IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 15, 2019, accepted February 2, 2019, date of publication March 19, 2019, date of current version June 10, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2900593

APPAS: A Privacy-Preserving Authentication Scheme Based on Pseudonym Ring in VSNs

TIANHAN GAO[1], XINYANG DENG[1], QINGSHAN LI[2], MARIO COLLOTTA[3], AND ILSUN YOU[4], (Senior Member, IEEE)
[1]Software College, Northeastern University, Shenyang 110169, China
[2]Information Security Laboratory, Peking University, Beijing 100871, China
[3]Faculty of Engineering and Architecture, Kore University of Enna, 94100 Enna, Italy
[4]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea

Corresponding author: Ilsun You (isyou@sch.ac.kr)

This work was supported in part by the National Natural Science Foundation of China under Grant 61402095, and in part by the Soonchunhyang University Research Fund.

ABSTRACT Vehicular social networks (VSNs) provide a variety of services for users based on social relationships through vehicular ad hoc networks (VANETs). During the communication in VSNs, vehicles are at risk of exposure to privacy information. Consequently, how to guarantee the security and privacy of vehicles is a critical issue. Ring signature is an effective mechanism to achieve anonymous authentication and communication. However, how to establish rings and how to select ring members become open problems. In this paper, a privacy-preserving scheme based on the pseudonym ring in VSNs is proposed. Hierarchical network architecture and trust model are established. A series of authentication protocols are then elaborated. According to the security and performance analysis, the proposed scheme is more robust and efficient compared with the typical ones.

INDEX TERMS Privacy-preserving authentication, pseudonym, ring signature, VSNs.

I. INTRODUCTION

VANETs, a special kind of ad-hoc networks, guarantee drivers or passengers on the roads to obtain continuous and stable wireless network services, like traffic congestion prediction, safe driving, as well as onboard entertainment [1], [2]. VSNs are considered as the combination of VANETs and social networks. Based on the social relationship, users are able to get or share interesting and useful information during driving through VSNs [3], [5]. Since all messages are sent in the form of broadcast, the adversary around a vehicle can eavesdrop the messages, which makes the communication in VSNs more vulnerable. Consequently, how to ensure the security of communication in VSNs becomes particular important. Authentication is the fundamental approach to guarantee the reliability of the entities in VSNs [6]. However, the vehicle in VSNs needs to regularly send beacon messages, that includes its current location, speed, and direction etc. [7]–[10], which may result in privacy disclosure. Thus, the anonymous authentication scheme comes to be the urgent need for the security of VSNs.

Currently, pseudonym certificate [12], [13], [29] and group signature [14]–[18] are thought as two main approaches to achieve anonymous authentication in VSNs. For the pseudonym certificate schemes, a large number of pseudonyms and certificates need to be issued by the trust authority. When participating in authentication, vehicle needs to randomly select the pseudonym and the corresponding certificate as legal identity. Nevertheless, according to [19] and [20], each vehicle has to hold a large number of pseudonyms and certificates to fully meet the privacy requirements, which pushes great pressure on vehicles with insufficient computing and storage resources. In addition, once the vehicle is revoked, all pseudonyms and certificates should be added to the Certificate Revocation List (CRL), which is also a huge challenge for CRL's management. As a special signature mechanism, group signature is widely adopted for anonymous authentication in VSNs due to the features of nonlinkability, anonymity, and traceability. During authentication, group signature is able to prove the reliability of vehicles without exposing their identities. Meanwhile, the existence

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

of the group manager ensures vehicle's traceability. Once the vehicle is found to be illegal, the group manager can revoke the signature and reveal the true identity of the vehicle. However, in certain scenarios, the vehicle needs to show its identity information to obtain some specific services, where group signature is hard to reach the goal.

Ring signature, as another group-oriented signature mechanism that contains the information of a group of users rather than the group manager, is applied for the authentication in VSNs [21]. Consequently, higher privacy protection is supplied. In [22] and [23], each vehicle is allowed to generate the signature without the help of RSU or other vehicle, which provides a non-repudiation proof of the signature generated by the vehicle. However, how to generate a ring and disclose the illegal vehicles are not discussed. Identity-based ring signature [27] is deemed to be a special ring signature, where the public key of ring members is able to be efficiently generated. Reference [21] adopts such a signature mechanism to achieve vehicle's anonymity. In order to sign message, the vehicle collects the identity of the surrounding vehicles: VID and generates proof of the message by using ID-based ring signature mechanism. The verifier can verify that the signature belongs to one of the ring members, while does not know which one is. However, the non-traceability and unconditional anonymity make it difficult to revoke illegal node or provide identity-based services. Therefore, the further improvement has to be made to solve the problems.

In this paper, we propose a privacy-preserving authentication scheme based on pseudonym ring in VSNs (APPAS). We combine pseudonyms with ring signatures to make the following contributions: (1) Pseudonym is adopted as the identity of vehicle to meet the requirement of identity-based service. (2) Ring signature is applied to ensure the non-linkability and anonymity of vehicles during authentication. (3) Pseudonym ring is designed to effectively reduce the pressure and cost of the pseudonym generation, maintenance, and revocation. (4) Roadside unit (RSU) is in charge of maintaining the ring members, which achieves the goal of traceability of illegal vehicles.

The rest of this paper is organized as follows. In Section II, we introduce the necessary preliminaries. The proposed scheme is elaborated in section III. The security and performance analysis of the proposed scheme are given in section IV and section V respectively. Finally, we draw our conclusion in section VI.

II. PRELIMINARIES

A. VEHICULAR SOCIAL NETWORKS (VSNs)

As shown in Figure 1, VSNs [3] are special VANETs that provide a variety of services to users based on social relationships. As the important part of ITS [4], [24], VSNs can provide relevant vehicular applications and services according to the interests and demands of vehicle users. In general, with the help of RSU, the vehicle is able to join surrounding social network and gain the useful information [11]. However, security and privacy are necessary for the communication between vehicle and RSU. Consequently, establishing the trust relationship and preserving the privacy of the communication in VSNs become crucial.

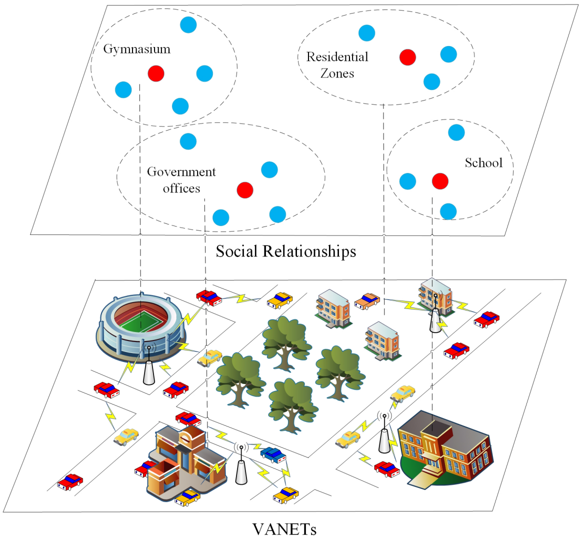

FIGURE 1. **Vehicle social networks.**

B. BILINEAR PAIRING

Let G_1 be additive cycle group, the prime order is p, and G_T be multiplicative group of the same order. A bilinear pairing e: $\mathrm{G}_1 \times \mathrm{G}_1 \rightarrow \mathrm{G}_\mathrm{T}$ satisfies the following properties [25].

1) Bilinear: For any $P, Q \in \mathrm{G}_1$, $a, b \in \mathrm{Z}_\mathrm{q}^*$, there are $e(aP, bQ) = e(P, Q)^{ab}$.
2) Non-degeneracy: Existing a certain $P, Q \in \mathrm{G}_1$ satisfies $e(P, Q) = 1$.
3) Computability: An efficient algorithm can calculate $e(P, Q) \in \mathrm{G}_\mathrm{T}$, where $P, Q \in \mathrm{G}_1$.

C. MATHEMATICAL HARD PROBLEMS

In this paper, the following mathematical hard problems are used to ensure the security of the proposed scheme.

Decision Diffie-Hellman Problem (DDHP): Given P, aP, bP, $cP \in \mathrm{G}_1$, where $a, b, c \in \mathrm{Z}_\mathrm{q}^*$, judging whether $c = ab \bmod P$ is difficult.

Computation Diffie-Hellman Problem (CDHP): Given P, aP, $bP \in \mathrm{G}_1$, where $a, b \in \mathrm{Z}_\mathrm{q}^*$, it is difficult to calculate abP.

D. IDENTITY-BASED RING SIGNATURE

Ring signature is first proposed by Rivest *et al.* [26]. In ring signature, a set of possible signers are specified, while the verifier can not reveal which member actually generate the signature. Besides, there is no group manager in ring signature, thus each group member is indistinguishable. Generally, a standard ring signature holds the features of unconditional anonymity, unforgeability, correctness etc..

The earliest identity-based ring signature mechanism was proposed by Zhang and Kim [27]. In identity-based ring signature, the verifier only needs to know the identity

TABLE 1. Symbol and description.

Symbol	Description
$\mathrm{ID_A}$	The identity of entity A
$\mathrm{PK_A/SK_A}$	The public key/privacy key of entity A
$\mathrm{K_{A-B}}$	The shared key between entity A and entity B
$\mathrm{C_{A-B}}$	The ciphertext generated by entity A to entity B
$\mathrm{Sign_A}$	A's signature
$\mathrm{PS_A}$	A's pseudonym
TS	The current timestamp
N	random number
EXP	Expiration of ring signature
$\mathrm{H_i}$	Hash function
$\|\|$	Connection operations between messages
$\mathrm{Z_q^*}$	The ring of integers
$\mathrm{Enc\_PK_A}\{M\}$	Using $\mathrm{PK_A}$ to encrypt message M
$\mathrm{Sign\_SK_A}\{M\}$	Using the $\mathrm{SK_A}$ to sign message M
$\mathrm{Sign\_ring\_SK_A}\{M\}$	Using $\mathrm{SK_A}$ to sign message M through ring signature mechanism
$\mathrm{Enc\_}K\{M\}$	Using symmetric key K to encrypt message M
$\mathrm{Sign\_cry\_\_SK_A\_PK_B}\{M\}$	Using $\mathrm{SK_A}$ and $\mathrm{PK_B}$ to signcrypt message M
$\mathrm{Cert_A}$	A's certification

information of all ring members to compute the public keys, which alleviates the management burden of the public key certificate. In addition, the verifier can not determine which one is the actual signer in a ring. Consequently, the signer's identity is well protected. However, the signers and verifiers should perform a large amount of computation, that limits the efficiency of the mechanism. Our proposed scheme borrows the idea from the ring signature scheme introduced by Chow *et al.* [28], which makes a balance between the security and efficiency. The details of the scheme are as follows.

1) Setup. PKG generates public parameter param $= \{G_1, G_2, e, P, q, \mathrm{H}, \mathrm{H_0}\}$, where $\mathrm{H}:\{0,1\}^* \rightarrow G_1$, $\mathrm{H_0}:\{0,1\}^* \rightarrow \mathrm{Z_q^*}$. PKG chooses $x \in \mathrm{Z_q^*}$ as the master key, and the public key is $\mathrm{P_{pub}} = xP$.
2) Extract. After receiving the signer's identity ID through the secure tunnel, PKG computes the signer's public key $\mathrm{Q_{ID}} = \mathrm{H}(ID)$ and private key $\mathrm{S_{ID}} = x\mathrm{Q_{ID}}$.
3) Ring-sign. If a signer wants to sign message M, the following operations will be executed.
    a) Choose $\mathrm{U_i} \in G_1$ and compute $\mathrm{h_i} = \mathrm{H_0}(M\|\|L\|\|\mathrm{U_i})$, where $L = (\mathrm{ID_1}, \mathrm{ID_2}, \ldots \mathrm{ID_n})$.
    b) Select $\mathrm{r_s'} \in \mathrm{Z_q^*}$ and get $\mathrm{U_s} = \mathrm{r_s'}\mathrm{Q_{ID}} - \sum_{\mathrm{i}\neq \mathrm{s}}\{\mathrm{U_i} + \mathrm{h_i}\mathrm{Q_{ID}}\}$.
    c) Compute $\mathrm{h_s} = \mathrm{H_0}(M\|\|L\|\|\mathrm{U_s})$, $V = (\mathrm{h_s} + \mathrm{r_s'})\mathrm{S_{ID}}$.
    d) The signature on message M is: $\sigma = \{\cup_{\mathrm{i}=1}^{\mathrm{n}}\{\mathrm{U_i}\}, V\}$.
4) Ring-verify. After receiving M and σ, the verifier performs the following operations to verify the signature.
    a) $\mathrm{h_s} = \mathrm{H_0}(M\|\|L\|\|\mathrm{U_s})$ is computed.
    b) Check $\mathrm{e}(\mathrm{P_{pub}}, \sum_{\mathrm{i}=1}^{\mathrm{n}}(\mathrm{U_i} + \mathrm{h_i}\mathrm{Q_{ID}})) == e(P, V)$ to verify whether σ is legal.

III. THE PROPOSED SCHEME

Before introducing the proposed scheme, the relevant symbols and descriptions are shown in Table 1.

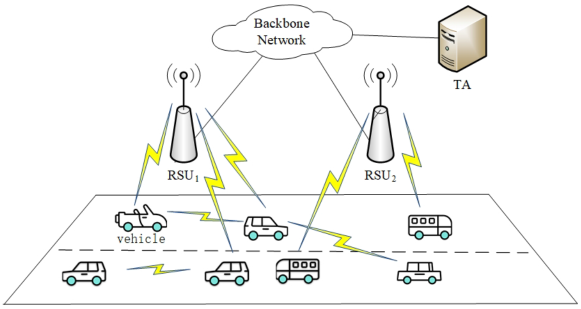

FIGURE 2. Network architecture.

A. NETWORK ARCHITECTURE

As shown in Figure 2, the whole network architecture consists of three parts. The first part is the trust authority (TA) that is responsible for generating and publishing public parameters, issuing corresponding legitimate private keys for RSUs and vehicles. Besides, TA also plays an important role in building pseudonym ring. The second part is a number of roadside units (RSUs). In the proposed scheme, RSU helps the legal vehicles to achieve anonymous communication. The last part is vehicles. Once identified as a legal node, vehicle is able to obtain corresponding network services from RSU in an anonymous way.

B. TRUST MODEL

The trust model of the proposed scheme is depicted as Figure 3. TA, as a third party authority, is trusted by all the other entities in VSNs. Through submitting legal registration credentials, other entities and TA can build the trust relationship. Vehicles and RSUs do not trust any entities except TA. The aim of proposed scheme is to build the trust relationship among vehicles and RSUs anonymously.

C. SYSTEM INITIALIZATION

During system initialization, TA generates and publishes public parameters. The details are depicted as follows.

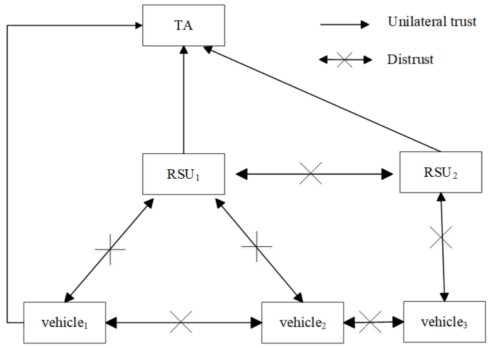

FIGURE 3. Trust model.

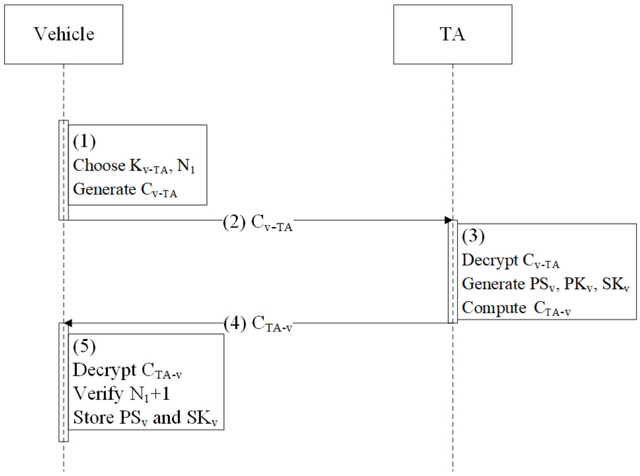

FIGURE 4. Vehicle registration protocol.

1) TA chooses an additive group G_1 and a multiplicative group G_T of prime order q, where the generator of G_1 is P.
2) TA selects a bilinear pairing e: $G_1 \times G_1 \rightarrow G_T$, hash functions H_1:$\{0, 1\}^* \rightarrow G_1$, H_2: $\{0, 1\}^* \rightarrow Z_q^*$, and H_3: $\{0, 1\}^* \times G_1 \rightarrow Z_q^*$.
3) TA chooses $SK_{TA} \in Z_q^*$ as the private key and the public key is $PK_{TA} = SK_{TA}P$. TA selects $K \in \{0, 1\}^*$ as a secret key.

TA publishes the param= $\{G_1, G_T, e, q, P, PK_{TA}, H_1, H_2, H_3\}$.

D. INITIAL REGISTRATION

In this section, vehicle and RSU send the identity information to TA for registration to obtain private key or pseudonym.

1) VEHICLE REGISTRATION PROTOCOL

As shown in figure 4, vehicle generates and sends the registration message to TA for acquiring the private key. The details are shown as following.

1) Vehicle generates the session key $K_{v-TA} \in \{0, 1\}^*$ and the random number $N_1 \in Z_q^*$. The message $<ID_v, K_{v-TA}, N_1>$ is then encrypted to get $C_{v-TA} = Enc\_PK_{TA}\{ID_v, K_{v-TA}, N_1\}$.
2) Vehicle sends C_{v-TA} to TA.

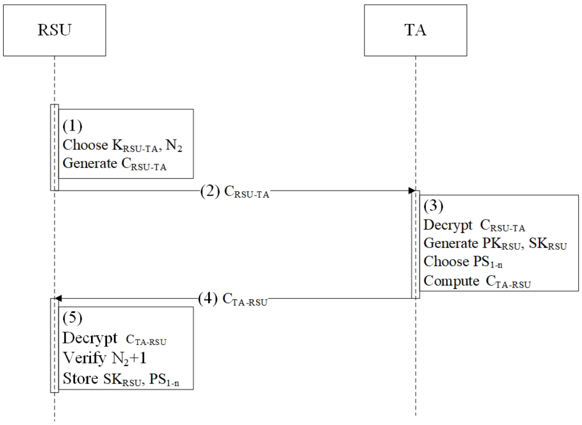

FIGURE 5. RSU registration protocol.

3) After receiving the ciphertext from vehicle, TA decrypts C_{v-TA} and gets $<ID_v, K_{v-TA}, N_1>$. Then TA utilizes K to encrypt ID_v and gets pseudonym $PS_v = Enc\_K\{ID_v\}$. TA computes $PK_v = H_1(PS_v)$, $SK_v = SK_{TA}PK_v$. Finally, TA encrypts $<PS_V, SK_V, N_1 + 1>$ to get $C_{TA-v} = Enc\_K_{v-TA}\{PS_v, SK_v, N_1 + 1\}$.
4) TA sends C_{TA-v} to vehicle.
5) Once receiving C_{TA-v}, vehicle decrypts C_{TA-v} and obtains $<PS_v, SK_v, N_1 + 1>$. Vehicle verifies $N_1 + 1$. If the verification is successful, vehicle stores PS_v and the corresponding private key SK_v. Otherwise, vehicle's registration is failed.

2) RSU REGISTRATION PROTOCOL

As shown in Figure 5, RSU is able to obtain the private key through RSU registration protocol.

1) RSU chooses the session key $K_{RSU-TA} \in \{0, 1\}^*$ and $N_2 \in Z_q^*$. RSU then encrypts the message $<ID_{RSU}, K_{RSU-TA}, N_2>$ to get ciphertext $C_{RSU-TA} = Enc\_K_{RSU-TA}\{ID_{RSU}, K_{RSU-TA}, N_2\}$.
2) RSU sends C_{RSU-TA} to TA.
3) After receiving the ciphertext from RSU, TA uses its privacy key to decrypt C_{RSU-TA} to get $<ID_{RSU}, K_{RSU-TA}, N_2>$. Then TA computes the public key $PK_{RSU} = H_1(ID_{RSU})$ and private key $SK_{RSU} = SK_{TA}PK_{RSU}$. TA selects n pseudonyms for the registered vehicles: $PS_{1-n} = \{PS_1, PS_2 \ldots PS_n\}$. Finally, $<SK_{RSU}, N_2 + 1, PS_{1-n}>$ are encrypted to get $C_{TA-RSU} = Enc\_K_{RSU-TA}\{SK_{RSU}, N_2 + 1, PS_{1-n}\}$.
4) TA sends C_{TA-RSU} to RSU.
5) When getting C_{TA-RSU}, RSU decrypts C_{TA-RSU} to obtain $<SK_{RSU}, N_2 + 1, PS_{1-n}>$. Then RSU verifies $N_2 + 1$. If the verification is successful, RSU stores SK_{RSU}, PS_{1-n}. Otherwise, the registration is failed.
6) As shown in Figure 6, after successful verifying the messages from TA, RSU generates a pseudonym ring with a storage space of n, and puts the pseudonyms PS_{1-n} into the pseudonym ring in turn. Meanwhile, TA selects index $\in \{0, 1 \ldots n - 1\}$ randomly as a pointer.

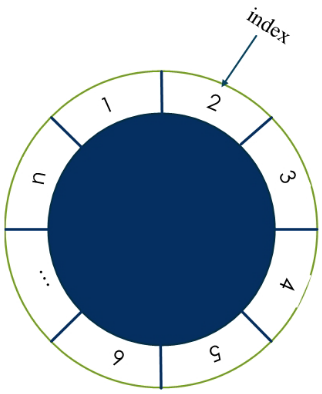

FIGURE 6. Pseudonym ring.

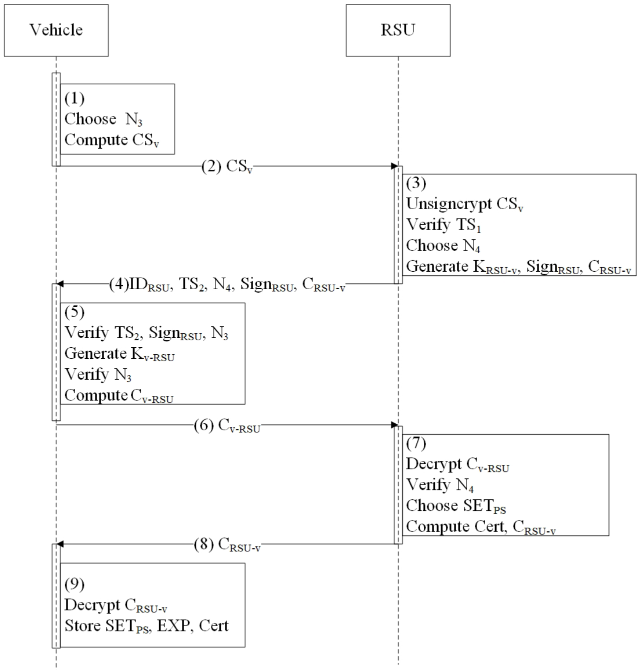

FIGURE 7. Initial authentication protocol.

E. INITIAL AUTHENTICATION PROTOCOL

The initial authentication protocol launches when the vehicle enters the coverage range of RSU for the first time. In the process, the vehicle and RSU use the signcryption mechanism proposed by Chen and Malonelee [32] and the signature mechanism designed by Choon and Cheon [33] respectively to achieve mutual authentication. Besides, the ciphertext and signature include key-agreement parameter, which can help communicating parties to build session key. Once the trust relationship between vehicle and RSU is established, vehicle will get the pseudonym ring. The details of initial authentication protocol are shown as Figure 7.

1) Vehicle chooses random number $N_3 \in Z_q^*$ and uses SK_v to signcrypt <PS_v, N_3, TS_1>: $CS_v = Sign\_Cry\_SK_v\_PK_{RSU}\{PS_v, N_3, TS_1\}$, where CS_v includes key-agreement parameter r_vPK_v, $r_v \in Z_q^*$.
2) Vehicle sends CS_v to RSU.
3) When receiving the ciphertext from vehicle, RSU decrypts and verifies CS_v to get <PS_v, N_3, TS_1>. Then RSU checks the freshness of TS_1. If TS_1 is not fresh, the authentication is failed. Otherwise RSU chooses random number $N_4 \in Z_q^*$ and generates the session key $K_{RSU-v} = r_{RSU}r_vPK_v$, where $r_{RSU} \in Z_q^*$. RSU then signs <ID_{RSU}, TS_2, N_3, N_4> to get $Sign_{RSU} = Sign\_SK_{RSU}\{ID_{RSU}, TS_2, N_4\}$. Meanwhile, RSU encrypts N_3 to get ciphertext $C_{RSU-v} = Enc\_K_{RSU-v}\{N_3\}$, where $Sign_{RSU}$ includes the key-agreement parameter $r_{RSU}PK_{RSU}$.
4) RSU sends <$ID_{RSU}, TS_2, N_4, Sign_{RSU}, C_{RSU-v}$>, to vehicle.
5) When receiving the message from RSU, vehicle checks the freshness of TS_2. If TS_2 is not fresh, the authentication is failed. Otherwise, vehicle continues to verify $Sign_{RSU}$. If the verification is successful, vehicle generates the shared key with RSU $K_{v-RSU} = r_vr_{RSU}PK_{RSU}$ and decrypts C_{RSU-v} to get N_3. Then vehicle verifies if N_3 is legal, if the verification is successful, vehicle encrypts N_4: $C_{v-RSU} = K_{v-RSU}\{N_4\}$ and executes step 6). Otherwise, initial authentication fails.
6) Vehicle sends C_{v-RSU} to RSU.
7) Once C_{v-RSU} is received, RSU first decrypts C_{v-RSU} and gets N_4. Then RSU checks if N_4 is legal. If the verification is successful, RSU updates the pointer index with the vehicle's pseudonym PS_v, then RSU chooses m pseudonyms randomly:(SET_{PS}) and signs them to get $Cert = Sign\_SK_{RSU}\{SET_{PS}||EXP\}$, finally, RSU encrypts <SET_{PS}, EXP, Cert> to get $C_{RSU-v} = K_{RSU-v}\{SET_{PS}, EXP, Cert\}$ and executes step 7). Otherwise initial authentication fails.
8) RSU sends C_{RSU-v} to vehicle.
9) When getting the message from RSU, vehicle decrypts C_{RSU-v} and stores <SET_{PS}, EXP, Cert>.

F. HANDOVER AUTHENTICATION PROTOCOL

Taking Figure 2 as the scenario, once vehicle leaves RSU_1 accessed in the initial authentication and enters the coverage range of RSU_2, the handover authentication protocol will be triggered. During the handover authentication, vehicle generates ring signature for authentication. RSU_2 verifies the signature anonymously. The specific process is shown in Figure 8.

1) Vehicle selects random number $N_5 \in Z_q^*$, and uses the private key SK_v to generate ring signature $Sign_v = Sign\_ring\_SK_v\{ID_{RSU_1}, Cert, N_5, TS_3, r_vPK_v\}$.
2) Vehicle sends <SET_{PS}, ID_{RSU_1}, EXP, Cert, N_5, TS_3, r_vPK_v, $Sign_v$> to RSU_2.
3) When receiving the message from vehicle, RSU_2 verifies EXP, Cert, and $Sign_v$ respectively. If all the verifications are successful, RSU_2 regards vehicle as a legal mode and generates the session key $K_{RSU_2-v} = r_{RSU_2}r_vPK_v$. Otherwise, the authentication

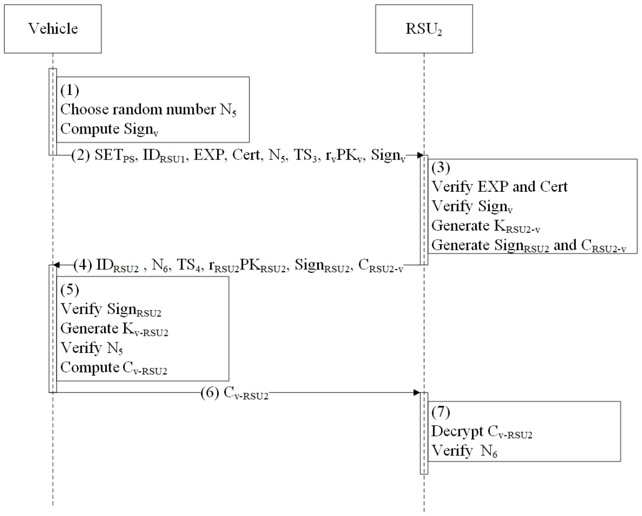

FIGURE 8. Handover authentication protocol.

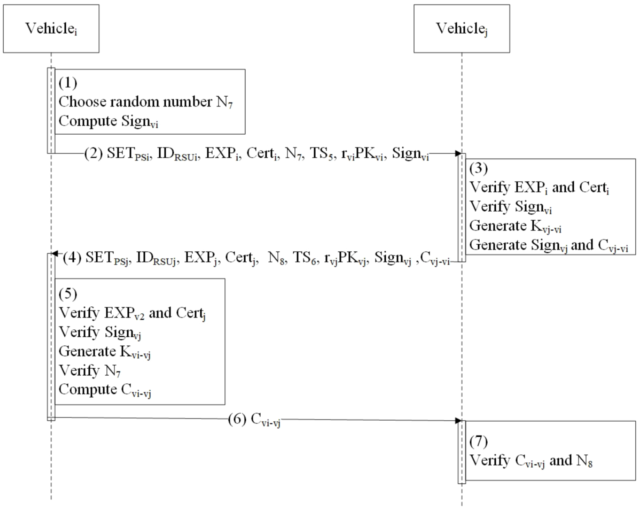

FIGURE 9. V2V authentication protocol.

is fail. Finally, RSU_2 derives the signature $Sign_{RSU_2} = Sign\_SK_{RSU_2}\{ID_{RSU_2}, N_6, TS_4, r_{RSU_2}PK_{RSU_2}\}$ and $C_{RSU_2-v} = Enc\_K_{RSU_2-v}\{N_5\}$.

4) RSU_2 sends $<ID_{RSU_2}$, N_6, TS_4, $r_{RSU_2}PK_{RSU_2}$, $Sign_{RSU_2}$, $C_{RSU_2-v}>$ to vehicle.
5) When receiving the message from RSU_2, vehicle verifies $Sign_{RSU_2}$. If the verification is successful, the vehicle generates the session key $K_{v-RSU_2} = r_vr_{RSU_2}PK_{RSU_2}$ and decrypts C_{RSU_2-v} to get N_5, If N_5 is legal, then vehicle encrypts N_6 to get $C_{v-RSU} = K_{v-RSU}\{N_6\}$. If one of the verifications fails, handover authentication is failed.
6) Vehicle sends C_{v-RSU_2} to RSU_2.
7) RSU_2 decrypts C_{v-RSU_2} with K_{RSU_2-V} to get N_6. If N_6 is legal, then the trust relationship between RSU_2 and vehicle is built. Otherwise, handover authentication is failed.

Once the vehicle's Cert is about to expire, the vehicle needs to request a new pseudonym ring from the RSU being accessed. The vehicle should send its own pseudonym PS_v to RSU_2 through the secure channel. After receiving the request from vehicle, RSU_2 will execute step 7-9 in the initial authentication protocol.

G. V2V AUTHENTICATION PROTOCOL

In order to build the trust relationship between vehicles ($vehicle_i$ and $vehicle_j$), the V2V authentication protocol is executed as Figure 9.

1) $Vehicle_i$ selects the random number $N_7 \in Z_q^*$ and uses the private key SK_{vi} to generate a ring signature $Sign_{vi} = Sign\_ring\_SK_{vi}\{ID_{RSU_i}, Cert_i, N_7, TS_5, r_{vi}PK_{vi}\}$.
2) $Vehicle_i$ sends $<SET_{PSi}$, ID_{RSU_i}, EXP_i, $Cert_i$, N_7, TS_5, $r_{vi}PK_{vi}$, $Sign_{vi}>$ to $vehicle_j$.
3) When receiving the message from $vehicle_i$, $vehicle_j$ checks EXP_i, $Cert_i$, and $Sign_{vi}$ respectively. If one of the verification is not successful, V2V authentication fails. Otherwise, $vehicle_j$ generates session key $K_{vi-vj} = r_{vj}r_{vi}PK_{vi}$, the signature $Sign_{vj} = Sign\_SK_{vj}\{ID_{RSU_j}, Cert_j, N_8, TS_6, r_{vj}PK_{vj}\}$, and $C_{i-j} = Enc\_K_{vi-vj}\{N_7\}$.
4) $Vehicle_j$ sends $<SET_{PSj}$, ID_{RSU_j}, EXP_j, $Cert_j$, TS_6, N_8, $r_{vj}PK_{vj}$, $Sign_{vj}$, $C_{i-j}>$ to $vehicle_i$.
5) Upon receipt of the message from $vehicle_j$, $vehicle_i$ verifies EXP_j, $Cert_j$, and $Sign_{vj}$. If one of the verifications fails, then $vehicle_j$ is thought as an illegal vehicle, V2V authentication fails. Otherwise, $vehicle_j$ generates session key $K_{vi-vj} = r_{vi}r_{vj}PK_{vj}$ and decrypts C_{i-j} to get N_7. If N_7 is legal, $vehicle_j$ encrypts the random number N_8 with K_{vi-vj} to obtain $C_{vi-vj} = K_{vi-vj}\{N_8\}$. Otherwise, V2V authentication fails.
6) $Vehicle_i$ sends C_{vi-vj} to $vehicle_j$.
7) $Vehicle_j$ decrypts C_{vi-vj} through the shared key K_{vi-vj} to obtain N_8. If N_8 is legal, the trust relationship is established between v_i and v_j. Otherwise, V2V authentication fails.

IV. SECURITY ANALYSIS

In VSNs, the security of communication between vehicles directly affects the security of the whole network. Consequently, we first give a formal security proof of the proposed V2V authentication protocol under SVO logic [30]. As each vehicle is equipped with an OBU, vehicle is thus represented by OBU in the security proof. Afterwards, we further present some security analysis of V2V authentication protocol.

A. SVO LOGIC

SVO logic [30] is a security protocol analysis measure proposed by Syverson and Orschot in 1994. It establishes a reasonable theoretical model for the logical system. In the formal semantics, some concepts are redefined and some limitations in the AT logic [31] are eliminated. The advantages of

TABLE 2. Notation and description in SVO.

Notation	Description
$\vdash \varphi$	φ 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
$\mathrm{fresh}(X)$	X is fresh
$\{X\}K$	The ciphertext encrypted by K
$[X]K$	The message signed by K

SVO are mainly embodied in the following four aspects.

- Clear semantics of modal theory are defined.
- A fairly detailed computational model is introduced.
- Excellent extensibility.
- Conciseness.

1) SYMBOLS

In order to facilitate the following security proof, the relevant notations and descriptions are given as Table 2.

2) FORMAL DESCRIPTION

(1) Goals

The main aim of this phase is to establish a trust relationship between vehicles, including achieving mutual authentication between vehicles, ensuring that the exchanging message is fresh, and establishing a shared key. Consequently, In SVO, the goal can be set as below:

G$_1$: OBU$_i$ believes OBU$_j$ says (ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vj}$PK$_{vj}$) OBU$_j$ believes OBU$_i$ says (ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$)

G$_2$: OBU$_i$ believes OBU$_j$ says (N$_7$) OBU$_j$ believes OBU$_i$ says (N$_8$)

G$_3$: OBU$_i$ believes sharedkey (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}-$, OBU$_i$, OBU$_j$) OBU$_j$ believes sharedkey (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}-$, OBU$_j$, OBU$_i$)

G$_4$: OBU$_i$ believes sharedkey (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}+$, OBU$_i$, OBU$_j$) OBU$_j$ believes sharedkey (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}+$, OBU$_j$, OBU$_i$)

G$_5$: OBU$_i$ believes fresh (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$) OBU$_j$ believes fresh (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$)

(2) Assumptions

P1: OBU$_i$ believes fresh(TS$_8$) OBU$_j$ believes fresh(TS$_7$)

P2: OBU$_i$ believes OBU$_i$ received (([ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vj}$PK$_{vj}$]ring_SK$_{\mathrm{OBU}_j}$) $\supset$ PK$_\delta$ (OBU$_j$, r$_{\mathrm{OBU}_j}P$)) OBU$_j$ believes OBU$_j$ received (([ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$] ring_SK$_{\mathrm{OBU}_i}$) $\supset$ PK$_\delta$(OBU$_i$, r$_{\mathrm{OBU}_i}P$))

P3: OBU$_i$ believes OBU$_i$ received {N$_7$}K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$ OBU$_j$ believes OBU$_j$ received {N$_8$}K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$

P4: OBU$_i$ believes PK$_\sigma$(OBU$_j$, PK$_{\mathrm{OBU}_j}$) OBU$_j$ believes PK$_\sigma$(OBU$_i$, PK$_{\mathrm{OBU}_i}$)

P5: OBU$_i$ believes SV([ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vj}$PK$_{vj}$] ring_SK$_{\mathrm{OBU}_j}$, ring_PK$_{\mathrm{OBU}_j}$, (ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vj}$PK$_{vj}$)) OBU$_j$ believes SV([ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$] ring_SK$_{\mathrm{OBU}_i}$, ring_PK$_{\mathrm{OBU}_i}$, (ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$))

P6: OBU$_i$ believes ((OBU$_j$ says (ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vi}$PK$_{vi}$)) $\supset$ PK$_\delta$ (OBU$_j$, r$_{\mathrm{OBU}_j}P$)) OBU_j believes ((OBU$_i$ says (ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$)) $\supset$ PK$_\delta$ (OBU$_i$, r$_{\mathrm{OBU}_i}P$))

P7: OBU$_i$ believes PK$_\delta$ (OBU$_i$, r$_{\mathrm{OBU}_i}P$) OBU$_j$ believes PK$_\delta$ (OBU$_j$, r$_{\mathrm{OBU}_j}P$)

P8: OBU$_i$ believes OBU$_i$ sees PK$_\delta$ (OBU$_i$, r$_{\mathrm{OBU}_i}P$) OBU$_j$ believes OBU$_j$ sees PK$_\delta$ (OBU$_j$, r$_{\mathrm{OBU}_j}P$)

P9: $\neg$ (OBU$_i$ said {N$_8$}K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$) $\neg$ (OBU$_j$ said {N$_7$}K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$)

P10: OBU$_i$ believes fresh(N$_7$) OBU$_j$ believes fresh(N$_8$)

(3) Security proof

From P2, P4, Ax4, we can get:

S1: OBU$_i$ believes OBU$_j$ said (ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vj}$PK$_{vj}$) OBU$_j$ believes OBU$_i$ said (ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$)

From S1, P1, Ax19, we can get:

S2: OBU$_i$ believes OBU$_j$ says (ID$_{\mathrm{RSU}_j}$, Cert$_j$, N$_8$, TS$_6$, r$_{vj}$PK$_{vj}$) OBU$_j$ believes OBU$_i$ says (ID$_{\mathrm{RSU}_i}$, Cert$_i$, N$_7$, TS$_5$, r$_{vi}$PK$_{vi}$) (G$_1$ **is proved**)

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

S3: OBU$_i$ believes PK$_\delta$ (OBU$_j$, r$_{\mathrm{OBU}_j}P$) OBU$_j$ believes PK$_\delta$ (OBU$_i$, r$_{\mathrm{OBU}_i}P$)

From S3, P7, Ax5, we can get:

S4: OBU$_i$ believes sharedkey (K$_{\mathrm{OBU}_i-\mathrm{OBU}_i}$, OBU$_i$, OBU$_j$) OBU$_j$ believes sharedkey (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$, OBU$_j$, OBU$_i$) where K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$ $=$ F(r$_{\mathrm{OBU}_j}$, r$_{\mathrm{OBU}_i}P$), K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$ $=$ F(r$_{\mathrm{OBU}_i}$, r$_{\mathrm{OBU}_j}P$)

From P2, Ax1, Ax10, we can get:

S5: OBU$_i$ believes (OBU$_i$ sees PK$_\delta$ (OBU$_j$, r$_{\mathrm{OBU}_j}P$)) OBU$_j$ believes (OBU$_j$ sees PK$_\delta$ (OBU$_i$, r$_{\mathrm{OBU}_i}P$))

From S5, P8, Ax5, we can get:

S6: OBU$_i$ believes OBU$_i$ sees sharedkey (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$, OBU$_i$, OBU$_j$) OBU$_j$ believes OBU$_j$ sees sharedkey (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$, OBU$_j$, OBU$_i$) where K$_{\mathrm{OBU}_j-}$$OBU_i = F(r_{OBU_j}, r_{OBU_i}P)$, K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$ $=$ F(r$_{\mathrm{OBU}_i}$, $r_{OBU_j}P$)

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

S7: OBU$_i$ believes sharedkey (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}-$, OBU$_i$, OBU$_j$) OBU$_j$ believes sharedkey (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}-$, OBU$_j$, OBU$_i$) (G$_3$ **is proved**)

From P1, P2, S4, Ax17, Ax18, we can get:

S8: OBU$_i$ believes fresh (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$) OBU$_j$ believes fresh (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$) (G$_5$ **is proved**)

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

S9: confirm $_{\mathrm{OBU}_i}$ (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}$) confirm $_{\mathrm{OBU}_j}$ (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}$)

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

S10: OBU$_i$ believes sharedkey (K$_{\mathrm{OBU}_i-\mathrm{OBU}_j}+$, OBU$_i$, OBU$_j$) OBU$_j$ believes sharedkey (K$_{\mathrm{OBU}_j-\mathrm{OBU}_i}+$, OBU$_j$, OBU$_i$) (G$_4$ **is proved**)

From P3, S4, Ax3, we can get:

S11: $\mathrm{OBU_i}$ believes $\mathrm{OBU_j}$ said $(\mathrm{N_7})$ $\mathrm{OBU_j}$ believes $\mathrm{OBU_i}$ said $(\mathrm{N_8})$

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

S12: $\mathrm{OBU_i}$ believes $\mathrm{OBU_j}$ says $(\mathrm{N_7})$ $\mathrm{OBU_j}$ believes $\mathrm{OBU_i}$ says $(\mathrm{N_8})$ ($\mathrm{G_2}$ **is proved**)

B. FURTHER SECURITY ANALYSIS

Besides the security proof, correctness, minimum disclosure, conditional anonymity and distributed resolution authority, perfect forward privacy, and unforgeability of the authentication protocol are further analyzed.

1) CORRECTNESS

In V2V authentication, if message M is signed correctly and the signature σ is not tamper during propagation, σ must satisfy the verification equation.

2) MINIMUM DISCLOSURE

The proposed protocol executes authentication depending on a set of legal pseudonyms, there is no additional disclosure of the real identities of the entities.

3) CONDITIONAL ANONYMITY & DISTRIBUTED RESOLUTION AUTHORITY

In V2V authentication, even if the adversary can attach all ring members' pseudonyms, the probability of determining the true pseudonym of the vehicle is less than 1/m, where m is the number of the pseudonym ring members stored in vehicle. Besides, we cannot only rely on RSU or TA to identify the true identity of the vehicle. However, in some special scene, super investigator can use $\mathrm{ID_{RSU}}$ and Cert to require illegal vehicle's pseudonym $\mathrm{PS_v}$ from RSU, then TA uses k to decrypt $\mathrm{PS_v}$ and reveal illegal vehicle's true identity. Thus, the real identity of the vehicle can be identified through the cooperation of RSU and TA.

4) PERFECT FORWARD PRIVACY

The identity of the ring member is displayed in an anonymity form and the signatures of each vehicle do not contain exactly the same members. Consequently, after the verification of a vehicle's signature, the verifier cannot reduce the probability of obtaining the true identity of the signer through the signature or message.

5) UNFORGEABILITY

Without knowing the vehicle's private key, the probability of an adversary forging a legal ring signature is negligible even though he/she is able to obtain the signature of M from a random oracle model.

V. PERFORMANCE ANALYSIS

In this section, the proposed scheme (APPAS) is compared with EDKM [18] and PACP [13] in computation cost and transmission overhead for the performance analysis.

TABLE 3. Symbol, description and execution time.

Symbol	Description	Execution time(ms)
$\mathrm{T_{mtp}}$	The execution time of hash-to-point	4.4
$\mathrm{T_{bp}}$	The execution time of bilinear pairing	4.5
$\mathrm{T_{pm}}$	The shared key between point multiplication	0.6

A. COMPUTATION COST

Computation cost refers to the total amount of computation that a vehicle needs to perform during the authentication process. Due to weak computation capabilities, vehicle's computation cost makes a great impact on the authentication efficiency. Thus, we give the comparison analysis on V2V authentication among different schemes. Before the detailed analysis, the symbol, description and execution time of some necessary operations in the schemes are shown in table 3 according to [34].

In EDKM, in order to derive the signature σ, $\mathrm{vehicle_i}$ computes $U = \mathrm{H_1(r_2}||M)\in \mathrm{G_1}$, $V = \mathrm{H_1(r_2g_1}||M)\in \mathrm{G_1}$, $\mathrm{T_1} = \alpha U, \mathrm{T_2} = \alpha \mathrm{V_i} + \mathrm{A_i^{j,k}}$, and $\delta = \alpha \mathrm{x_i}$ respectively, where $\mathrm{r_2}$ and α are random numbers, $<\mathrm{x_i}, \mathrm{A_i^{j,k}}>$ is the group key. Then vehicle $_i$ selects random number $\mathrm{r}_\alpha, \mathrm{r_x}, \mathrm{r}_\delta$ and generates $\mathrm{R_1, R_2, R_3}, c, \mathrm{s}_\alpha, \mathrm{s}_\delta$:

$$
\begin{aligned}
R_1 &= \mathrm{r}_\alpha U.\\
R_2 &= \mathrm{e(T_2, P_1)^{r_x} e(V_i, P_2)^{-r_\alpha} e(V_i, P_1)^{-r_\delta}}.\\
R_3 &= \mathrm{r_x T_1} - \mathrm{r}_\delta U.\\
c &= \mathrm{H_2(M||r_2||T_1||T_2||R_1||R_2||R_3)}.\\
\mathrm{s}_\alpha &= \mathrm{r}_\alpha + c\alpha, \mathrm{s_x} = \mathrm{r_x} + cx_i.\\
\mathrm{s}_\delta &= \mathrm{r}_\delta + c\delta.
\end{aligned}
$$

The signature is $\sigma = (\mathrm{r_2, T_1, T_2}, c, \mathrm{s}_\alpha, \mathrm{s_x}, \mathrm{s}_\delta)$. After receiving σ from $\mathrm{vehicle_j}$, $\mathrm{vehicle_i}$ for verification should compute $U = \mathrm{H_1(r_2}||M)$ and $\mathrm{V_j} = \mathrm{H_1(r_2g_1}||M)$. Then, $\tilde{\mathrm{R}}_1, \tilde{\mathrm{R}}_2, \tilde{\mathrm{R}}_3$ are calculated:

$$
\begin{aligned}
\tilde{\mathrm{R}}_1 &= \mathrm{s}_\alpha U - c\mathrm{T_1}.\\
\tilde{\mathrm{R}}_2 &= \mathrm{e(T_2, P_1)^{s_x} e(V_j, P_2)^{-s_\alpha} e(V_j, P_1)^{-s_\delta}}\\
&\qquad \times(e(\mathrm{T_2, P_2})/\mathrm{e(PK^1_{RM_j}, PK^1_{RM_j})})^{\mathrm{c}}.\\
\tilde{\mathrm{R}}_3 &= \mathrm{s_x T_1} - \mathrm{s}_\delta U.
\end{aligned}
$$

Finally, $\mathrm{vehicle_i}$ checks whether $c == \mathrm{H_2(M||r_2||T_1||T_2||\tilde{R}_1||\tilde{R}_2}||\tilde{R}_3)$. If the equation holds, σ is legal. Otherwise, the authentication is failed. Consequently, we can get the computation cost in V2V of EDKM is:

$$
\begin{aligned}
\mathrm{CC_{EDKM}} &= \mathrm{26T_{PM} + 8T_{BP} + 4T_{MTP}}\\
&= 69.2(\mathrm{ms})
\end{aligned}
\tag{1}
$$

In PACP, $\mathrm{vehicle_i}$ computes its signature depending on BLS signature mechanism [37] and $\mathrm{vehicle_j}$ verifies the signature from. Then the encryption and decryption operation are required to execute including: $\lambda^{\mathrm{j}}_{\mathrm{(a,i)}} = \mathrm{e}(\Gamma^{\mathrm{j}}_{\mathrm{(a,i)}}, \sigma^{\mathrm{j}}_{\mathrm{a}}P)$, $\rho = \mathrm{H_2}(k, M), C =< \mathrm{H}(\rho P) \oplus (\lambda^{\mathrm{j}}_{\mathrm{(a,i)}})^k, e(P, \sigma^{\mathrm{j}}_{\mathrm{a}}P)^k, M \oplus \mathrm{H_1(e}(\sigma^{\mathrm{j}}_{\mathrm{a}}P, \mathrm{H}(\rho P)P)) >$, $\Gamma^{\mathrm{j}}_{\mathrm{(a,i)}} = U \oplus V^{\mathrm{S}^{\mathrm{j}}_{\mathrm{(a,i)}}}$, and

TABLE 4. The length of the parameters.

Factor	Size(byte)
G_1	128
G_2	40
Z_q^*	20
$HASH_{SHA-256}$	256
Expiration time	4
Certification	120

$M' = W \oplus H_1(e(\sigma_a^j P, \Gamma^j_{(a,i)}P))$. Besides, vehicle has to generate a signature and verify the signature from other vehicle. Since the authors do not specify the specific signature scheme, it is assumed that its signature mechanism is the BLS short signature scheme [37]. Thus, two hash-to point operations, two bilinear pairing operations, and one point multiplication operation are asked to executed. The computation cost of PACP is:

$$\begin{aligned} CC_{PACP} &= 6Tmtp + 6Tbm + 16Tpm \\ &= 63(ms) \end{aligned} \tag{2}$$

In APPAS, to sign message M, vehicle$_i$ first computes $h_i = H_2(M||L||U_i)$, and gets $U_s = r'_s Q_{ID} - \sum_{i\neq s}\{U_i + h_i Q_{ID}\}$. Then $h_s = H_0(M||L||U_s)$ and $V = (h_s + r'_s)\ S_{ID}$ are computed. The signature is $\sigma = \{\cup_{i=1}^{n}\{U_i\}, V\}$. When receiving σ, vehicle$_j$ computes $h_s = H_0(M||L||U_s)$, and checks $e(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID})) == e(P, V)$ to verify whether σ is legal. Thus the computation cost of APPAS in V2V authentication is:

$$\begin{aligned} CC_{APPAS} &= (m^2 + m + 1)T_{PM} + 2T_{BP} \\ &= (m^2 + m + 1) \times 0.6 + 8.8(ms) \end{aligned} \tag{3}$$

where m is the number of pseudonym members used in ring signature. According to (1-3), we can see that when the number of pseudonym ring member is less than 9, APPAS owns superiority in computation cost.

B. COMMUNICATION OVERHEAD

Communication overhead(CO) refers to the size of total message transmitted in V2V authentication. As EDKM and PACP do not define the content of message M, the size of message M is ignored. According to [38] and [39], the length of the parameters is defined respectively as table 4.

In EDKM, the signature is $\sigma = (r_2, T_1, T_2, c, s_\alpha, s_x, s_\delta)$, where $r_2 \in Z_q^*$, $T_1 \in G_1$, $T_2 \in G_1$, $c \in Z_q^*$, $s_\alpha \in G_1$, $s_x \in G_1$, $s_\delta \in G_1$, $\sigma \in G_1$. Consequently, the communication overhead of EDGK is:

$$\begin{aligned} CC_{EDGK} &= 6 \times 128 + 2 \times 20 \\ &= 808(bytes) \end{aligned} \tag{4}$$

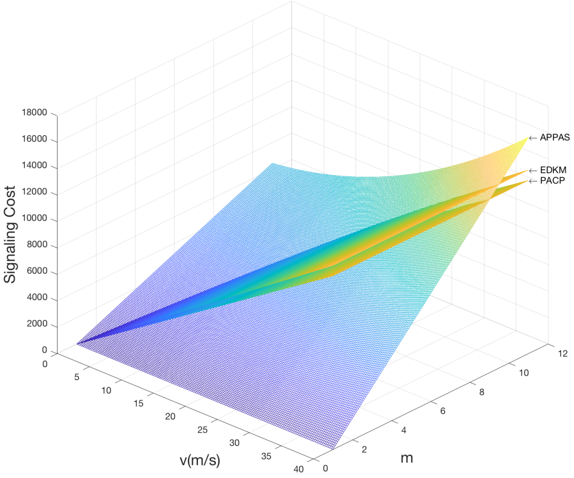

FIGURE 10. Signaling cost.

In PACP, in order to prove the legitimacy of vehicle's identity, vehicle broadcasts $PN^j_{(a,i)} = <\sigma_a^j P, \gamma^j_{(a,i)}, t^j_{(a,i)}, SIG(t^j_{(a,i)}, \gamma^j_{(a,i)}; S_{R_i}), Cert_{R_i}>$, where $\sigma_a^j P \in G_1$, $\gamma^j_{(a,i)} \in G_1$, $t^j_{(a,i)}$ is the expiration time, $SIG(t^j_{(a,i)}, \gamma^j_{(a,i)}; S_{R_i}) \in G_1$. Besides, ciphertext $C = < H(\rho P) \oplus (\lambda^j_{(a,i)})^k, e(P, \sigma_a^j P)^k, M \oplus H_1(e(\sigma_a^j P, H(\rho P)P)) >$ Thus, the communication overhead of PACP is:

$$\begin{aligned} CC_{PACP} &= 4 \times 128 + 120 + 4 + 2 \times 256 \\ &= 1148(bytes) \end{aligned} \tag{5}$$

In APPAS, the signature is $\sigma = \{\cup_{i=1}^{n}\{U_i\}, V\}$, where $U_i \in G_1$, $V \in G_1$. Therefore, the communication overhead of APPAS is:

$$\begin{aligned} CC_{PACP} &= n \times 128 + 128 \\ &= (n+1) \times 128(bytes) \end{aligned} \tag{6}$$

According to (4-6), we can see that when n is less than 6, APPAS owns lower communication overhead.

C. SIGNALING COST

The signaling cost refers to the amount of authentication signaling costs. In this section, the fluid-flow model [35] is adopted to analyze the signaling cost. In fluid-flow model, we suppose that all the subnets are circles with the same radius, and vehicle's movement direction is considered in the range of $(0, 2\pi)$. The crossing rate(R) and signaling cost (SC) can be defined as:

$$R = \frac{\rho v L}{\pi} \tag{7}$$

$$SC = AL \times R \tag{8}$$

where ρ, v, L refer to vehicles' density, vehicles' average speed, and the perimeters of a cell respectively, AL means authentication latency. We sets transmission delay $TD = 20ms$, $L = 100m$, $\rho = 0.1(1/m^2)$, $v = 0 \sim (40m/s)$, $m = 1 \sim 11$ according to [36]. As shown in Figure 10, we can see that APPAS owns certain advantages in signaling cost compared with other schemes when the number of pseudonym is about 7 to 9.

VI. CONCLUSION

Pseudonym and group signature are two important approaches to achieve the anonymous authentication of vehicles in VSNs. However, the mechanisms suffer from either privacy strength or efficiency. In this paper, we integrate identity-based ring signature mechanism and pseudonym to propose an effective authentication scheme, which satisfies the anonymous authentication needs in VSNs. Security and performance analysis demonstrate that the proposed scheme is robust and efficient.

In the future work, a novel key management protocol will be researched in depth due to the importance of key management in VSNs.

REFERENCES

[1] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIPJ. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 62, Mar. 2018.

[2] X. Kong, M. Li, T. Tang, K. Tian, L. Moreira-Matias, and F. Xia, "Shared subway shuttle bus route planning based on transport data analytics," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 4, pp. 1507–1520, Oct. 2018.

[3] A. M. Vegni and V. Loscrí, "A survey on vehicular social networks," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.

[4] F. Xia, J. Wang, X. Kong, Z. Wang, J. Li, and C. Liu, "Exploring human mobility patterns in urban scenarios: A trajectory data perspective," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 142–149, Mar. 2018.

[5] X. Wang *et al.*, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, to be published.

[6] K. Chen, L. Dong, and X. Lai, "Security analysis of cryptographic protocols based on trusted freshness," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 18, no. 6, pp. 219–232, Nov. 2008.

[7] S. A. A. Shah, E. Ahmed, F. Xia, A. Karim, M. Shiraz, and R. M. Noor, "Adaptive beaconing approaches for vehicular ad hoc networks: A survey," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1263–1277, Jun. 2018.

[8] Y.-C. Wei, Y.-M. Chen, and H.-L. Shan, "Beacon-based trust management for location privacy enhancement VANETs," in *Proc. 13th Asia–Pacific Netw. Oper. Manage. Symp.*, Taipei, Taiwan, Sep. 2011, pp. 1–8.

[9] 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.

[10] Y. Chen and Y. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.

[11] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016.

[12] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *Proc. Int. Conf. Pervasive Comput. Appl.*, Birmingham, U.K., Jul. 2007, pp. 424–429.

[13] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[14] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *Proc. IEEE Int. Conf. Commun.*, vol. 29, no. 16, May 2010, pp. 1–6.

[15] M. Han, L. Hua, L. Wang, H. Jiang, and S. Ma, "Effcient communication protocol of group negotiation in VANET," *J. Commun.*, vol. 39, no. 1, pp. 34–45, Jan. 2018.

[16] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for VANETs," in *Proc. GLOBECOM Workshops*, Atlanta, GA, USA, Dec. 2013, pp. 4609–4614.

[17] 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.

[18] 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.

[19] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *Int. J. Netw. Secur.*, vol. 17, no. 2, pp. 135–141, 2015.

[20] J. Zhang, W. Zhen, and M. Xu, "An efficient privacy-preserving authentication protocol in VANETs," in *Proc. IEEE 9th Int. Conf. Mobile Ad-Hoc Sensor Netw.*, Dec. 2013, pp. 272–277.

[21] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *Proc. 2nd Int. Conf. SecureComm Workshops*, Aug./Sep. 2006, pp. 1–5.

[22] B. K. Chaurasia and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," in *Transactions on Computational Science XIII* (Lecture Nodes in Computer Science). Berlin, Germany: Springer, 2011, pp. 147–156.

[23] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Comput. Elect. Eng.*, vol. 38, no. 3, pp. 573–581, 2012.

[24] H. J. Miller and S.-L. Shaw, *Geographic Information Systems for Transportation: Principles and Applications*. London, U.K.: Oxford Univ. Press, 2001.

[25] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing," in *Advances in Cryptology—CRYPT*. Philadelphia, PA, USA: Springer, 2001, pp. 213–229.

[26] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2001, pp. 552–565.

[27] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* New York, NY, USA: Springer-Verlag, 2002, pp. 533–547.

[28] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Berlin, Germany: Springer, 2005, pp. 499–512.

[29] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, Mar. 2015.

[30] P. F. Syverson and P. C. van Oorschot, "On unifying some cryptographic protocol logics," in *Proc. IEEE Comput. Soc. Symp.*, Mar. 1994, pp. 14–28.

[31] M. Abadi and M. R. Tuttle, "A semantics for a logic of authentication," in *Proc. ACM Annu. Symp. Princ. Distrib. Comput.*, New York, NY, USA, 1991, pp. 201–216.

[32] L. Chen and J. Malone-Lee, "Improved Identity-based signcryption," in *Public Key Cryptography—PKC*. Berlin, Germany: Springer, 2005, pp. 362–379.

[33] J. C. Choon and J. H. Cheon, "An Identity-Based Signature from Gap Diffie–Hellman Groups," in *Proc. Int. Workshop Public Key Cryptogr.* New York, NY, USA: Springer-Verlag, 2003, pp. 18–30.

[34] M. Scott, "On the efficient implementation of pairing-based protocols," in *Cryptography and Coding*. Berlin, Germany: Springer, 2011.

[35] S. Pack and Y. Choi, "A study on performance of hierarchical mobile IPv6 in IP-based cellular networks," *IEICE Trans. Commun.*, vols. E87-B, no. 3, pp. 462–469, 2004.

[36] J.-H. Lee and J.-M. Bonnin, "HOTA: Handover optimized ticket-based authentication in network-based mobility management," *Inf. Sci.*, vol. 230, no. 4, pp. 64–77, 2013.

[37] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. ASIACRYPT*, vol. 2248, 2001, pp. 514–532.

[38] X. Boyen and L. Martin, *Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*, document RFC 5091, 2007.

[39] C. Adams and D. Pinkas, *Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)*, document RFC 3161, Jan. 2001.

TIANHAN GAO received the B.E. degree in computer science and Technology and the M.E. and Ph.D. degrees in computer application technology from Northeastern University, China, in 1999, 2001, and 2006, respectively. In 2006, he joined the Software College, Northeastern University, as a Lecturer. He obtained an early promotion to an Associate Professor, in 2010. He has been a Visiting Scholar with the Department of Computer Science, Purdue, from 2011 to 2012. He obtained the doctoral tutor qualification, in 2016. He has authored or co-authored more than 50 research publications. His primary research interests include next-generation network security, wireless mesh network security, security and privacy in ubiquitous computing, and virtual reality.

XINYANG DENG received the B.E. degree from the Software College, Dalian University of Foreign Languages, in 2014, and the M.E. degree from the Software College, Northeastern University, in 2018. He is currently pursuing the degree with the Software College, Northeastern University. His primary research interests include next-generation network security, PMIPv6 security, and identity-based cryptography.

QINGSHAN LI received the B.E. degree in management information system from Northeastern University, in 1999, and the M.E. degree in software engineering from Peking University, China, in 2012, where he is currently pursuing the Ph.D. degree in computer software and theory. In 2009, he joined Peking University as an Associate Research Fellow. He was the Technical Director and the Vice President of the Network Security Department, Neusoft Group, before 2009. He is also the Associate Director and a Research Fellow with the Information Security Laboratory, Peking University. His primary research interests include network security and intelligent mobile terminal security, especially the detection technology for advanced persistent threat (APT).

MARIO COLLOTTA received the confirmation by the National Advisory Commission in order to become an Associate Professor, in 2017. Since 2010, he has been a tenured Assistant Professor (SSD ING-INF/05) of computer engineering with the Faculty of Engineering and Architecture, Kore University of Enna, Italy. He is currently the Chair of the BD Course in computer science engineering with the Kore University of Enna. He is scientific responsible of the Computer Engineering and Networks Laboratory, Kore University of Enna. His research interests include the study of innovative solutions and approaches in control real-time application systems and networks.

ILSUN YOU (SM'13) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was a Research Engineer with Thin Multimedia, Inc., Internet Security Co., Ltd., and Hanjo Engineering Co., Ltd. He is currently an Associate Professor with the Department of Information Security Engineering, Soonchunhyang University. He has focused on 4/5G security, security for wireless networks and mobile Internet, and the IoT security. He has published more than 180 papers in these areas. He is a Fellow of the IET. He has served or is currently serving as a main organizer of international conferences and workshops, such as MIST, MobiWorld, and MobiSec. He is the Editor-in-Chief of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (JoWUA). He serves on the Editorial Board of *Information Sciences* (INS), the *Journal of Network and Computer Applications* (JNCA), the IEEE ACCESS, *Intelligent Automation and Soft Computing* (AutoSoft), the *International Journal of Ad Hoc and Ubiquitous Computing* (IJAHUC), *Computing and Informatics* (CAI), and the *Journal of High Speed Networks* (JHSN).

• • •