Information Sciences 476 (2019) 211–221

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Privacy-preserving authentication scheme with full aggregation in VANET

Hong Zhong, Shunshun Han, Jie Cui*, Jing Zhang, Yan Xu

School of Computer Science and Technology, Anhui University, Anhui Province, China

ARTICLE INFO

Article history:
Received 1 October 2017
Revised 30 May 2018
Accepted 14 October 2018
Available online 15 October 2018

Keywords:
Certificateless aggregate signature
Privacy-preserving
Full aggregation
VANET

ABSTRACT

Vehicular Ad-hoc Network (VANET) is the fundamental of intelligent transportation systems. Security and privacy are the important issues needed to be addressed. Existing schemes for privacy-preserving vehicular communications face many challenges, such as strong assumption on ideal tamper-proof device (TPD) and reducing the cost of computation and communication. In order to overcome the challenge, we propose a privacy-preserving authentication scheme with full aggregation in VANET, using certificateless aggregate signature to achieve secure vehicle-to-infrastructure (V2I) communications. The technique of aggregate signature can achieve message authentication and greatly save the bandwidth and computation resources. In addition, we use pseudonym to realize conditional privacy preserving and a trace authority (TRA) is responsible for generating pseudonym and tracking the real identity during the communication if it is necessary. When a vehicle enters an area under a new road side unit (RSU)'s coverage, we precalculate some data for once, thus the computation cost in sign phase can be reduced. The length of aggregated signature is constant which reduces the communication and storage overhead.

1. Introduction

Transportation safety and efficiency have drawn a lot of attention from the society. It is important to build an intelligent transportation system. Recently, the concept of vehicular ad hoc networks (VANET) has been proposed by some researchers to enhance road safety and transportation efficiency. In VANET, vehicles communicate with each other in a wireless way, and they broadcast some traffic-related information periodically. An application server can collect the traffic-related information and make some analysis, and traffic control center can get feedback from application server and make optimal strategy to manage the traffic.

A typical structure of VANET is composed of Trusted Authority (TA), Road Side Unit (RSU) and vehicles equipped with On-Board Unit (OBU). According to the provision of Dedicated Short Range Communication (DSRC) protocol, each vehicle broadcasts traffic-related news, e.g.congestion situation, weather conditions, accident conditions, vehicle's speed and location etc., every 100-300 milliseconds. RSU can receive the traffic-related messages and verify them to ensure the integrity and validity. Besides, RSU is also able to send valid traffic-related messages to traffic control center. The traffic control center can make some reasonable strategies to enhance traffic efficiency based on the received messages.

* Corresponding author.
E-mail address: cuijie@mail.ustc.edu.cn (J. Cui).

https://doi.org/10.1016/j.ins.2018.10.021
0020-0255/

Security and privacy are the key issues in VANET [9]. For example, the message must be checked for integrity and authenticated before it is used, otherwise the malicious vehicle may modify the messages and even disguise itself as the legal vehicle to send the wrong messages. The fake messages may cause a car accident or mislead the traffic control center to make unreasonable strategy. For the privacy issue, vehicles may do not want their personal information, such as the real identity, to be known by others. On the contrary, traceability is also required under some circumstances. For example, a vehicle that sends fake messages should not be escaped from using pseudonym. That is to say, conditional privacy-preserving is needed in VANET.

Data compression is another challenge in VANET. Application server receives messages from RSUs. With the increase of traffic density under the RSU's coverage, the number of messages will greatly increase as well. A message must be signed before been sent, thus a lot of signatures will be sent which causes huge burden for communication and storage. By using the technique of aggregate signature, we can aggregate n signatures into one signature which can effectively solve the challenge.

The rest of our paper is organized as follows. Section 2 reviews the related works in VANET. Section 3 describes the background knowledge we have used in the paper. Section 4 describes the proposed scheme in detail. Section 5 gives the security proof and analysis of the proposed scheme. Section 6 evaluates the performance of our schemes. Finally, we make a conclusion and describe the future work in section 7.

2. Related work

To satisfy the security requirement in VANET, a great many schemes were proposed by scholars. Raya and Hubaux [16] proposed a privacy preserving authentication scheme based on traditional public key infrastructure (PKI). A lot of key pairs and corresponding anonymous certificates need to be preloaded in OBU. During the communication, a public/secret-key pair is chosen by the vehicle randomly every time. By using them vehicles can achieve authentication and integrity. However, the authority needs to store all the vehicle's certificates and the vehicle has to preload a lot of public/private key pairs and related digital certificates which causes huge storage burden. Besides, when the authority wants to track the vehicle's real identity, it has to execute an exhaustive search in a huge database. Lu et al. [14] proposed an efficient conditional privacy preservation protocol for secure vehicular communications. In this scheme, RSU is responsible for generating the short time public key certificates and store them in its local database. For tracking the real identity, RSU has to maintain a huge certificate list, which cause big burden for certificate management.

To alleviate the certificate manage problem, some identity-based schemes were proposed. In the identity-based cryptography [17], vehicle's public key can easily be calculated by using its identity. This method alleviates the work of certificate management, however it suffers a key escrow problem. Zhang et al. [22] proposed an identity-based batch authentication scheme which is called IBV. They use the ID-based signature to reduce the cost of transmission and alleviate the cost for verifying public key certificates. The pseudonym of vehicle can be generated offline, because the master secret is preloaded in tamper-proof device (TPD). However, by launching the side channel attack, an adversary may obtain the master system secret. Once the adversary gets the secret, he can masquerade a legal vehicle and send any message he wants, which is a great risk for the system. Lu et al. [13] proposed a lightweight privacy-preserving scheme, TA uses hash chain technique to generate pseudo identity which leads to the reduction of computational overhead while achieving conditional privacy. A lot of identity-based schemes were proposed by scholars [5,10,19], but most of these schemes have a strong assumption that the system master secret must be preloaded in the TPD and no attacker can obtain the master secret from it which is too ideal to deploy.

Certificateless public key cryptography (CL-PKC) scheme can avoid the key escrow problem, since a trusted third party is introduced which is called private key generator (PKG). PKG is in charge of generating the partial key for the user, and the user combines his chosen vehicle secret key with the partial key to construct the full private key. This method alleviates the work of certificate management. And a lot of CL-PKC based schemes were proposed [1,21,27]. The first CL-PKC based scheme was proposed by Al-Riyami and Paterson [1]. Yum and Lee [21] introduced a general construction for CL-PKC based schemes. Hu et al. [8] found out that the construction of Yum and Lee scheme [21] is not secure and proposed a new one. Zhang et al. [27] introduced an improved security model and proposed a scheme with better efficiency.

Aggregate signature can effectively reduce the computation cost and communication cost, which is useful in resource constrained scenario. Certificateless cryptography solves the key escrow problem, so it is natural to introduce the definition of certificateless aggregate signature (CLAS). Various efficient and secure schemes based on it were proposed by scholars. However, most of schemes [2,26] need a large number of costly pairing operation during the verification procedure, that is to say the pairing operations grows linearly as the number of signatures increases. Xiong et al. [20] introduced an efficient provably secure CLAS scheme. Their verification only needs a constant number of pairing operations. However, He et al. [4] pointed out that Xiong et al.'s scheme is insecure under forgery attack which means an adversary can sign any message and generate a legal signature. Liu et al. [11] proposed a CLAS scheme used for roaming authentication in wireless network. The sign phase was divided into online part and offline part, and the user can make a pre-calculation when he is offline, so it can reduce the cost when he is online.

We propose an privacy preserving scheme based on certificateless aggregate signature for secure V2I communications, and our scheme can achieve full aggregation. We use the RSU as the aggregator to aggregate the signatures signed by the vehicle under its coverage. The vehicles under the same RSU's coverage share a same state information which is the identity

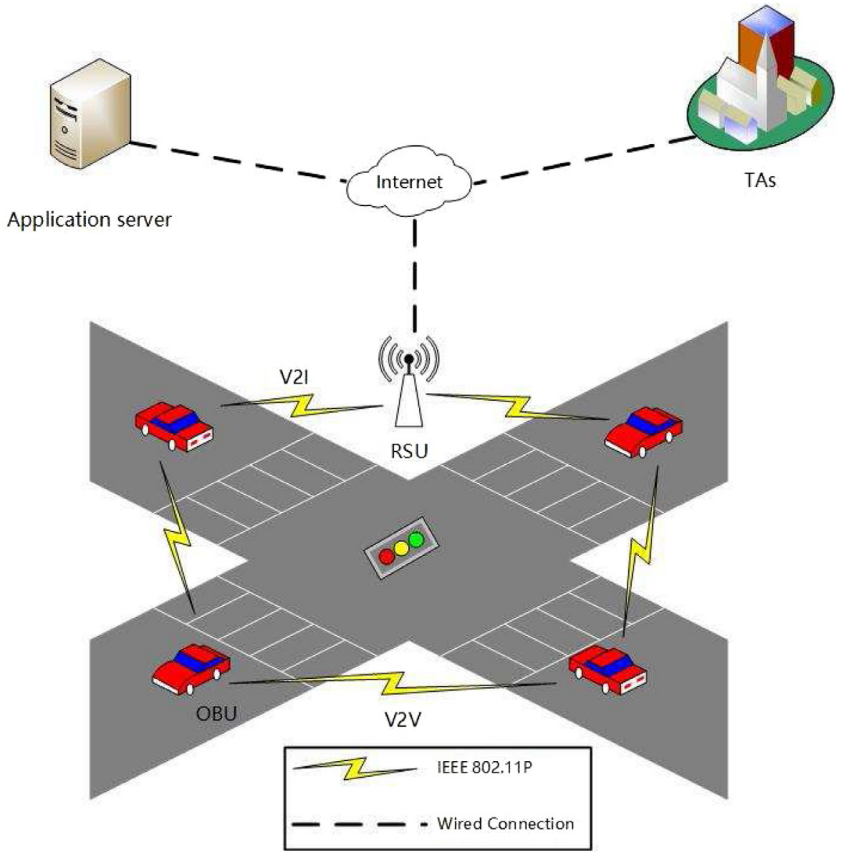

Fig. 1. System architecture.

of the RSU and it is used in the sign algorithm. So the signatures can be fully aggregated which greatly reduces the cost of communication. A legal authority is responsible for generating pseudonyms for vehicles, and the pseudonyms can be updated when the network is available, so our scheme is free of depending on ideal TPD. Before generating a message the vehicle can make a pre-calculation and store it for using in the sign procedure. The method reduces the computation overhead during the sign phase. And the security proof shows that the scheme is secure under the type-I and type-II attack.

3. Background

In this section, we describe the system model, security requirements and some mathematical knowledge.

3.1. System model

VANETs are usually two-layer network which consist of upper layer and lower layer [22], as shown in Fig. 1. The lower layer is composed of RSUs and vehicles equipped with an OBU. They communicate through DSRC protocol. Each vehicle has a real identity, a number of pseudo identities and corresponding public/private key pairs, and each message needs to be signed before they are sent. RSUs that receive the traffic-related messages should check the validity and integrity of signatures by verifying the corresponding signatures. The upper layer consists of TAs and application server (such as a traffic control center). RSUs can communicate with TAs and application server through secure wired channel. Application server can make deep analysis after collecting the traffic-related messages.

Fig. 1 illustrates the system architecture of the proposed scheme. There are four entities in our scheme [6]: TAs (private key generator (PKG) and trace authority (TRA)), roads ide units (RSUs), application server and onboard units (OBUs) installed in vehicles. TRA is responsible for generating pseudonyms for vehicles and can track the real identity from the pseudonyms the vehicle used. PKG is in charge of assigning partial private key for vehicles. For the environment of actual implementation, PKG and TRA can be built together or viewed as one [3,12]. OBU periodically broadcasts traffic-related message. RSU can verify the message sent by OBU, then send the valid message and the aggregated signature to application server. Application server will collect the traffic-related message sent by RSUs and make further analysis about the traffic situation. And we make the following assumption:

1. TRA and PKG are always trusted. And they do not collude and can not be comprised, which is often assumed in VANET schemes [18]. We reasonably assume that they are separated.
2. RSU are semi-trusted, which means that it is honest but curious about the vehicle's privacy. Since they are implemented by the roadside and can be easily comprised.
3. OUB are not trusted, and the message sent by OBU has to be authenticated.

3.2. Security requirements

Consider the privacy and security issue, the proposed scheme needs to satisfy the security requirements of identity privacy-preserving, message authentication,traceability, unlinkability and replay attack resistance. The detailed description of these requirements are as follows:

1. *Message authentication:* RSUs need to verify the signed messages are sent by legal vehicles without being forged or modified by malicious vehicle.
2. *Identity privacy-preserving:* The real identity of vehicles should keep anonymous during the communication. No any other third party except TRA can track the real identity from pseudonyms.
3. *Traceability:* Under some circumstances, for example, a wrong message causes car accident or a dispute happens. TRA is able to retrieve the real identity of vehicles.
4. *Unlinkability:* A malicious vehicle or RSU cannot distinguish an anonymous entity from its message signatures.
5. *Replay attack resistance:* An adversary is not able to use the received signed message and try to send it when it is invalid.

3.3. Bilinear maps and hard problems

The proposed scheme is based on bilinear maps, and we will introduce the concept of bilinear map in detail. Let G_1 denote an additive cyclic group with prime order q and G_2 be a multiplicative cyclic group with the same order . Let P denote the generator of G_1. Let e be a bilinear map such that $e : G_1 \times G_1 \rightarrow G_2$ and satisfy the following properties:

1. *Bilinear:* Given $P, Q, R \in G_1; a, b \in Z_q^*$, we have: $e(P, Q + R) = e(P, Q)e(P, R)$. Specially, for any $e(P, Q + R) = e(P, Q)e(P, R)$, we have:$e(aP, bQ) = e(P, bQ)^a = e(aP, Q)^b = e(P, Q)^{ab} = e(abP, Q) = e(P, abQ)$.
2. *Non-degenerate:* There exists $P, Q \in G_1$, such that $e(P, Q) \neq 1_{G_2}$, where 1_{G_2} is the identity element of G_2.
3. *Computable:* There exists efficient algorithm which can calculate $e(P, Q)$.
4. *Symmetric:* For all $P, Q, \in G_1, e(Q, P) = e(P, Q)$.

The security of proposed scheme is based on Computational Diffie-Hellman (CDH) problem. We will introduce the definition of CDH problem.

Definition 1. Given $P, aP, bP \in G_1$ as described above for unknown $a, b \in Z_q^*$, the goal of CDH problem is to find abP.

The CDH problem is $(t - \varepsilon)$ hard, if there exists no probabilistic polynomial algorithm $\mathcal{A}$ who can solve CDH problem in time at most t with probability ε as: Advantage$_{\mathcal{A}} = \Pr[xyP \leftarrow \mathcal{A}(P, aP, bP) : a, b \in Z_q^*] \geq \varepsilon$.

4. The proposed CLAS scheme

In this section, we will introduce our CLAS scheme. First, we will make a high level description, and then we will introduce our scheme in detail.

4.1. High level description

At a high level, our scheme can be divided into seven algorithms: system setup, pseudonym generation, partial key generation, vehicle key generation, sign, verify, aggregate and aggregate verify. We will firstly make a brief introduction of the seven algorithms. The notations used in our scheme are listed in Table 1.

1. **System setup**: On input a security parameter λ., TAs generate the master secret/public key pair respectively and publish the public system parameters.
2. **Pseudonym generation**: On input a vehicle's real identity RID_i which uniquely identifies the vehicle(such as the license plate number), TRA generates the pseudo identity for the vehicle.
3. **Partial key generation**: On input a vehicles pseudo identity PID_i, KGC generates the partial private key psk_i by using its master secret key.
4. **Vehicle key generation**: A vehicle choose a pseudo identity PID_i as input, and randomly selects a number then outputs the secret/public key pair(vsk_i, vpk_i).

Table 1
Notation.

Notations	Descriptions
G_1	A cyclic additive group.
G_2	A cyclic multiplicative group.
P	Generator of G_1.
e	A bilinear map e: $G_1 \times G_1 \rightarrow G_2$.
V_i	The ith vehicle.
R_j	The jth RSU.
s, P_{pub}	Private/public key of PKG.
α, T_{pub}	Private/public key of TRA.
PKG	A private key generator.
TRA	A trace authority.
RID_i	A real identity of a vheicle.
ID_{Rj}	An identity of a RSU.
vpk_i, vsk_i	Public/secret key of a vehicle.
psk_i	A partial private key of V_i.
PID_i	Pseudo identity of V_i.
VP_i	Valid period of PID_iP.

5. **Sign**: A vehicle uses the private signing key(psk_i, vsk_i) to sign a message $m_i \in \{0, 1\}^*$ and outputs a certificateless signature σ_i.
6. **Verify**: On input a certificateless signature σ_i on message m_i, pseudo identity PID_i and corresponding public key vpk_i, RSU outputs the signature is valid or not.
7. **Aggregate**: After receiving a set of n message-signature pairs, RSU can aggregate n signatures into a single one by calculating $\sigma = \sum_{i=1}^{n} \sigma_i$.
8. **Aggregate verify**: On input a certificateless aggregate signature on n messages, n pseudo identities and corresponding public keys, application server outputs whether the certificateless signature is valid or not.

4.2. Our construction

- **System setup**

On input a security parameter λ, the TAs generate two groups G_1, G_2 with the same prime order q, where G_1 is a cyclic additive group and G_2 is cyclic multiplicative group. P is a generator of G_1, and there exists a bilinear map e: $G_1 \times G_1 \rightarrow G_2$. PKG chooses a random number $s \in Z_q^*$ and calculates $P_{pub} = sP$, where s is used for partial private key generation and is only known to PKG. TRA chooses a random number $\alpha \in Z_q^*$ and calculates $T_{pub} = \alpha P$, where α is used for pseudo identity generation and is only known to PKG. TAs choose four cryptographic hash functions:$H_0 : \{0, 1\}^* \rightarrow G_1, H_1 : \{0, 1\}^* \rightarrow G_1, H_2 : \{0, 1\}^* \rightarrow Z_q^*$, and H_3: $\{0, 1\}^* \rightarrow G_1$. Then they publish $< q, G_1, G_2, e, P, P_{pub}, T_{pub}, H_1, H_2, H_3, H_4 >$ as the public system parameters.

- **Pseudonym generation**

Before joining the VANET, the vehicle should obtain the pseudonyms generated by TRA. To achieve anonymous, the real identity which uniquely identifies the vehicle is not allowed to use during the communication. A vehicle V_i chooses a random number $k_i \in Z_q^*$ and calculates $PID_{i,1} = k_iP$, then the vehicle sends (RID_i, $PID_{i,1}$) to TRA in a secure way. After receiving (RID_i, $PID_{i,1}$), TRA first checks whether the RID_i exists in its local database, and then calculates $PID_{i,2} = RID_i \oplus H_0(\alpha PID_{i,1}, VP_i)$ where VP_i is the valid period of PID_i. Then the $PID_i = (PID_{i,1}, PID_{i,2}, VP_i)$ is transmitted to PKG via a secure channel.

- **Partial key generation**

Given a pseudo identity PID_i, PKG calculates $Q_i = H_3(PID_i)$, $psk_i = sQ_i$ and sets psk_i as a partial private key. Then PKG transmits (PID_i, psk_i) to the vehicle.

Actually, the partial private key is a signature on PID_i for the PKG's key pair(P_{pub}, α). The vehicle can verify the correctness by checking whether $e(psk_i, P) = e(Q_i, P_{pub})$ equals or not. If it holds, store the pseudonym and corresponding partial private key in the OBU.

We use the preloading method [16] in the scheme, and in the pseudonym generation and partial-key generation phase, a number of short period pseudonyms and corresponding partial private keys are stored in OBU. The pseudonyms and corresponding partial private keys will be updated at a time when the network is free and available after proper authentication between vehicle and TAs through a secure channel.

- **Vehicle key generation**

The vehicle V_i chooses a random number $x_i \in Z_q^*$ as the vehicle secret key vsk_i and calculates the vehicle public key $vpk_i = x_iP$.

- **Sign**

Messages sent by vehicle have to be signed to ensure authentication and integrity. In our scheme, we divide the sign phase into two steps. In the first step,when the vehicle enters an area under a new RSU's coverage, the vehicle needs to make a pre-calculation for once and store the result in TPD. In the second step, when the vehicle needs to sign a message, it uses the result calculated in the first step to generate a signature. The specific description of the sign algorithm is as follows:

1. When a vehicle V_i enters a new RSU's area, it first calculates $H_j = H_1(ID_{Rj}), S_i = psk_i + vsk_i H_j$ and stores it in TPD. Note that, H_j and S_i only need to be calculated once if vehicle V_i is under the R_j's coverage. When the vehicle leaves the current area and gets into a new area, they need to be recalculated.
2. When a vehicle V_i needs to sign a message m_i, it randomly picks a pseudo identity PID_i and chooses the current time as the timestamp t_i. Where t_i gives the freshness of the signed message to against reply attack. The vehicle chooses a random number $r_i \in Z_q^*$ and calculates $R_i = r_i P$. Then calculate $h_i = H_2\left(m_i, PID_i, vpk_i, ID_{Rj}\right), T_i = r_i H_j + h_i S_i$. Finally, $\sigma_i = (R_i, T_i)$ is a signature on $m_i || t_i$ of PID_i. Then, V_i sends $\{PID_i, m_i, vpk_i, t_i, \sigma_i\}$ to the nearby RSU.

- **Verify**

Once a RSU receives the signed message $\{PID_i, m_i, vpk_i, t_i, \sigma_i\}$, it first checks the freshness of t_i. Suppose the time when the RSU receives the signed message is t_{RSU} and Δt is the max delay during the transmission defined before. If $\Delta t \geq t_{RSU} - t_i$, RSU continues the verification procedure. The RSU R_j calculates $H_j = H_1(ID_{Rj})$ and stores it in its storage. There is one thing that needs to be noticed, that is, H_j only needs to be calculated once for R_j, because R_j is an immobile unit and its identity will not change. Then R_j calculates $Q_i = H_3(PID_i),\ h_i = H_2\left(m_i, PID_i, vpk_i, ID_{Rj}\right)$ and checks whether $e(P, T_i) = e(P_{pub}, h_i Q_i) e(H_j, R_i + h_i vpk_i)$ holds or not. If it holds, accept the signed message; otherwise reject.

- **Aggregate**

In our scheme, RSU plays the role of aggregator who can aggregate a series of individual signatures into a single one. Without losing generality, assume a set of vehicles $\{V_1, V_2, ..., V_n\}$ with pseudo identities $\{PID_1, PID_2, ..., PID_n\}$, vehicle public keys $\{vpk_1, vpk_2, ..., vpk_n\}$ and corresponding message-signature pairs $\{(m_1 \parallel t_1, \sigma_1 = (R_1, T_1), ..., (m_n \parallel t_n, \sigma_n = (R_n, T_n)\}$, the RSU calculates $R = \sum_{i=1}^{n} R_i, T = \sum_{i=1}^{n} T_i$ and outputs the aggregated signature $\sigma = (R, T)$.

- **Aggregate verify**

Once an application server receives the certificateless aggregated signature $\sigma = (R, T)$ and corresponding messages, pseudo identities, vehicle public keys. The application server will check the freshness of t_i for i=1,2,...,n. If it's under a valid period, then the application server calculates $Q_i = H_3(PID_i),\ h_i = H_2\left(m_i, PID_i, vpk_i, ID_{Rj}\right)$, and checks whether $e(P, T) = e(P_{pub}, \sum_{i=1}^{n} h_i Q_i) e(H_j, R + \sum_{i=1}^{n} h_i vpk_i)$ holds or not. If it holds, accept the signed message; otherwise reject. If there exists some messages which are not under a valid period, application server would still execute the aggregate verify procedure as the above described; if the verification passes, the application server will drop the stale messages after that.

5. Security proof and analysis

In this section, we will first give the security proof of the proposed scheme, and then we will analyze the security requirements described in part 3.

5.1. Security proof

We define the two types of adversary $\mathcal{A}_1$ and $\mathcal{A}_2$. Adversary $\mathcal{A}_1$ can replace vehicle's public key vpk_i but cannot reveal the system master key. Adversary $\mathcal{A}_2$ knows the master secret key of PKG(malicious but passive KGC) and can generate the partial private key for the vehicle but does not know the vehicle secret key. We first describe two games for $\mathcal{A}_1$ and $\mathcal{A}_2$, and the security of our scheme can be modeled through the game between the challenger and the adversary.

Game 1: Let $\mathcal{C}$ be the challenger and ℓ be the security parameter.

1. $\mathcal{C}$ executes Setup(ℓ) to get the private/public key pair of PKG.
2. During the simulation, $\mathcal{A}_1$ can make the following queries: create-vehicle, partial-key, vehicle-secret-key, vehicle-public-key replacement and sign.
3. $\mathcal{A}_1$ outputs a certificateless aggregate signature σ^* signed by n vehicles with pseudo identities $L^*_{PID} = \{PID^*_1, PID^*_2, ..., PID^*_n\}$, vehicle public keys $L^*_{vpk} = \{vpk^*_1, vpk^*_2, ..., vpk^*_n\}$ and corresponding message-signature pairs $\{(m_1 \parallel t_1, \sigma_1 = (R_1, T_1), ..., (m_n \parallel t_n, \sigma_n = (R_n, T_n)\}$.

We say that $\mathcal{A}_1$ wins the Game iff

1. σ^* is a legal certificateless aggregate signature on messages $\{M^*_1, M^*_2, ..., M^*_n\}$ under pseudo identities $\{PID^*_1, PID^*_2, ..., PID^*_n\}$ and the corresponding public keys $\{vpk^*_1, vpk^*_2, ..., vpk^*_n\}$.

2. at least one pseudonym, without loss of generality, say $PID_1^* \in L_{PID}^*$ has not been queried during the partial-key query and (PID_1^*, M_1^*) has not been queried during the sign query.

Definition 2. The proposed scheme is said to be type-I secure if there is no polynomial-time adversary $\mathcal{A}_1$ can win the Game with non-negligible probability.

Game 2: Let $\mathcal{C}$ be the challenger and ℓ be the security parameter.

1. $\mathcal{C}$ execute Setup(ℓ) to get the private/public key pair of PKG. And $\mathcal{A}_2$ is not allowed making any query during the stage.
2. During the simulation, $\mathcal{A}_2$ can make the following queries: create-vehicle, vehicle-secret-key, vehicle-public-key replacement and sign.
3. $\mathcal{A}_2$ outputs a certificateless aggregate signature σ^* signed by n vehicles with pseudo identities $L_{PID}^* = \{PID_1^*, PID_2^*, ..., PID_n^*\}$, vehicle public keys $L_{vpk}^* = \{vpk_1^*, vpk_2^*, ..., vpk_n^*\}$ and corresponding message-signature pairs $\{(m_1 \parallel t_1, \sigma_1 = (R_1, T_1), ..., (m_n \parallel t_n, \sigma_n = (R_n, T_n)\}$.

We say that $\mathcal{A}_2$ wins the Game iff

1. σ^* is a legal certificateless aggregate signature on messages $\{M_1^*, M_2^*, ..., M_n^*\}$ under pseudo identities $\{PID_1^*, PID_2^*, ..., PID_n^*\}$ and the corresponding public keys $\{vpk_1^*, vpk_2^*, ..., vpk_n^*\}$.
2. At least one of the pseudonym, without loss of generality, say $PID_1^* \in L_{PID}^*$ has not been queried during the vehicle-secret-key query to get the vsk_1 and (PID_1^*, M_1^*) has not been queried during the sign query.

Definition 3. The proposed scheme is said to be type-II secure if there is no polynomial-time adversary $\mathcal{A}_2$ can win the Game with non-negligible probability.

Theorem 1. *In the random oracle model, the proposed scheme is existentially unforgeable against adaptively chosen-message, chosen-identity and public-key- replacement attack under the CDH hard problem assumption.*

Lemma 1. *In the random oracle model, if an adversary $\mathcal{A}_1$ can forge a valid certificateless signature during the time t with a non-negligible probability ε after making $q_{H_i}(i = 1, 2)$ queries to random oracles H_i for $i = 1, 2$, q_{psk} partial private key queries, q_{vsk} vehicle secret key queries and q_s sign queries, then there exists an algorithm C who can solve the CDH problem with probability $\varepsilon' \geq \left(1 - \frac{1}{q_c+1}\right)^{q_{psk}+q_{vsk}} \cdot \left(1 - \frac{1}{q_s+1}\right)^{q_s} \frac{1}{(q_c(q_s+1))\varepsilon}$ at time $t' < t + O(3q_c + q_{H_1} + q_{H2} + 4q_s + 2n + 1)t_m$ where t_m denote the time for a scalar multiplication.*

Proof. Given a random instance (*P, aP, bP*) of CDH problem, challenger $\mathcal{C}$ interacts with the adversary $\mathcal{A}_1$. By using the forgery algorithm $\mathcal{A}_1$, $\mathcal{C}$ outputs the CDH problem solution *abP*.

$\mathcal{C}$ executes the setup algorithm on input a security parameter ℓ to generate the system parameters *params*, and sets $P_{pub} = aP$ then sends *params* to $\mathcal{A}_1$. $\mathcal{C}$ randomly chooses a number $t \in \{1, 2, ..., q_c\}$ and maintains three lists $H_1^{list}, H_2^{list}, PK^{list}$ which are empty at first. $\mathcal{A}_1$ can adaptively make the following queries to $\mathcal{C}$: □

5.1.1. Create vehicle queries

$\mathcal{C}$ maintains the $PK^{list} = \{(PID_i, psk_i, vsk_i, vpk_i)\}$. Suppose $\mathcal{A}_1$ makes a query on $PID_i (i \in [1, q_c])$, $\mathcal{C}$ checks the PK^{list}, if the list includes (PID_i, psk_i, vsk_i, vpk_i), then respond (Q_i, vpk_i). Otherwise, execute the following operations:

1. If $i \neq t$, $\mathcal{C}$ randomly chooses $\alpha_i, x_i \in Z_q^*$ and sets $Q_i = \alpha_i P, D_i = \alpha_i(aP), vpk_i = x_i P$, where x_i is the vehicle secret key.
2. If $i = t$, $\mathcal{C}$ randomly chooses $\alpha_i, x_i \in Z_q^*$, and set $Q_i = bP - aP, D_i = \perp, vpk_i = x_i P$, where x_i is the vehicle secret key.

In the above two situations, $\mathcal{C}$ inserts (PID_i, psk_i, vsk_i, vpk_i) to the list and responds (Q_i, vpk_i).

5.1.2. Partial-key queries

Suppose $\mathcal{A}_1$ makes a query on $PID_i (i \in [1, q_{psk}])$, and $\mathcal{C}$ checks the PK^{list} first. If the list does not include (PID_i, psk_i, vsk_i, vpk_i), $\mathcal{C}$ outputs "$\perp$". Otherwise, $\mathcal{C}$ executes the following operations:

1. If $i \neq t$, $\mathcal{C}$ responds psk_i.
2. If $i = t$, $\mathcal{C}$ halts and fails.

5.1.3. Vehicle-secret-key queries

Suppose $\mathcal{A}_1$ makes a query on $PID_i (i \in [1, q_{vsk}])$, and $\mathcal{C}$ checks the PK^{list} first. If the list does not include (PID_i, psk_i, vsk_i, vpk_i), $\mathcal{C}$ outputs "$\perp$". Otherwise, $\mathcal{C}$ executes the following operations:

1. If $i \neq t$, $\mathcal{C}$ responds vsk_i.
2. If $i = t$, $\mathcal{C}$ halts and fails.

5.1.4. Vehicle-public-key replacement queries

Suppose $\mathcal{A}_1$ makes a query on $(PID_i, vpk_i^{'})$, and $\mathcal{C}$ check the PK^{list} first. If the list includes (PID_i, psk_i, vsk_i, vpk_i), $\mathcal{C}$ updates the vpk_i. Otherwise, $\mathcal{C}$ outputs "$\perp$".

H_1 queries: $\mathcal{C}$ maintains the $H_1^{list} = \{(ID_{Rj}, \beta_i, H_i)\}$. Suppose $\mathcal{A}_1$ makes a query on $ID_{Rj}(i \in [1, q_{H_1}])$, $\mathcal{C}$ checks the H_1^{list} first. If the list does not include (ID_{Rj}, β_i, H_i), $\mathcal{C}$ randomly chooses $\beta_i \in Z_q^*$ and sets $H_i = \beta_i(aP)$, then inserts (ID_{Rj}, β_i, H_i) to the list. Otherwise, $\mathcal{C}$ responds H_i.

H_2 queries: $\mathcal{C}$ maintain the $H_2^{list} = \{(m_i, ID_i, vpk_i, ID_{Rj}, h_i, p_i)\}$. Suppose $\mathcal{A}_1$ makes a query on $(m_i, PID_i, vpk_i, ID_{Rj})(i \in [1, q_{H_2}])$, $\mathcal{C}$ check the H_2^{list} first. If the list includes (ID_{Rj}, β_i, H_i), $\mathcal{C}$ responds h_i. Otherwise, $\mathcal{C}$ executes the following operations:

1. If $PID_i \neq PID_t$, $\mathcal{C}$ randomly chooses $h_i \in Z_q^*$ and inserts $(m_i, ID_i, vpk_i, ID_{Rj}, h_i, p_i = \perp)$ to the list.
2. If $PID_i = PID_t$, $\mathcal{C}$ randomly chooses $h_i \in Z_q^*$ and tosses a coin to set $p_i \in \{0, 1\}(pr[p_i = 0] = \delta, pr[p_i = 0] = 1 - \delta)$.

In the above two situations, $\mathcal{C}$ inserts (m_i, ID_i, vpk_i, ID_{Rj}, h_i, p_i) to the list and responds h_i.

5.1.5. Sign queries

Suppose$\mathcal{A}_1$ makes a query on $(mj, PID_k)(i \in [1, q_s])$, $\mathcal{C}$check the PK^{list} first. If the list does not include (PID_i, psk_i, vsk_i, vpk_i), outputs "$\perp$". Otherwise, $\mathcal{C}$ checks the corresponding $PK^{list}, H_1^{list}, H_2^{list}$ and executes the following operations:

1. If $PID_k \neq PID_t$, $\mathcal{C}$ randomly chooses $x_i \in Z_q^*$ and generates the signature $\sigma_i = (R_i, T_i)$ where $R_i = r_iP, T_i = h_i.psk_k + (x_i.h_i + r_i)\beta_i(aP)$.
2. If $PID_k = PID_t$ and $p_i = 0$, $\mathcal{C}$ randomly choose $x_i \in Z_q^*$ and generate the singnature $\sigma_i = (R_i, T_i)$ where $R_i = -\beta_i^{-1}.h_i(bP), T_i = h_i.\alpha_t(aP) + \beta_i.h_i.x_t(aP)$.
3. If $PID_k = PID_t$ and $p_i = 1$, $\mathcal{C}$ halts and fails.

After making the queries, $\mathcal{A}_1$ outputs a tuple (m^*, PID^*, R^*, T^*) where $m^* = (m_1^*, m_2^*, ..., m_n^*), PID^* = (PID_1^*, PID_1^*, ..., PID_n^*)$. ($R^*$, T^*) is the certificateless aggregated signature signed by n users whose pseudo identity is $PID_i(i = 1, 2, ..., n)$ on message. According to the assumption, the signature is valid, so $\mathcal{A}_1$ wins the game. If $PID_k = PID_t$, $\mathcal{C}$ halts and fails. Otherwise, $\mathcal{C}$ executes the following operations:

1. If $p^* = 0$, $\mathcal{C}$ halts and fails.
2. If $p^* \neq 0$, $\mathcal{C}$ uses $\mathcal{A}_1$ to solve the CDH hard problem.

Because $\mathcal{A}_1$ generates a valid signature, the forged aggregated signature must satisfy $R^* = \beta^{*-1}(h^*\alpha^*P + bP), T^* = (h + 1)abP + \beta^*h^*x^*(aP)$. Where α^*, vpk^* are obtained from PK^{list}, β^* is obtained from H_1^{list} and h^* is obtained from H_2^{list}. Finally, $\mathcal{C}$ uses σ^* to solve the CDH problem and outputs $abP = (h^* + 1)^{-1}(T^* - \beta^*h^*x^*(aP))$.

The instance of $\mathcal{C}$ solvping the CDH problem can be transformed into the following three incidents

E_1: $\mathcal{C}$ does not quit during the game.

E_2: $\mathcal{A}_1$ forges a valid signature through the game.

E_3: E_2 happens, and there exists $i \in [1, n]$ satisfying $PID^* = PID_t$ and $p^* = 1$P.

If the above incidents happen, $\mathcal{C}$ wins the game. So the probability of $\mathcal{C}$ winning the game is $\Pr[E_1 \wedge E_2 \wedge E_3] = \Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_1 \wedge E_2]$ where $\Pr[E_1] \geq (1 - \frac{1}{q_c})^{q_{psk}+q_{vsk}}(1 - \delta)^{q_s}, \Pr[E_2|E_1] \geq \varepsilon, \Pr[E_3|E_1 \wedge E_2] \geq \frac{\delta}{q_c}$ and $\delta(1 - \delta)^{q_s}$ can achieve the maximum when $\delta = \frac{1}{q_s+1}$. So we can infer to the result that: $\varepsilon^{'} = \Pr[C(P, aP, bP) \rightarrow abP] \geq (1 - \frac{1}{q_c})^{q_{psk}+q_{vsk}}(1 - \frac{1}{q_s+1})^{q_s}\frac{1}{q_c(q_s+1)}\varepsilon$.

Theorem 2. *In the random oracle model, the proposed scheme is existentially unforgeable against the adversary $\mathcal{A}_2$'s adaptive chosen-message, chosen-identity and public-key- replacement attack under the CDH hard problem assumption.*

Lemma 2. *In the random oracle model, if an adversary $\mathcal{A}_2$ can forge a valid certificateless signature during the time t with a non-negligible probability ε, then there exists an algorithm $\mathcal{C}$ who can solve the CDH problem with probability $\varepsilon^{'} \geq \left(1 - \frac{1}{q_c}\right)^{q_{psk}+q_{vsk}}.\left(1 - \frac{1}{q_s+1}\right)^{q_s}\frac{1}{(q_c(q_s+1))\varepsilon}$ at time $t' < t + O(3q_c + q_{H_1} + q_{H2} + 4q_s + 2n + 1)t_m$ where t_m denote the time for a scalar multiplication.*

The proof of type-II secure is similar with the proof of type-I secure so the proof process is omitted.

5.2. Analysis of security requirements

We give a brief introduction of the security requirements in VANET including identity privacy-preserving, message authentication, traceability, unlinkability and replay attack resistance. Then we will make an analysis that the proposed scheme satisfy the above security requirements.

1. *Message authentication:* In our scheme, each message generated by the vehicle needs to be signed before being sent to the nearby RSU, and RSU can verify the message to ensure that the message has not been forged or modified by an adversary or illegal vehicle.

Table 2
The comparison of related CLAS schemes.

Scheme	Sign a message	Indiviual verify	Aggregate verify	SL
[26]	$3\mathcal{S}+2\mathcal{H}$	$4\mathcal{P}+3\mathcal{H}$	$(n+3)\mathcal{P}+(2n+1)\mathcal{H}$	$(n+1)\mathcal{P}_1$
[20]	$3\mathcal{S}$	$3\mathcal{P}+\mathcal{H}+2\mathcal{S}$	$3\mathcal{P}+n\mathcal{H}+2n\mathcal{S}$	$(n+1)\mathcal{P}_1$
[24]	$5\mathcal{S}+3\mathcal{H}$	$5\mathcal{P}+5\mathcal{H}+2\mathcal{S}$	$5\mathcal{P}+(2n+3)\mathcal{H}+2n\mathcal{S}$	$2\mathcal{P}_1$
[11]	$3\mathcal{S}$	$3\mathcal{P}+2\mathcal{H}+2\mathcal{S}$	$3\mathcal{P}+(n+1)\mathcal{H}+2n\mathcal{S}$	$2\mathcal{P}_1$
Our scheme	$3\mathcal{S}$	$3\mathcal{P}+\mathcal{H}+2\mathcal{S}$	$3\mathcal{P}+n\mathcal{H}+2n\mathcal{S}$	$2\mathcal{P}_1$

2. *Identity privacy-preserving:* During the communication, the real identity of vehicle keep anonymous in the message. Each vehicle communicates with others using the pseudo identity generated by TRA. No adversary can learn the real identity from the pseudonym.
3. *Traceability:* TRA can track the real identity from the vehicle's pseudonym by calculating $RID_i = PID_{i,2} \oplus H_0(\alpha PID_{i,1}, VP_i)$ and the private key of TRA α is keep secret and only known to itself.
4. *Unlinkability:* During the communication, the vehicle signs different messages using different pseudonyms and corresponding secret keys. The pseudonyms do not have any link, so our scheme achieves the unlinkability.
5. *Replay attack resistance:* In the sign algorithm, we use a timestamp t in the signature generation process to ensure that the RSUs receive the newest messages. So, it is impossible for an adversary to send the received signed message and try to send it when it is invalid.

6. Performance evaluation

In this section ,we will first make a comparison between our scheme and existing CLAS schemes about computation and communication cost, and then we will evaluate the efficiency of our scheme and some other VANET-based schemes.

6.1. The comparison between our scheme and CLAS schemes

Computational overhead is an important factor in evaluating the performance of the scheme. We first define the notation of the time overhead of some cryptographic-related operations in the proposed scheme and other schemes. Let $\mathcal{P}$ be the time for making a pairing operation, $\mathcal{H}$ be the time for making a map-to-point hash function, and $\mathcal{S}$ be the time for executing a scalar multiplication. The above three operations are the main operations that affect the efficiency of the scheme, so we only take these three time consuming operations into consideration, and regardless of the time for executing the operations of addition and one-way hash function . Besides, we use *SL* to denote the length of the aggregated signature, and use $\mathcal{P}_1$ to denote the length of a point in G_1.

We adopt the experiment in [7], by using the MIRACL cryptographic library, we choose the Tate Pairing over an MNT curve at a 80-bit security level and embedding degree 6. The experiment is executed in a machine which equipped with a Intel i7 3.07GHz CPU. For simplicity, we assume that vehicles and RSUs have the same equipment and execute the same Tate pairing operation. The experiment results are as follows: $\mathcal{P}$ is about 3.21 ms, $\mathcal{H}$ is about 0.09 ms, $\mathcal{S}$ is about 0.39 ms.

Table 2 lists the comparison between our scheme and other existing CLAS [11,20,24,26] schemes in terms of computation cost and communication cost. We consider the cost in three phase: message signing, individual verification, and aggregate verify. It is easy to see that our scheme has better performance in terms of computation cost and the length of aggregated signature is constant which is independent from the number of signatures. Compared with scheme in [20,26], the fully aggregation is achieved without increasing the computation overhead, that is, the length of aggregated signature is fixed, while the length of aggregated signature in [20,26] grows linearly as the number of signatures increases.

6.2. The comparison between schemes in VANET

Scholars have proposed many schemes to satisfy the requirement of privacy and security. In [23], Zhang et al. proposed a privacy-preserving scheme based on identity-based aggregate signature.They use a common string synchronization algorithm to ensure the vehicle shares the same string in a certain time interval.The individual signature can be aggregated into an aggregate signature and the aggregated signature can be re-aggregated. In 2017, Zhang et al. [25] proposed an distributed aggregate privacy-preserving authentication scheme in VANET. In their scheme, RSU acts as a lower TA which is in charge of registering for the vehicle under its coverage. Their scheme does not rely on the ideal TPD, the security information stored in TPD can be periodically updated. However, the scheme does not indicate who is the aggregator in the aggregation phase.

In [15], Malhi and Batra proposed an efficient certificateless aggregate signature in VANET. A key generator center is responsible for generating partial key for a vehicle, and RSU is responsible for generating pseudonyms for the vehicle. When the vehicle enters an area under a new RSU's coverage, the pseudonym needs to be updated. However the scheme cannot against replay attack and the length of aggregated signature grows linearly when the number of signatures increases.

We make a comparison between our scheme and the related work [15,23,25]. From the security analysis in Section 5.2 we can see that our scheme satisfies all the requirements including authentication, anonymity, traceability, unlinkability, and

Table 3
The comparison of computation cost between schemes in VANET.

	Verify one signature	Verify n signatures
[23]	$3\mathcal{P}+2\mathcal{H}+2\mathcal{S}$	$3\mathcal{P}+2n\mathcal{H}+2n\mathcal{S}$
[15]	$3\mathcal{P}+3\mathcal{S}$	$3\mathcal{P}+3n\mathcal{S}$
[25]	$2\mathcal{P}+2\mathcal{H}+2\mathcal{S}$	$2\mathcal{P}+2n\mathcal{H}+2n\mathcal{S}$
Our scheme	$3\mathcal{P}+\mathcal{H}+2\mathcal{S}$	$3\mathcal{P}+n\mathcal{H}+2n\mathcal{S}$

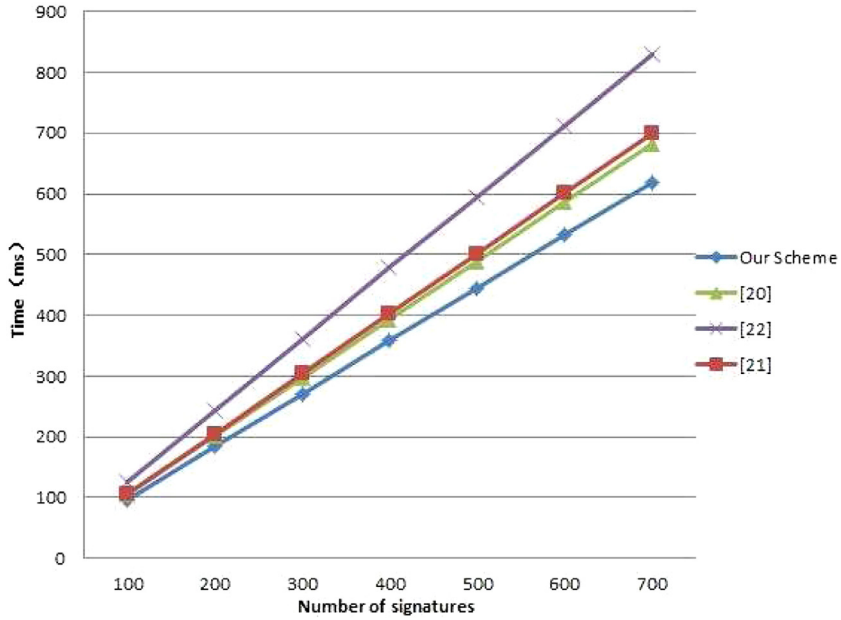

Fig. 2. Computation cost vs the number of signatures.

replace attack resistance. And Table 3 shows the comparison between the above schemes in terms of computation cost when verifying one signature and verifying n signatures. As shown in Section 6.1, we will only consider the dominant time-consuming operation while ignore the lightweight operation such as one-way hash function and point addition operation. And Fig. 2 shows the relationship between computation cost and the number of signatures. It is easy to see that our scheme has a better performance compared with the schemes in [15,23,25].

7. Conclusion

We propose a privacy-preserving authentication scheme which achieves full aggregation in VANET, and we can see that the scheme satisfies the security requirements in VANET through the security analysis. We divide the sign phase into two steps and utilize the pre-calculation method to reduce the computation cost in sign phase. RSU can aggregate multiple signatures into a single one, and the length of aggregated signature is a constant size which greatly reduces the transmission overhead between RSU and application server and the efficiency of verification for application is improved. In the future work, we will consider to use a more lightweight signature scheme to reduce the computation and communication cost.

Acknowledgments

The work was supported by the National Natural Science Foundation of China (Nos. 61872001, 61572001, 61702005), the Open Fund of Key Laboratory of Embedded System and Service Computing (Tongji University), Ministry of Education (No. ESSCKF2018-03), the Natural Science Foundation of Anhui Province (No. 1708085QF136), the Open Fund for Discipline Construction, Institute of Physical Science and Information Technology, Anhui University and the Excellent Talent Project of Anhui University. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: Asiacrypt, vol. 2894, Springer, 2003, pp. 452–473.

[2] J. Camenisch, S. Hohenberger, M.O. Pedersen, Batch verification of short signatures, in: Eurocrypt, vol. 4515, Springer, 2007, pp. 246–263.
[3] J. Cui, J. Zhang, H. Zhong, R. Shi, Y. Xu, An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks, Inf. Sci. (2018).
[4] D. He, M. Tian, J. Chen, Insecurity of an efficient certificateless aggregate signature with constant pairing computations, Inf. Sci. 268 (2014) 458–462.
[5] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2681–2691.
[6] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, M.K. Khan, An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Inf. Sci. 317 (2015) 48–66.
[7] S.J. Horng, S.F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, M.K. Khan, b-specs+: Batch verification for secure pseudonymous authentication in VANET, IEEE Trans. Inf. Forensics Secur. 8 (11) (2013) 1860–1875.
[8] B.C. Hu, D.S. Wong, Z. Zhang, X. Deng, Key replacement attack against a generic construction of certificateless signature, in: ACISP, vol. 6, Springer, 2006, pp. 235–246.
[9] J.-P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Secur. Privacy 2 (3) (2004) 49–55.
[10] C.-C. Lee, Y.-M. Lai, Toward a secure batch verification with group testing for VANET, Wirel. Netw. 19 (6) (2013) 1441–1449.
[11] D. Liu, R. Shi, S. Zhang, Z. Hong, Efficient anonymous roaming authentication scheme using certificateless aggregate signature in wireless network, J. Commun. (2016).
[12] N.W. Lo, J.L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings, IEEE Trans. Intell. Transp. Syst. 17 (5) (2016) 1319–1328.
[13] R. Lu, X. Lin, Z. Shi, X.S. Shen, A lightweight conditional privacy-preservation protocol for vehicular traffic-monitoring systems, IEEE Intell. Syst. 28 (3) (2013) 62–65.
[14] R. Lu, X. Lin, H. Zhu, P.H. Ho, X. Shen, Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications, in: INFOCOM 2008. the Conference on Computer Communications. IEEE, 2008. 1229–1237.
[15] A.K. Malhi, S. Batra, An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks, Discr. Math. Theor. Comp. Sci. 17 (1) (2015).
[16] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.
[17] A. Shamir, et al., Identity-based cryptosystems and signature schemes., in: Crypto, vol. 84, Springer, 1984, pp. 47–53.
[18] K.A. Shim, Cpas: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61 (4) (2012) 1874–1883.
[19] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, M.K. Khan, Enhancing security and privacy for identity-based batch verification scheme in VANETs, IEEE Trans. Veh. Technol. 66 (4) (2017) 3235–3248.
[20] H. Xiong, Z. Guan, Z. Chen, F. Li, An efficient certificateless aggregate signature with constant pairing computations, Inf. Sci. 219 (2013) 225–235.
[21] D.H. Yum, P.J. Lee, Generic construction of certificateless signature, in: Acisp, vol. 4, Springer, 2004, pp. 200–211.
[22] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, in: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, IEEE, 2008, pp. 246–250.
[23] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, B. Qin, Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response, IEEE Trans. Comput. 65 (8) (2016) 2562–2574.
[24] L. Zhang, B. Qin, Q. Wu, F. Zhang, Efficient many-to-one authentication with certificateless aggregate signatures, Comput. Netw. 54 (14) (2010) 2482–2491.
[25] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, Distributed aggregate privacy-preserving authentication in VANETs, IEEE Trans. Intell. Transp. Syst. 18 (3) (2017) 516–526.
[26] L. Zhang, F. Zhang, A new certificateless aggregate signature scheme, Comput. Commun. 32 (6) (2009) 1079–1085.
[27] Z. Zhang, D.S. Wong, J. Xu, D. Feng, Certificateless public-key signature: security model and efficient construction, in: ACNS, 6, 2006, pp. 293–308.