Research Article

A Distributed Pseudonym Management Scheme in VANETs

Xiaoling Zhu,1 Yang Lu,1,2 Benhong Zhang,1 and Zhengfeng Hou1

1 School of Computer and Information, Hefei University of Technology, Hefei 230009, China
2 The Anhui Provincial Key Laboratory of Mine IoT and Mine Safety Supervisory Control, Hefei 230088, China

Correspondence should be addressed to Xiaoling Zhu; zhuxl@hfut.edu.cn

Received 22 December 2012; Accepted 3 April 2013

Academic Editor: Xu Yongjun

Copyright © 2013 Xiaoling Zhu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security and privacy have been important issues in VANETs. Anonymity is an effective way to achieve privacy protection, and it sometimes requires to be disclosed for determining traffic liability. In most pseudonym schemes, an authority is aware of a vehicle's secret, and its compromise will result in the leakage of a large amount of privacy information. So, we propose a distributed traceable pseudonym management scheme in VANETs. In the scheme, a blind signature method is adopted to achieve strict separation of issuance and tracking. The distributed tracking protocol is proposed to enhance the robustness for tracking, which is based on the improved scheme for shared generation of RSA keys. An efficient pseudonymous authentication mechanism is proposed to reduce the communication overhead. Compared with other related proposals, our scheme is unforgeability, especially against authority forge attacks, and has better robustness. Moreover, the performance analysis shows that it is efficient in VANETs.

1. Introduction

Vehicle-to-vehicle and vehicle-to-infrastructure communications improve vehicle's perception from the surrounding environment. Vehicular ad hoc networks (VANETs) will be used widely in collision avoidance, road-hazard notification, and coordinated driving systems [1]. Nonetheless, there are many security threats in VANETs [2–4]. For example, an attacker might tamper with messages to evade accident liability or forge information to meet specific needs. The attacker also might eavesdrop on broadcast messages, analyze data, and track a vehicle. So, security and privacy have been important issues in VANETs.

A number of studies have been made on the issues of security and privacy preservation. Raya and Hubaux [5, 6] pointed out that anonymity is conditional for liability purposes and that authority can disclose the pseudonym. In [5, 6], a security protocol was introduced. Although this protocol can effectively meet the conditional privacy requirement, it is far from efficient and can hardly become a scalable and reliable approach, because the authority has to keep all the anonymous certificates for each vehicle. Lin et al. [7] proposed a security and privacy preserving protocol. With group signature, security, privacy, and traceability can be achieved without inducing the overhead of managing a huge number of stored certificates at the authorities’ sides. Calandriello et al. [8, 9] proposed on-the-fly pseudonym generation and self-certification, which alleviates the overhead of managing certificates. Group signature method is adopted to ensure that legitimate nodes can generate their pseudonyms anonymously. Lu et al. [10] presented a conditional privacy preservation protocol, which improves efficiency in terms of the minimized anonymous keys storage at each vehicle. Performance evaluation shows that the protocol can achieve much better efficiency than Raya and Hubaux’s [5, 6] and Lin et al’s [7] when vehicles are revoked. Zhang et al. [11] proposed a scalable robust authentication protocol. In [11], some roadside units (RSUs) serve as the issuer of vehicles’ private key, and a signcryption method is employed to distribute the keys securely. Hao et al. [12] proposed a distributed key management framework, which has advantages in the revocation of malicious vehicles and system maintenance. An efficient cooperative message authentication protocol is developed to reduce the computation and communication overhead in the group signature.

The above reported schemes [7–12] are based on group signature. In Boneh et al’s group signature scheme [13], each user’s private key is generated by the private-key issuer, which
is a hidden security threat. In [7–9], each vehicle’s group private key is computed by a member manager. In [10], a trusted authority is required; the authority generates valid private keys for on-board unit and RSU. In [11], RSU generates and sends the group private key to the vehicle. In [12], some measures are adopted to prevent RSU from misbehaving, but authorities cannot decide which is the malicious, RSU or the vehicle or both, when they find a mismatch. Therefore, these schemes [7–12] suffered from private key revealing attacks, in which the private-key issuer knows each user’s private key.

Schaub et al. [14] adopted blind signature technology to achieve the separation of issuing and tracking. But the disadvantages of the scheme are that V-token \( V_i = E_{PKCA} (id \parallel r_i) \) is produced by a vehicle alone; thus, the vehicle might forge other vehicle’s V-token. Moreover, if CA is not credible, it can generate V-token by itself and sign it. CA can obtain the pseudonym certificate from a pseudonym provider and impersonate any vehicle. To solve the above problems, this paper presents a distributed pseudonym management scheme in secure VAnETs. The main contributions of the scheme are as follows. (1) Pseudonym is co-produced by the issuer and the vehicle. Either party attempting to deceive can be detected. It can resist authority forge attacks. (2) An efficient pseudonym authentication mechanism is proposed by finding the optimal number of messages with the pseudonym certificate, which not only reduces the communication overhead but also ensures the message authentication probability \( P_{auth} > 95\% \). (3) Distributed pseudonym tracking based on secret sharing method is presented. The initialization of the tracking protocol does not require a trusted center, thus avoiding any single point of failure. It offers better robustness.

The remainder of this paper is organized as follows. The pseudonym management model is given in Section 2. The pseudonym issuance protocol, the pseudonymous authentication protocol, and the distributed tracking protocol are presented in Sections 3, 4, and 5, respectively. Section 6 analyzes and compares the security and the performance of our scheme with other related schemes. Finally, the conclusion of this paper is given in Section 7.

### 2. Pseudonym Management Model

There are three types of entities: (1) a vehicle \( V \). Its identity is \( ID_V \), corresponding to a long-term public key \( (N_V, e_V) \) and a long-term private key \( d_V \). Its pseudonym is \( ID_{PV} \), corresponding to a short-term public key \( (N_{PV}, e_{PV}) \) and a short-term private key \( d_{PV} \). The vehicle contains a sensing input module, a wireless communication module, a central processing module, and a hardware security module (HSM) [15]. The HSM generates public and private keys, stores private keys, and provides digital signature service. (2) An authority: it is divided into certificate authority (CA), pseudonym certificate authority (PCA), and tracking authority (TA). PCA issues pseudonym certificates, but it does not know the pseudonym. Only TA knows the relationship between the pseudonym and the identity. CA issues \( Cert_V \), and \( Cert_{PV} \) contains \( ID_V \) and \( (N_V, e_V) \). PCA issues \( Cert_{PV} \), and \( Cert_{PV} \) contains \( ID_{PV} \) and \( (N_{PV}, e_{PV}) \). (3) TA. Its pseudonym is ID, and corresponds to a long-term public key \( (N, e) \) and \( d \), respectively. There are some PCAs in the model, and \( V \) may apply for a pseudonym to the neighboring PCA. Only a few suspicious vehicles need to be disclosed, so TAs are rare. But if only one authority acts as TA, abuse can occur. Based on the secret sharing method, we extend one authority to \( k \) authorities forming \( T_A = \{T_{A_1}, T_{A_2}, \ldots, T_{A_k}\} \). \( T_A \) (1 \( \leq i \leq k \)) may be a law enforcement agency, a judge, or a privacy protection agency. TA’s identity is ID, Assume that the vehicle is preloaded with the public keys of CA, PCA, and TAs during the vehicle’s initialization. (3) Roadside unit (RSU): it communicates with vehicles and other devices on the internet.

The security and privacy requirements in the model are as follows.

**Anonymity.** For other entities (such as PCA, attackers) except TAs, it is computationally infeasible to disclose the identity from a pseudonym.

**Traceability.** If the members in TAs implement the protocol honestly, at least \( m \) members can disclose collaboratively the identity from a pseudonym.

**Unforgeability.** For any entity, it is computationally infeasible to forge a false signature or impersonate another entity.

**Robustness.** If any authority compromises, the implementation of pseudonym issuance, pseudonymous authentication, and tracking are not affected.

The process of pseudonym management is shown in Figure 1. (1) The vehicle \( V \) gets an identity certification from CA. (2) \( V \) applies for pseudonym certificates. (3) PCA issues some pseudonym certificates to \( V \). (4) \( V \) communicates with other vehicles and RSU with the pseudonym certificates. (5) Once other vehicles find suspicious vehicles, they submit a tracking request to TAs. (6) TAs disclose the identity from the pseudonym.

The model consists of three protocols: a pseudonym issuance protocol, a pseudonymous authentication protocol, and a distributed tracking protocol. TAs’ public key \( (N, e) \) is generated during the initialization stage and used in the pseudonym issuance protocol. Pseudonym certificates are generated in the issuance protocol and used in the pseudonymous authentication protocol. Once suspicious messages appear in pseudonymous authentication, the distributed tracking protocol is activated.

### 3. Pseudonym Issuance Protocol

Chaum [16] first proposed the concept of a blind signature, which allows users to get a message signature without leaking any contents. The pseudonym certificate issuance protocol adopts the blind signature method.

1. \( V \) sends \( ID_V \parallel n \parallel (ID_V \parallel n)^{d_V} mod N_V \parallel Cert_V \) to PCA, where \( n \) is the number of pseudonyms.

2. PCA verifies \( (ID_V \parallel n)^{d_V} mod N_V \), if passed, and sends \( ID_{PCA} \parallel ID_V \parallel exp \parallel (ID_{PCA} \parallel ID_V \parallel exp)^{d_{PCA}} mod N_{PCA} \) to \( V \), where \( exp \) is the expiration date.
During the initialization stage, the prerequisite of implementing the protocol is that V has got TAs’ public key \((N, e)\) and PCA’s public key \((N_{\text{PCA}}, e_{\text{PCA}})\). Before applying for a pseudonym, the short-time public and private keys of the vehicle have been already generated. (1) V sends a request signed with \(d_t\) to PCA to prove its identity ID\(_V\). (2) PCA sends the signature secretly, not only to prove PCA’s identity but also to coproduce PCA’s pseudonym. Sending the signature secretly can prevent the signature from leaking. (3) V produces pseudonyms and blinds them. In (4), (5), and (6) PCA opens \(n\) commitments among \(2n\) commitments to verify. If passed, PCA signs blindly the remaining \(n\) commitments. (7) V removes the blind factors and gets the pseudonym certificates.

In Schaub et al.’s issuance protocol [14], CA signs V-tokens for a vehicle. Pseudonym provider (PP) checks the validity of V-tokens; if valid, PP issues a pseudonym certificate. Four rounds of interaction are required. If CA wants to cheat, it will not interact with a vehicle. And it will obtain a fake pseudonym certificate and impersonate a vehicle, so will PP.

In our issuance protocol, PCA issues directly a pseudonym certificate to a vehicle, and three rounds of interaction are required. A pseudonym is coproduced by V and PCA. PCA cannot provide \(r_i \parallel r_i^{d_t}\) to forge a pseudonym of V. V cannot provide \((ID_{\text{PCA}} \parallel ID_V \parallel \exp_{\text{PCA}}\) to forge the pseudonym of another vehicle \(V^*\). Even if V eavesdrops on the communication between \(V^*\) and PCA, V cannot decrypt \((ID_{\text{PCA}} \parallel ID_V \parallel \exp_{\text{PCA}}\) mod \(N_{\text{PCA}}\). So, it fails to forge the pseudonym. Furthermore, the cut-choose method is also adopted in our protocol, like in Schaub et al.’s protocol, and prevents content spoofing to a certain extent.

As a result, our issuance protocol maintains good property of vehicular privacy in the presence of an authority and provides security against authority forge attack. Moreover, the communication overhead is reduced from four rounds to three rounds.
4. Pseudonymous Authentication Protocol

A complete authentication message consists of six fields: messageID || payload || timestamp || signature || certificate || TTL. "MessageID" is the message number during the same pseudonym period. "Payload" contains collision data, location, direction, speed, and so on. "Timestamp" is the inclusion of certificates in messages. Concrete methods to reduce the communication overhead of secure messages by omitting the periodic omission of certificates, neighbor-based certificate omission, and congestion-based certificate omission were proposed in [9], [18], and [19], respectively. In these schemes, the optimal parameter was obtained by means of simulation. In contrast to the earlier proposals, we found the optimal parameter by means of probability analysis.

Define that \( \alpha \) is the number of messages and \( \lambda \) is the number of messages with pseudonym certificate during one pseudonym period. If at least one message with certificate is accepted by the receiver, other arrived messages with the same pseudonym can be authenticated. Define the message authentication probability \( P_{\text{auth}} \) as \( P_{\text{auth}} = 1 - (1 - P_{\text{accept}})^\lambda \), where \( P_{\text{accept}} \) is the packet reception rate. We used a packet reception rate model of broadcast channel in a good channel condition \( P(d) = -0.004d + 1/7 \sin(\pi/125d) + 1 \) [9], where \( d \) is the distance between the sender and the receiver.

Figure 2 shows the relationship among the message authentication probability \( P_{\text{auth}} \), the intervehicle distance \( d \), and the number of messages with certificate \( \lambda \). Assuming that \( \lambda \) is a constant, \( P_{\text{auth}} \) decreases with the increase of \( d \); assuming that \( d \) is a constant, \( P_{\text{auth}} \) increases with the increase of \( \lambda \). From the figure, it can be further observed that if \( \lambda \geq 5 \) and \( d \leq 130 \), then \( P_{\text{auth}} > 95\% \). That means we take \( \lambda = 5 \), which can meet the need of most vehicles for broadcast message authentication. Thus, \( \lambda = 5 \) is the optimal number of messages with the pseudonym certificate.

We define \( \text{len} \) as the average message length, and Figure 3 shows the relationship between \( \text{len} \) and \( \alpha \) under the condition of \( \lambda = 5 \). The parameter \( \text{len} \) decreases with the increase of \( \alpha \). It means that during a pseudonym period the more the messages are, the less communication overhead is.

5. Distributed Tracking Protocol

Based on the secret sharing scheme [20], TAs’ private key \( d \) is assigned to the \( k \) authorities, and any one subset of at least \( m \) of them can disclose the secret. Generally, there is a trusted center during the initialization stage of the secret sharing scheme. Once the center compromises, the privacy will be leaked. Boneh and Franklin [21] discussed the generation of RSA keys without a dealer, but the protocol required the help of a third party. Cocks [22] presented another protocol to generate shared RSA keys without the help of a third party. There exists a large number of modular exponentiation operations to generate the modulus, and thus the efficiency of the protocol is poor. Malkin et al. [23] extended two parties [21] to \( k \) parties.

Instead of time-consuming modular exponentiation, we use modular multiplication to generate \( N \), where \( N \) is
the modulus of RSA. And furthermore, we extend the \((k, k)\) threshold scheme to a more general form \((m, k)\), where \(m\) is the number of members and \(k\) is the threshold value. Based on the above ideas, the distributed tracking protocol is developed. It consists of distributed generation of modulus \(N\), distributed generation of private key and secret share, and collaborative tracking. The first two parts are completed collaboratively by all members during initialization, and the third part is implemented collaboratively by at least \(m\) members during the tracking stage.

5.1. Distributed Generation of Modulus \(N\). Each member TA\(_{i}\) \((1 \leq i \leq k)\) picks random primes \(p_{i}, q_{i}\) and computes modulus \(N = \left(\sum_{i=1}^{k} p_{i}\right)\left(\sum_{i=1}^{k} q_{i}\right)\) without revealing \(p_{i}, q_{i}\). Assuming that \(k\) is an odd, the steps are as follows:

1. TA\(_{i}\) picks two random primes \(p_{i}, q_{i}\) and a random \(r_{i,j} \in \mathbb{Z}_{p}\) (prime \(P > N\)). TA\(_{i}\) computes and sends \(r_{i,j}p_{i}\) and \(r_{i,j}q_{i}\) to TA\(_{j}\) \((1 \leq j \leq k, j \neq i)\).
2. TA\(_{i}\) computes \(r_{i,j}p_{j}q_{j}\) and \(r_{i,j}q_{i}p_{j}\) and sends \(r_{i,j}p_{j}q_{j} + r_{i,j}q_{i}p_{j}\) to TA\(_{j}\).
3. TA\(_{i}\) computes \(s_{i,j} = (1/r_{i,j})(r_{i,j}p_{j}q_{j} + r_{i,j}q_{i}p_{j}) = p_{j}q_{j} + p_{i}q_{i}\) \((j \neq i)\),

\[
N_{i} = \sum_{j=1}^{k} s_{i,j} + 2p_{i}q_{i} \tag{4}
\]

and broadcasts \(N_{i}\) in TAs.
4. All members compute \(\sum_{i=1}^{k} N_{i}\) and get \(N = \sum_{i=1}^{k} N_{i}/2\).
5. Any member in TAs picks an integer \(g \in \mathbb{Z}_{N}^{\ast}\) randomly and broadcasts \(g\) in TAs.
6. TA\(_{i}\) computes and broadcasts \(V_{1} = g^{N-p_{i}-q_{i}+1} \mod N\); all other members TA\(_{j}\) \((2 \leq i \leq k)\) compute and broadcast \(V_{i} = g^{p_{i}q_{j}} \mod N\); all members verify \(V_{1} = \prod_{i=1}^{k} V_{i} \mod N\).
7. If the verification fails, all members execute steps (1)–(6) again. Otherwise, success is returned.

5.2. Distributed Generation of Private Key and Secret Share. \(\phi(N)\) is Euler function of \(N\), denoted as \(\phi\). If \(N\) is the product of two primes,

\[
\phi = N - \sum_{i=1}^{k} p_{i} - \sum_{i=1}^{k} q_{i} + 1. \tag{5}
\]

1. TA\(_{i}\) computes \(\phi_{i} = N - p_{i} - q_{i} + 1\), and another member TA\(_{j}\) \((2 \leq i \leq k)\) computes \(\phi_{j} = -p_{i} - q_{i}\). Then, each member TA\(_{i}\) \((1 \leq i \leq k)\) broadcasts \(\phi_{i} \mod e\) in TAs.
2. TA\(_{j}\) collects \(\phi_{i} \mod e\), and computes \(\psi = \sum_{j=1}^{k} \phi_{j} \mod e = \phi \mod e\) and \(\zeta = \psi^{-1} \mod e\). TA\(_{j}\) obtains its own private key

\[
d_{j} = \left[ \frac{\zeta \phi_{j}}{e} \right]\tag{6}
\]

3. TA\(_{j}\) picks a random degree \(m\) \(-1\) polynomial \(c(x) \in Z_{p}^{\ast}[x]\), satisfying \(c(0) = d_{j}\). It computes \(s_{i,j} = c(ID_{j})\) and sends \(s_{i,j}\) to TA\(_{j}\) \((j \neq i)\) secretly.
4. TA\(_{j}\) collects \(s_{i,j}\), then computes the secret share

\[
s_{j} = \sum_{j=1}^{k} s_{i,j} \mod P. \tag{7}
\]

After implementing the protocol, each member obtains the private key \(d_{j}\) and secret share \(s_{j}\). The operation of computing \(\phi \mod e\) reveals \(\log_{e} e\) low bits of \(\phi\). In order to protect \(\phi\) from revealing more bits, we take a small \(e\).

5.3. Collaborative Tracking

1. The vehicle \(V^{*}\) reports the signed message with a certificate to a tracking authority such as TA\(_{1}\). TA\(_{1}\) checks whether the signed message and the certificate are valid.
2. If passed, TA\(_{1}\) extracts ID\(_{PV}\) from Cert\(_{PV}\) and sends ID\(_{PV}\) to other members. If \(m - 1\) members accept a tracking request, they constitute a tracking group. Assume that their identities are ID\(_{1}\), ID\(_{2}\), …, ID\(_{m}\).
3. Participants TA\(_{i}\) \((2 \leq i \leq m)\) send ID\(_{PV}^{\alpha_{i}}\) mod \(N\) to TA\(_{1}\), where \(\alpha_{i} = s_{i,i}(0)\) mod \(P\).
4. TA\(_{1}\) tries all possible \(u\) and \(x\) \((0 \leq u \leq k - 1, -m < x \leq 0)\) and computes

\[
ID_{PV}^{xP+u} \prod_{i=1}^{m} ID_{PV}^{\alpha_{i}} \mod N = r \mid r^{d_{j}} \mod N_{V} \mid (ID_{PCA} \mid ID_{V} \mid \exp)^{d_{PCA}} \mod N_{PCA}. \tag{8}
\]

It extracts \((ID_{PCA} \mid ID_{V} \mid \exp)^{d_{PCA}} \mod N_{PCA}\) and further gets ID\(_{PCA}\) \| ID\(_{V}\) \| \exp with \(e_{PCA}\). TA\(_{1}\) gets ID\(_{V}\) according to the actual meaning of the strings.

Then TA\(_{1}\) submits ID\(_{V}\) to PCA, and PCA puts it into the blacklist. PCA will reject the request of the vehicle in the blacklist for pseudonym certificates. So, the pseudonym tracking protocol combined with the pseudonym issuance protocol can realize the revocation of malicious vehicles.

In Lin et al’s protocol [7], a centralized method for tracking is adopted. A trace manager (TM) computes a vehicle’s private key from a signed message in order to disclose the vehicle’s identity. Once TM is compromised, a large amount of privacy information is leaked.

In Schaub et al.’s protocol [14], the secret sharing method for tracking is adopted to prevent misuse and abuse of a system. The method is distributed, but it generally requires a trusted center to distribute secret share in the initialization.
phase. Therefore, the trusted center will be a secure bottleneck.

In our tracking protocol, all the processes in the secret sharing method adopt a fully distributed structure, such as generation of private key and secret share, generation of modulus $N$ and collaborative tracking. As a result, our tracking protocol avoids a single point of failure.

6. Analysis

6.1. Security Analysis

Proposition 1. Neither issuing authorities nor other vehicles can determine the relationship between a pseudonym and an identity in the protocol family, so the scheme achieves anonymity.

Proof. (1) During the issuance stage, PCA gets $c_i = (x_i \cdot t_{PCA}) \cdot \text{SHA}(b_i) \mod N_{PCA}$. V picks $x_i$ randomly, so PCA cannot get $b_i$ and ID$_{PV}$. Though PCA knows ID$_{PV}$, it cannot establish the relationship between ID$_V$ and ID$_{PV}$.

(2) Other vehicles get the signed messages and extract ID$_{PV} = (r_i \parallel r_i^{d_i}) \mod N_V \parallel (ID_{PCA} \parallel ID_V \parallel \text{exp}_{d_{PCA}}) \mod N_{PCA}$. They do not know TAs’ private key $d$ and thus cannot obtain $V$’s identity ID$_V$.

Proposition 2. The $m$ authorities in TAs can disclose the identity ID$_{PV}$ from a pseudonym ID$_{PV}$, so the scheme achieves traceability.

Proof. Let $\psi = \phi \mod e = \sum_{i=1}^{k} \phi_i \mod e$, $\xi = -\psi^{-1} \mod e$, and then $\xi \phi + 1 = -\phi^{-1} \phi + 1 = 0 \mod e$, indicating $e \mid (\xi \phi + 1)$.

Since $d \cdot e = 1 \mod \phi$, this gives $d = (\xi \phi + 1) \mod e = (\sum_{i=1}^{k} \phi_i + 1) \mod e$. Let $d_i = [\xi \phi_i / e]$; then

\[ d = \sum_{i=1}^{k} d_i + u \quad (0 \leq u \leq k - 1). \] (9)

Construct a degree $m - 1$ polynomial $c(x) = \sum_{j=1}^{k} c_j(x) \mod P$, obviously satisfying $c(0) = \sum_{j=1}^{k} c_j(0) = \sum_{j=1}^{k} d_j$ and $c(ID_V) = \sum_{j=1}^{k} c_j(ID_V) = \sum_{j=1}^{k} s_j = s_i$.

According to the Lagrange interpolation formula $\sum_{j=1}^{m} d_j = \sum_{j=1}^{m} s_j l_j(0) \mod P$, let $\alpha_i = s_j l_j(0) \mod P$, so

\[ \sum_{j=1}^{k} d_j = \sum_{i=1}^{m} \alpha_i + xP. \] (10)

Since $0 \leq \sum_{j=1}^{k} d_j < \phi$, $0 \leq \alpha_i < P$, $0 \leq \sum_{i=1}^{m} \alpha_i < mP$, therefore $-m < x \leq 0$.

Taking the formula (10) into the formula (9), we can obtain the following formula:

\[ d = \sum_{i=1}^{m} \alpha_i + xP + u \quad (0 \leq u \leq k - 1, \quad -m < x \leq 0). \] (11)

Consider the issuance protocol and obtain

\[ r \parallel r^{d_i} \mod N_V \parallel (ID_{PCA} \parallel ID_V \parallel \text{exp})^{d_{PCA}} \mod N_{PCA} \]

\[ = ID_{PV}^d \cdot ID_{PV}^{\sum_{i=1}^{m} \alpha_i + xP + u} \]

\[ = ID_{PV}^{xP + u} \cdot \prod_{i=1}^{m} ID_{PV}^{\alpha_i} \mod N. \] (12)

Compute $((ID_{PCA} \parallel ID_V \parallel \text{exp})^{d_{PCA}})^{d_{PCA}} \mod N_{PCA}$ with $e_{PCA}$ and obtain $V$’s identity ID$_V$.

Proposition 3. Regardless of the PCA, the vehicles and the outside attacker, forging the pseudonym certificate is as difficult as solving a large integer factorization problem.

Proof. A pseudonym ID$_{PV}$ is coproduced by $V$ and PCA, because $r_i \parallel r_i^{d_i} \mod N_V$ is provided by $V$ and $(ID_{PCA} \parallel ID_V \parallel \text{exp})^{d_{PCA}} \mod N_{PCA}$ is provided by PCA.

(1) PCA cannot provide $r_i \parallel r_i^{d_i} \mod N_V$ to forge a pseudonym.

(2) $V$ cannot provide $(ID_{PCA} \parallel ID_V \parallel \text{exp})^{d_{PCA}} \mod N_{PCA}$ to forge the pseudonym of $V^*$.

(3) An external attacker without $V$’s and PCAs’ private keys cannot pass the authentication, because the issuance protocol is with two-way authentication. Therefore, the attacker neither obtains the blind signature nor personates PCA to sign the pseudonym certificate.

In short, forging an RSA signature or cracking an RSA cipher is as difficult as factorizing a large integer, so the scheme achieves unforgeability.

Proposition 4. The scheme is robust.

Proof. (1) The separation of pseudonym issuance authorities and tracking authorities, to some extent, reduces the risk.

(2) Some PCAs are deployed in the model. Once a PCA fails, other PCAs can still provide pseudonym issuance service.

(3) In the pseudonymous authentication protocol, the optimal number of messages with the pseudonym certificates is suggested. It ensures the message authentication probability $P_{\text{auth}} > 95\%$. That means when a message arrives, a vehicle can verify the signature with high probability. Therefore, the protocol not only reduces the communication overhead but also ensures robustness.

(4) During the TAs initialization stage, the generation of modulus $N$ and the generation of the private key and the secret share are distributed fully. So, the scheme does not require a trusted center, and it avoids any single point of failure.

(5) During the TAs operation stage, as long as the number of compromised members is not more than $m - 1$, privacy cannot be leaked.

We further compared our scheme with similar works that are intended to ensure conditional privacy preserving communication [7,14]. The results of comparisons of security features among our scheme, Lin et al.’s scheme [7], and
Table 1: Security features comparisons.

|                         | Anonymity | Traceability | Authentication | Unforgeability (especially against authority attacks) | Robustness (especially for tracking) |
|-------------------------|-----------|--------------|----------------|------------------------------------------------------|--------------------------------------|
| Lin et al.’s scheme [7] | Yes       | Yes          | Yes            | No                                                   | Centralized                         |
| Schaub et al.’s scheme [14] | Yes     | Yes          | Yes            | No                                                   | Distributed                         |
| Our scheme              | Yes       | Yes          | Yes            | Yes                                                  | Fully distributed                   |

Table 2: Computation cost comparisons.

|                         | Issuance                  | Signature and verification | Tracking                  |
|-------------------------|---------------------------|----------------------------|---------------------------|
| Lin et al.’s scheme [7] | $T_{exp}$                 | $12T_{exp} + T_{P} + 12T_{exp} + 2T_{P}$ | $2T_{exp}$               |
| Schaub et al.’s scheme [14] | $7T_{e} + 4T_{d} + (T_{e} + T_{d})/n$ | $T_{e} + T_{d}$ | $T_{d}$ |
| Our scheme              | $6T_{e} + 3T_{d} + 3(T_{e} + T_{d})/n$ | $T_{e} + T_{d}$ | $(k + 1)T_{d}$ |

Computation time (ms)

- Lin et al.’s [7] 0.6
- Schaub et al.’s [14] 17.4 + 4.2/n
- Ours 13.2 + 12.6/n

Table 3: Communication cost comparisons.

|                         | Issuance (rounds) | Signed messages (B) | Tracking (B) |
|-------------------------|-------------------|---------------------|--------------|
| Lin et al.’s scheme [7] | 1                 | 289                 | 309          |
| Schaub et al.’s scheme [14] | 4            | 1031               | 512 + 519/m  |
| Our scheme              | 3                 | 235 + 796 $\lambda/\alpha$ | 512 + 519/m |

Schaub et al.’s scheme [14] are shown in Table 1. All the three schemes provide anonymity, traceability, and authentication. Lin et al.’s scheme is based on a group signature method, in which a member manager (MM) generates member private keys and sends them privately; MM knows all private keys, and it can forge a valid group signature on an arbitrary message. Schaub et al.’s scheme adopts a blind signature method to issue certificates, and thus CA or PP does not know the relationship of an identity and a pseudonym; unfortunately, CA or PP can forge a pseudonym certificate for itself. Therefore, Lin et al. and Schaub et al.’s schemes are not secure against authority forge attacks. In our scheme, a pseudonym is coproduced by a manager and a vehicle; neither PCA nor V is capable of providing complete data to forge a pseudonym; our scheme is unforgeable, especially against authority forge attacks.

As mentioned in Section 5, the tracking methods for Lin et al., Schaub et al. and ours are centralized, distributed, and fully distributed, respectively. Our scheme has better robustness.

6.2. Performance Analysis

6.2.1. Computation Overhead. For convenience to evaluate the computation cost of the protocol, we ignored the computation cost of some operations such as a hash function and a multiplication operation, since they are quite light in terms of load. We focused on some time-consuming operations defined in the following notations.

- $T_P$: The time of executing a bilinear map operation.
- $T_{exp}$: The time of executing a modular exponentiation operation in the cyclic group.
- $T_e$: The time of executing RSA encryption or RSA verification.
- $T_d$: The time of executing RSA decryption or RSA signature.

In order to provide the precise comparisons of computation cost, we use the experiment data in [24–26] to evaluate them. The experiment environment is operated on a standard PC, whose processor is Pentium IV with the maximum clock speed of 3 GHz. The pairing system is considered the Tate pairing system. The order of a non-supersingular curve over a finite field $E(\mathbb{F}_p)$ is 160 bits, which is as difficult to break as 1024-bit RSA. In this experiment environment, it requires 4.5 ms to perform a bilinear map operation and 0.6 ms to perform a modular exponentiation operation [25, 26]. It requires 0.2 ms to perform RSA encryption/verification and 4 ms to perform RSA decryption/signature [24].

The results of comparisons of computation cost are shown in Table 2, where $n$ is the number of pseudonym certificates obtained at one time and $k$ is the number of tracking authorities. Some common parameters and secret keys are generated in the system initialization, and for convenience we did not evaluate the computation cost of the initialization in all the three schemes. In Schaub et al.’s scheme and ours, the average computation costs for issuance and tracking are considered.

Compared with Lin et al.’s scheme, ours and Schaub et al.’s scheme require less computation for signature and verification and more computation for issuance and track. Compared with Schaub et al.’s, our scheme requires less computation for issuance if $n > 2$ and more computation for tracking.

6.2.2. Communication Overhead. In Table 3, $\alpha$ is the number of signed messages and $\lambda$ is the number of signed messages with pseudonym certificate during one pseudonym period in
the authentication protocol; \( m \) is the threshold value in the distributed tracking protocol. The communication cost of Lin et al.’s scheme is the lowest, but their scheme suffered from the private key revealing attacks, in which MM knows the private key of each member. Schaub et al.’s scheme and ours rely on the blind signature method and achieve vehicular privacy protection in the presence of the authority. Compared with Schaub et al.’s scheme, our scheme is efficient in terms of the communication overhead.

6.2.3. Storage Overhead. In Schaub et al.’s scheme and ours, the storage cost of the vehicle is high because some pseudonym certificates need to be stored; the storage cost of the manager for tracking is very little because an identity can be obtained directly from the pseudonym certificate. On the contrary, the storage cost of the manager in Lin et al.’s scheme is high because the record set \( (A_z, ID_z) \) needs to be stored.

7. Conclusions

In this paper, a secure and efficient pseudonym management scheme for vehicular ad hoc networks is proposed. The scheme not only maintains the property of conditional privacy preservation but also provides the advantages in security against authority forge attacks and better robustness. In the scheme, a pseudonym is coproduced by \( V \) and PCA to avoid the deception of either party. A blind signature method is used to achieve the separation of issuance and tracking. Based on the improved share generation scheme of the RSA keys, the distributed tracking protocol is proposed to avoid a single point of failure. By searching for the optimal number of messages with a pseudonym certificate, the efficient pseudonym authentication mechanism is given to reduce communication overhead. By uniting the pseudonym issuance protocol and the tracking protocol, malicious vehicles are revoked easily. Moreover, compared with Schaub et al’s scheme, the communication cost and computation cost in our scheme are lower. As a result, our proposed scheme is suitable for anonymous communication with tracking requirements in VANETs, since it provides security, robustness, and efficiency.

For future research, we will discuss interdependencies of various factors, establish systematic evaluation mechanism of the overall performance, and further enhance the performance.

Acknowledgments

The authors acknowledge the financial support of the National Natural Science Foundation of China (no. 60873195), the National High Technology Research and Development Program (“863” Program) of China (no. 2011AA060406), and the Natural Science Foundation of Anhui Province (no. 090412051). The authors are grateful for the anonymous referee for the careful checking and helpful comments that improved this paper.

References

[1] J. Blum, A. Eskandarian, and L. Hoffman, “Challenges of intervehicle adhoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 347–351, 2004.

[2] J. P. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” *IEEE Security and Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[3] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets-IV)*, pp. 1–6, College Park, Md, USA, November 2005.

[4] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[5] M. Raya and J. P. Hubaux, “The security of vehicular ad hoc networks,” in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN ’05)*, pp. 11–21, Alexandria, Va, USA, November 2005.

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

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

[8] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET ’07)*, pp. 19–28, Montreal, Canada, September 2007.

[9] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, “On the performance of secure vehicular communication systems,” *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 898–912, 2011.

[10] R. Lu, X. Lin, H. Zhu et al., “ECPP: efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proceedings of the IEEE 27th Conference on Computer Communications (INFOCOM ’08)*, pp. 1229–1237, Phoenix, Ariz, USA, 2008.

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

[12] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETs,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[13] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in *Advances in Crypto ’04*, vol. 3152 of Lecture Notes in Computer Science (LNCS), pp. 41–55, 2004.

[14] E. Schaub, F. Kargl, Z. Ma, and M. Weber, “V-tokens for conditional pseudonymity in VANETs,” in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’10)*, pp. 1–6, Sydney, Australia, April 2010.

[15] P. Papadimitratos, L. Buttyan, T. Holczer et al., “Secure vehicular communication systems: design and architecture,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[16] D. Chaum, “Blind signatures for untraceable payments,” in *Advances in Crypto ’82*, pp. 199–203, Plenum, 1982.

[17] R. Housley, W. Ford, W. Polk, and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” 2011, http://www.ietf.org/rfc/rfc2459.txt.

[18] E. Schoch and F. Kargl, “On the efficiency of secure beaconing in VANETs,” in *Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec ’10)*, pp. 111–116, New York, NY, USA, March 2010.
[19] M. Feiri, J. Petit, and F. Kargl, “Congestion-based certificate omission in VANETs,” in Proceedings of the 9th ACM international workshop on Vehicular Inter-Networking, Systems, and Applications, pp. 135–138, 2012.

[20] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[21] D. Boneh and M. Franklin, “Efficient generation of shared rsa keys,” in Proceedings of Crypto ’97, pp. 425–439, 1997.

[22] C. Cocks, “Split knowledge generation of rsa parameters,” in Proceedings of the 6th IMA International Conference on Cryptography and Coding, pp. 89–95, 1997.

[23] M. Malkin, T. Wu, and D. Boneh, “Experimenting with shared generation of RSA keys,” in Proceedings of the Internet Society’s 1999 Symposium on Network and Distributed System Security, pp. 43–56, San Diego, Calif, USA, 1999.

[24] OpenSSL, “The Open Source Toolkit for SSL/TLS,” 2012, http://openssl.org/.

[25] M. Scott, “Efficient implementation of cryptographic pairings,” 2007, ftp://ftp.disi.unige.it/pub/person/MoraF/CRYPTO/PARING/mscott-samos07.pdf.

[26] L. Chen, S. L. Ng, and G. Wang, “Threshold anonymous announcement in VANETs,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, 2011.