some cryptographic protocol logics," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, Washington, DC, USA, Mar. 1994, pp. 14–28.
[32] X. Boyen and L. Martin, *Identity-Based Cryptography Standard (IBCS) ♯1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*, document RFC 5091, 2007.
[33] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, document RFC 3161, 2001.
[34] J.-H. Lee and J.-M. Bonnin, "HOTA: Handover optimized ticket-based authentication in network-based mobility management," *Inf. Sci.*, vol. 230, pp. 64–77, May 2013.
[35] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Kerkyra, Greece, Jun. 2011, pp. 850–855.

**YANJI JIANG** received the B.S. and M.Sc. degrees in physics from Jilin University, Changchun, China, in 2007 and 2010, respectively. He is currently pursuing the Ph.D. degree with Liaoning Technology University. In 2010, he joined the Software College, Liaoning Technology University, as an Associate Research Fellow. His primary research interests include network security and machine learning.

**SHAOCHENG GE** received the B.E. and M.E. degrees from the College of Safety Science and Engineering, Liaoning Technology University, in 1996 and 2002, respectively, and the Ph.D. degree in mechanical power and engineering from Dalian Technology University, in 2006. He joined Liaoning Technology University. He is currently the Vice President of the College of Safety and Emergency Management Engineering, Taiyuan University of Technology. He is also a Professor and a Ph.D. Supervisor. His primary research interests include network security and emergency management.



**XUELI SHEN** received the B.E. and M.E. degrees from the College of Electronic Information and Engineering, Liaoning Technology University, in 1992 and 2008, respectively. He joined Liaoning Technology University. He is currently the Dean of College of Software, a Professor, and the master's Supervisor. His primary research interests include computer networks and deep learning.