An Efficient Certificateless Aggregate Signature Scheme Designed for VANET

Cui Li[1,*], Gang Wu[1], Lipeng Xing[1], Feng Zhu[1] and Liang Zhao[2]

Abstract: The Vehicular Ad-hoc Network (VANET) is the fundamental of smart transportation system in the future, but the security of the communication between vehicles and vehicles, between vehicles and roadside infrastructures have become increasingly prominent. Certificateless aggregate signature protocol is used to address this security issue, but the existing schemes still have many drawbacks in terms of security and efficiency: First, many schemes are not secure, and signatures can be forged by the attacker; Second, even if some scheme are secure, many schemes use a large number of bilinear pairing operation, and the computation overhead is large. At the same time, the length of the aggregated signature also increases linearly with the increase of user numbers, resulting in a large communication overhead. In order to overcome the above challenges, we propose a new certificateless aggregate signature scheme for VANET, and prove the security of the scheme under the random oracle model. The new scheme uses pseudonym to realize the conditional privacy protection of the vehicle's information. The new scheme does not use bilinear pairing operation, and the calculation efficiency is high. At the same time, the length of the aggregate signature of the new scheme is constant, thereby greatly reducing the communication and storage overhead. The analysis results demonstrate that the new scheme is not only safer, but also superior in performance to the recent related schemes in computation overhead and communication cost.

Keywords: Vehicular Ad-hoc network, certificateless cryptography, aggregate signature, random oracle model.

1 Introduction

With the rapid development of wireless sensor technology, the construction of smart cities is the trend of the times. The Vehicular Ad-hoc Network (VANET) is an extremely important part of smart cities and the foundation of future intelligent transportation systems. VANET is a mobile ad-hoc network formed by communications between vehicles and vehicles, between vehicles and roadside infrastructures [Kim and Lee (2016)]. While improving efficiency and the riding environment, the network also brings

[1] College of Information and Communication, National University of Defense Technology, Xi'an, China.

[2] Ansys, Southpointe 2600 ANSYS Drive Canonsburg, Commonwealth of Pennsylvania, 15317, USA.

[*] Corresponding Author: Cui Li. Email: shichangcu@126.com.

Received: 06 May 2019; Accepted: 04 June 2019.

CMC. doi:10.32604/cmc.2020.07188 www.techscience.com/journal/cmc

many security threats such as eavesdropping, tampering, tracking user privacy and so on.

Digital signature is one of the core technologies of information security, which could provide security services such as authentication, integrity and non-repudiation for data transmission. The digital signature based on traditional public key cryptography requires a trusted authentication center to issue a certificate to each user. When the number of users is large, the management and maintenance of the certificate is very complicated, which greatly reduces the performance of the system.

In order to reduce the management of certificates, Shamir proposed the idea of identity-based public key cryptography in 1984 [Shamir (1976)]. Users choose their own identity information as public key, which can effectively solve the problem of certificate management in traditional public key cryptosystem. However, the identity-based public key cryptosystem requires a trusted private key generation center. The private key generation center can obtain the private key of all users and can forge the signature of any user. Therefore, the identity-based public key cryptosystem suffers the key escrow problem.

In 2003, Al-Riyami et al. [Al-Riyami and Paterson (2003)] proposed the concept of Certificateless Public Key Cryptography (CL-PKC). In this system, the private key generation center only generates part of the private key of the user, the user then generates its own private key independently according to the partial private key generated by the private key generation center and the secret value selected by itself, thus solving the certificate management and key escrow problem. So far, a number of certificateless cryptography schemes have been proposed to meet different needs.

Aggregate signature was first proposed by Boneh et al. in 2003 [Boneh, Gentry, Lynn et al. (2003)], which is a research hotspot in recent years and often appears in top-level conference papers. In an aggregate signature scheme, different users sign different messages separately, and these signatures can be combined into one signature, and the verifier can verify whether the signature is from a specified user by simply verifying the synthesized signature, thereby reducing the signature verification workload and signature storage space. Aggregate signature is the “batch processing” and “compression” technology in the field of digital signatures, and is very suitable for VANET with limited bandwidth and resources. Gong et al. [Gong, Long, Hong et al. (2007)] first combined aggregate signature and certificateless public key cryptography to propose a certificateless aggregate signature scheme, whose security was proved under the random oracle model. Since then, a large number of certificateless aggregate signature schemes have been proposed [Shen, Chen, Shen et al. (2016); Zhang (2016); Yang, Wang, Ma et al. (2018); Wu, Xu, He et al. (2018)].

Wang et al. [Wang and Teng (2018)] designed a certificateless aggregate signature algorithm for VANET, but the solution cannot resist the attack of Type II attacker. Once the attacker intercepts a user’s one valid signature on a message, the attacker can forge a legitimate signature of the user on any message, that is, the algorithm does not satisfy unforgeability. Zhong et al. [Zhong, Han, Cui et al. (2019)] proposed a privacy-preserving authentication scheme with full aggregation in VANET, but the scheme still can’t resist the attack of type II attacker. In the scheme proposed by Cui et al. [Cui, Zhang, Zhong et al. (2018)], the user’s secret value is not used in the aggregate signature algorithm, so that the malicious KGC can arbitrarily forge the user’s signature. Ismaila et al. [Ismaila and Sunday

(2019)] point out that the scheme of Cui et al. [Cui, Zhang, Zhong et al. (2018)] is not safe, give detailed attack steps, and propose an improved scheme; however, there are so many hash functions and function parameters in the improved scheme which is very unfavorable for reading and comprehension. In addition, after careful analysis, the improved scheme is also insecure for the type II attacker. The attacker can still forge a user's legal signature of other messages after knowing a legal signature of the user. In the scheme of Kumar et al. [Kumar, Kumari, Sharma et al. (2018)] which is published in The Journal of Supercomputing, RSU's public key is added to the vehicle's signature algorithm, the attacker can arbitrarily forge the user's signature by replacing the RSU's public key. For the scheme of Malhi et al. [Malhi and Batra (2015)], Kumar et al. [Kumar and Sharma (2018)] point out that it is not safe for the Type II attacker, and propose an improved scheme. Although the improved scheme [Kumar and Sharma (2018)] is safe, the length of the aggregate signature increases with the number of users, which result in huge communication overhead; furthermore, the improved scheme does not give a security proof. Kumar et al. [Kumar, Kumari, Sharma et al. (2018)] proposed a certificateless aggregate signature scheme for medical wireless sensor networks which is published in Sustainable Computing, but the scheme still has the problem of long aggregated signature length. In addition, most of the existing schemes use bilinear pairing operations. From theoretical analysis [Chen, Cheng and Smart (2007)] and experimental results [Cao, Kou and Du (2010)], it is shown that under the same safety strength, the calculation of bilinear pairing is about 20 times higher than that of elliptic curve scalar multiplication. Therefore, the existing schemes generally have the problem of large computational overhead.

In summary, the existing VANET-based certificateless aggregate signature schemes still have three problems: First, many schemes don't research deep enough of the security model of the certificateless aggregate signature, which are not secure and cannot resist the attack of type I attacker or type II attacker; Second, most schemes require a large number of bilinear pairing operations, and the computational efficiency of these schemes are not high. For computing and bandwidth constrained VANET, there are still challenges in application; Third, the length of the aggregated signature increases linearly with the number of users, and the communication overhead is large. In order to solve these problems, we takes Zhong et al.'s [Zhong, Han, Cui et al. (2019)] scheme as an example to give the attack steps of type II attacker, analyzes the reasons for the attacks, and proposes a new VANET-based certificateless aggregate signature scheme. The security of the new scheme is proved under the random oracle model. The new scheme uses pseudonym to realize the conditional privacy protection of vehicle's information. The scheme does not use bilinear pairing operation, and the calculation efficiency is high. At the same time, the aggregate signature length of the new scheme is constant, which greatly reduces communication and storage overhead. In one word, the new solution effectively solves the problems in the existing programs.

2 Analysis of Zhong et al.'s scheme

The scheme proposed by Zhong et al. [Zhong, Han, Cui et al. (2019)] is the latest research results of VANET-based certificateless aggregate signature algorithm. By analyzing the algorithm of Zhong et al., it is found that the algorithm is insecure, which cannot resist the attack of type II attacker. The detailed attack steps of the Zhong et al.'s algorithm is given below.

2.1 Scheme review of Zhong et al.

Zhong et al.'s scheme can be divided into seven algorithms:

(1) System setup: Trusted authority (TA) generates two groups G_1, G_2 with the same prime order q. P is a generator of G_1, 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 TRA. TAs choose four cryptographic hash functions: H_0, H_1, H_2, H_3.

(2) Pseudonym generation: Before joining the VANET, the vehicle should obtain the pseudonyms generated by TRA. A vehicle V_i chooses a random number $k_i \in Z_q^*$ and calculates $PID_{i,1} = k_i P$, 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 $PID_i = (PID_{i,1}, PID_{i,2}, VP_i)$ is transmitted to PKG via a secure channel.

(3) 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.

(4) Vehicle key generation: The vehicle V_i chooses a random number $x_i \in Z_q^*$ as its secret key vsk_i and calculates the vehicle public key $vpk_i = x_i P$.

(5) Sign:

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 $h_i = H_2(m_i, PID_i, vpk_i, ID_{Rj})$, $T_i = r_i H_j + h_i S_i$. 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.

(6) 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 . if t_i is fresh, RSU continues the verification procedure. The RSU R$_j$ calculates $H_j = H_1(ID_{Rj})$ and stores it in its storage. Then R$_j$ calculates $h_i = H_2(m_i, PID_i, vpk_i, ID_{Rj})$, $Q_i = H_3(PID_i)$ 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.

(7) Aggregate: Assume a set of vehicles $V_1, V_2, \cdots, V_n$ with pseudo identities $PID_1, PID_2, \cdots, PID_n$, vehicle public keys $vpk_1, vpk_2, \cdots, vpk_n$ and corresponding message-signature pairs $(m_1 \| t_1, \sigma_1 = (R_1, T_1)), \cdots, (m_n \| t_n, \sigma_n = (R_n, T_n))$. The RSU calculates $R = \sum_{i=1}^{n} R_i$, $T = \sum_{i=1}^{n} T_i$ and outputs the aggregated signature $\sigma = (R,T)$.

(8) Aggregate verify: Once an application server receives the certificateless aggregate signature $\sigma = (R,T)$ and corresponding messages, pseudo identities, vehicle public keys. The application will check the freshness of $t_i (i = 1, 2, \cdots, n)$, if t_i is fresh, then the application server calculates $Q_i = H_3(PID_i)$, $h_i = H_2(m_i, PID_i, vpk_i, ID_{Rj})$ 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.

2.2 Attack of Zhong et al.'s scheme

The certificateless aggregate signature scheme faces two types of attackers: Type I and Type II. The Type I attacker is the outsider, who doesn't know the system master key, but can replace the user's public key; The Type II attacker is the malicious KGC, who knows the system's master key, but cannot replace the user's public key. After careful analysis, it is found that Zhong et al.'s scheme is not safe under the attack of Type II attacker. The following specific attack algorithm is constructed to prove that Zhong et al.'s scheme does not satisfy its claimed unforgeability.

Assume there is a vehicle A, whose pseudo identity is PID_a , partial private key is $psk_a = sQ_a = sH_3(PID_a)$, secret value is x_a , and the corresponding public key is $vpk_a = x_a P$. Now, the vehicle A is in the area of RSU ID_{Rj}, A calculates $H_j = H_1(ID_{Rj})$ and $S_a = psk_a + vsk_a H_j$.

The signature phase of vehicle A to message m_i is: A randomly selects $r_i \in Z_q^*$, calculates $R_i = r_i P$, $h_i = H_2(m_i, PID_a, vpk_a, ID_{Rj})$, $T_i = r_i H_j + h_i S_a$. $\sigma_a = (R_i, T_i)$ is the signature of vehicle A to message m_i .

Let Q be a type II attacker. Since Q knows the system's master key, Q knows the partial private key of user A. After Q intercepts one legal signature $\sigma_a = (R_i, T_i)$ of A to m_i, Q calculates $h_i = H_2(m_i, PID_a, vpk_a, ID_{Rj})$, since $T_i = r_iH_j + h_iS_a$, then $T_i = r_iH_j + h_i \ \ psk_a + vsk_aH_j \ \ = r_iH_j + h_i psk_a + h_i x_a H_j$. Q calculates $T_i - h_i psk_a = H_j(r_i + x_a h_i)$, then $r_i + x_a h_i = \frac{T_i - h_i psk_a}{H_j}$.

Q forges the signature of vehicle A to another message $m_i^{'}$ as follows: Q calculates $h_i^{'} = H_2(m_i^{'}, PID_a, vpk_a, ID_{Rj})$, let $f = \frac{h_i^{'}}{h_i}$, $R_i^{'} = fR_i$, $T_i^{'} = h_i^{'} psk_a + fH_j \frac{T_i - h_i psk_a}{H_j} = h_i^{'} psk_a + f(T_i - h_i psk_a) = fT_i$, $\sigma_i^{'} = (R_i^{'}, T_i^{'})$ is the forged signature of user A to message $m_i^{'}$.

Theorem 1 The signature generated by Q through the above method is legal.

Proof The verifier verifies the forged signature $\sigma_i^{'} = (R_i^{'}, T_i^{'})$ generated by Q. As long as the signature can be verified, that is, the equation $e(P, T_i^{'}) = e(P_{pub}, h_i^{'}Q_a)e(H_j, R_i^{'} + h_i^{'}vpk_a)$ holds, the signature is legal.

First, the verifier calculates $h_i^{'} = H_2(m_i^{'}, PID_a, vpk_a, ID_{Rj})$, then computes

$$\begin{aligned} & e(P, T_i^{'}) = e(P, fT_i) = e(P, T_i)^f \\ & = e(P_{pub}, h_iQ_a)^f e(H_j, R_i + h_ivpk_a)^f \\ & = e(P_{pub}, h_i fQ_a)e(H_j, f(R_i + h_ivpk_a)) \\ & = e(P_{pub}, h_i^{'}Q_a)e(H_j, fR_i + h_i^{'}vpk_a) \\ & = e(P_{pub}, h_i^{'}Q_a)e(H_j, R_i^{'} + h_i^{'}vpk_a) \end{aligned} \tag{1}$$

Since the equation $e(P, T_i^{'}) = e(P_{pub}, h_i^{'}Q_a)e(H_j, R_i^{'} + h_i^{'}vpk_a)$ holds, so the signature verification phase succeeded. Through the above attack steps, it can be known that the single signature of the Zhong et al.'s scheme can be forged, thus the aggregate signature can also be forged.

In summary, the VANET-based certificateless aggregate signature scheme proposed by Zhong et al. [Zhong, Han, Cui et al. (2019)] is not safe under the attack of type II attacker.

3 The proposed scheme

3.1 System model

In this paper, the system model of VANET consists of five entities: On Board Units (OBU) installed on the vehicle, Road Side Units (RSU) deployed on the infrastructure around the road, Key Generation Center (KGC), the Trace Authority (TRA) and the application server

(AS). These five entities are usually divided into two layers for communication, as shown in Fig. 1. The lower layer consists communications between OBU and OBU, between OBU and RSU, which is carried out through the DSRC protocol. The information is transmitted through the wireless channel, and there are security risks of eavesdropping, tampering and tracking user privacy. The upper layer contains communications between RSU and KGC, TRA and AS, and communication between TRA and KGC. The information is transmitted through the wired channel, and the communication is relatively safe. The specific description of each entity is as follows.

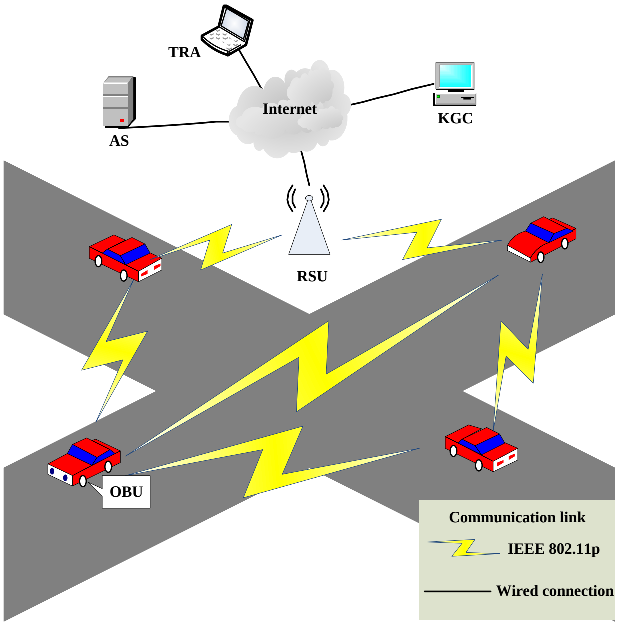

Figure 1: System model of VANET

TRA is the authority to manage vehicles. On one hand, it is responsible for system initialization and parameter generation. On the other hand, it accepts the registration of the vehicles, saves its true identity, and is responsible for tracking the owner to reveal the true identity of the owner when a traffic accident occurred or the car owner commits a crime. TRA is completely trustworthy and has enough computing and storage capabilities.

KGC assists TRA in completing system initialization and parameter generation, and is responsible for generating the vehicle's partial private key. KGC is semi-trusted, it is honest but curious. KGC knows the partial private key of each vehicle and tries to forge the user's signature.

AS is the program of the traffic control center. It analyzes the real-time traffic information and traffic accident information sent by the vehicles, and broadcasts the analysis results to each vehicle. The AS is completely trusted and has the same computing and storage capabilities as the TRA.

RSU is installed on both sides of the road. It collects real-time traffic information and various requests sent by the OBU, aggregates these messages and sends them to the AS for summary and analysis. RSU is semi-trusted and has limited storage and computing power.

OBU is an onboard unit installed on the vehicle. It collects information such as road conditions and locations in real time, and then sends the information to the RSU in the area where the vehicle is located. OBU is untrustworthy, and its storage and computing power is also limited by resources.

3.2 The new certificateless aggregate signature scheme

The new certificateless aggregate signature scheme for VANET proposed in this paper consists of eight algorithms: system setup algorithm, pseudonym generation algorithm, partial key generation algorithm, user key generation algorithm, signature algorithm, signature verification algorithm, signature aggregate algorithm and aggregate signature verification algorithm. Before describing the specific algorithm, the symbols used in the scheme of this paper are explained in Tab. 1.

Table 1: Notations used and the description

Symbol	Description
G_1	An additive cyclic group
P	Generator of G_1
ID_{Rj}	The j_{th} RSU’s identity
RID_i	The i_{th} vehicle’s real identity
PID_i / T_i	The i_{th} vehicle’s pseudo identity and its valid period
d_i	The i_{th} vehicle’s partial private key
x_i	The i_{th} vehicle’s secret value
α	TRA’s private key
s / P_{pub}	KGC’s private key / public key

(1) System setup algorithm

This algorithm is executed by TRA and KGC. Enter the security parameter ℓ, TRA selects a large prime number q, an additive cyclic group G_1 with order q. P is the generator of G_1. TRA randomly selects $\alpha \in Z_q^*$ as its master key to generate the pseudonym of the vehicle. KGC randomly selects $s \in Z_q^*$ as its master key, and calculates $P_{pub} = sP$. s is used to generate the partial private key of each vehicle. Defines five hash function $H_0 : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to Z_q^*$, $H_2 : \{0,1\}^* \to Z_q^*$, $H_3 : \{0,1\}^* \to Z_q^*$, H_4 : $0,1\ ^* \to Z_q^*$. TRA and KGC keep their master key α and s secret, and expose system parameters $q, G_1, p, H_0, H_1, H_2, H_3, H_4, P_{pub}$.

(2) Pseudonym generation algorithm

This algorithm is executed by TRA. Before joining the VANET, the vehicle must be registered with the TRA. Only registered vehicles can enjoy the various services provided by VANET.

The vehicle transmits its real identity RID_i to the TRA through a secure channel. TRA detects whether RID_i exists. If it exists, TRA randomly takes $k_i \in Z_q^*$, calculates $PID_i = RID_i \oplus H_0(\alpha, k_i, T_i)$, saves k_i and PID_i. PID_i is the pseudonym of the vehicle, and T_i is the valid period of the pseudonym. TRA returns the vehicle's pseudonym PID_i to the vehicle and sends PID_i to the KGC simultaneously.

(3) Partial key generation algorithm

The algorithm is executed by KGC. After KGC receives the pseudonym PID_i of the vehicle, KGC calculates $Q_i = H_1(PID_i)$ and $d_i = sQ_i$. The partial private key that KGC generates for the vehicle is d_i.

(4) User key generation algorithm

The vehicle with pseudonym PID_i selects a random number $x_i \in Z_q^*$ as its secret value and calculates the corresponding public key $P_i = x_i P$. The vehicle's private key is $S_i = (d_i, x_i)$.

(5) Sign

The vehicle with identity PID_i picks a timestamp t_i to resist the attacker's replay attack. The vehicle randomly selects $r_i \in Z_q^*$, calculates $R_i = r_i P$, $h_i = H_2(m_i, PID_i, P_i, R_i, t_i)$, $f_i = H_3(P_{pub}, P_i, m_i)$, $g_i = H_4(m_i, P_{pub}, P_i, t_i)$ and $V_i = h_i r_i + x_i f_i + d_i g_i$. The signature of vehicle PID_i on the message m_i and the latest time stamp t_i is $\sigma_i = \ R_i, V_i$. The vehicle sends the message $PID_i, P_i, m_i, t_i, \sigma_i$ to the RSU in the area.

(6) Signature verification algorithm

The algorithm is executed by RSU. After RSU receives the single signature $PID_i, P_i, m_i, t_i, \sigma_i$ of the user PID_i, RSU first checks whether the timestamp t_i is fresh. If it is not fresh, discards the signature; Otherwise, RSU calculates $h_i = H_2(m_i, PID_i, P_i, R_i, t_i)$, $f_i = H_3(P_{pub}, P_i, m_i)$, $g_i = H_4(m_i, P_{pub}, P_i, t_i)$, and verifies whether the equation $V_i P = P_{pub} Q_i g_i + h_i R_i + P_i f_i$ holds or not. If it holds, the message is received, otherwise it is rejected.

(7) Signature aggregate algorithm

This algorithm is executed by RSU. Enter the single signature of n users $PID_i, P_i, m_i, t_i, \sigma_i$ $(i = 1, 2, \cdots, n)$. RSU first checks if the timestamp t_i $(i = 1, 2, \cdots, n)$ is valid or not. If it is invalid, discards the signature; Otherwise, RSU calculates $h_i = H_2(m_i, PID_i, P_i, R_i, t_i)$, then calculates $R = \sum_{i=1}^{n} h_i R_i$, $V = \sum_{i=1}^{n} V_i$, and finally outputs the aggregate signature $\sigma = R, V$.

(8) Aggregate signature verification algorithm

Enter the aggregate signature $\sigma = R, V$ of users $(PID_1, PID_2, \cdots, PID_n)$ on messages $(m_1, m_2, \cdots, m_n)$, the user's corresponding public key is $(P_1, P_2, \cdots, P_n)$, and the timestamp sequence is $(t_1, t_2, \cdots, t_n)$, the AS first detects the freshness of the timestamp and the valid period T_i of PID_i . If it passes the verification, AS calculates $Q_i = H_1(PID_i)$, $f_i = H_3(P_{pub}, P_i, m_i)$ and $g_i = H_4(m_i, P_{pub}, P_i, t_i)$, then verifies whether the equation $VP = P_{pub} \sum_{i=1}^{n} g_i Q_i + R + \sum_{i=1}^{n} P_i f_i$ holds or not. If it holds, it accepts the signature, otherwise the signature is discarded.

4 Security proof of the new scheme

Under the random oracle model, the security of the new scheme will be proved. The certificateless aggregate signature scheme faces two types of adversary A_1 and A_2. The adversary A_1 does not know the system's master key, but it has the ability to replace the legitimate user's public key. The adversary A_2 knows the system's master key, but it does not have the ability to replace the legitimate user's public key. Chen et al. [Chen, Wei, Zhu et al. (2015)] detail the definition of the unforgeability and the corresponding games of the certificateless aggregate signature scheme under the adaptive chosen message and identity attacks of the two types of adversary, which will not be repeated here.

Theorem 2 Under the random oracle model, if there is an adversary A_1, who can break the unforgeability of the new aggregate signature scheme with non-negligible advantages ξ after making adaptive chosen message and identity attack queries in polynomial times, then there is a distinguisher B who can take polynomial times to solve a DLP difficulty problem with non-negligible advantages $Adv[B] \geq \frac{1}{ne(q_s+n)}\left(1-\frac{q_{ppk}}{2^{\ell}}\right)\xi$ (wherein, q_{ppk} and q_s are the maximum number of partial key generation query and single signature query respectively, n is the user number taking part in the aggregate signature.)

Proof A_1 is an attacker while B is a challenger to the DLP difficulty problem. Given a random DLP example P, xP , where x is unknown, B's goal is to solve the DLP problem by using A_1, that is calculate x.

B runs the system setup algorithm, generates the public parameters $q, G_1, p, H_0, H_1, H_2, H_3, H_4, P_{pub}$ and sends them to A_1. B set $P_{pub} = xP$, x is the system's master key. B maintains lists L_2 , L_3 , L_4 , L_{ppk} , L_{sk} and L_s to track the H_2 oracle, H_3 oracle, H_4 oracle, partial key generation query, secret value generation query and single signature query respectively. At the beginning, each list is empty. B chooses PID^* as the challenging identity. The probability of selecting PID^* is $\theta \in [\frac{1}{q_s+n}, \frac{1}{q_s+1}]$ (q_s is the maximum number of single signature query, n is the number of aggregate users in the forgery phase).

Query stage: The adversary A_1 makes the following query.

H_2 query: B keeps the list $L_2 = \{m_i, PID_i, P_i, R_i, t_i, h_i\}$, initially empty. When B receives the H_2 query from A_1, if there is a corresponding tuple in the list L_2, then value h_i is directly returned to A_1 ; Otherwise, B randomly selects $h_i \in Z_q^*$, adds $\{m_i, PID_i, P_i, R_i, t_i, h_i\}$ to list L_2 and returns h_i to A_1.

H_3 query: B keeps the list $L_3 = \{P_{pub}, P_i, m_i, f_i\}$, initially empty. When B receives the H_3 query from A_1, if there is a corresponding tuple in the list, B returns f_i directly to A_1; Otherwise, B randomly picks $f_i \in Z_q^*$, adds $\{P_{pub}, P_i, m_i, f_i\}$ to list L_3 and returns f_i to A_1.

H_4 query: B keeps the list $L_4 = \{m_i, P_{pub}, P_i, t_i, g_i\}$, initially empty. When B receives the H_4 query from A_1, if there is a corresponding tuple in the list, B returns g_i directly to A_1; Otherwise, B randomly selects $g_i \in Z_q^*$, adds $\{m_i, P_{pub}, P_i, t_i, g_i\}$ to list L_4 and returns g_i to A_1.

Partial Key Generation query: B keeps the list $L_{ppk} = \{PID_i, d_i\}$, initially empty. When B receives a partial key generation query, if there is a corresponding tuple in the list L_{ppk}, B directly returns d_i to A_1; Otherwise, B checks whether PID_i and PID^* is equal:

1) if $PID_i = PID^*$, B randomly selects $d_i^* \in Z_q^*$, calculates $d_i = d_i^* x$, adds $\{PID_i, d_i\}$ to list L_{ppk} and returns d_i to A_1.
2) if $PID_i \neq PID^*$, B randomly selects $d_i \in Z_q^*$, adds $\{PID_i, d_i\}$ to list L_{ppk} and returns d_i to A_1.

Secret value query: When A_1 asks for the secret value of PID_i, B searches the list L_{sk}. If the list contains the corresponding secret value, then the corresponding secret value x_i is returned to A_1; Otherwise, B randomly chooses $x_i \in Z_q^*$, calculates $P_i = x_i P$, adds $\{PID_i, x_i, P_i\}$ to list L_{sk} and returns x_i to A_1.

Public key replacement query: When A_1 wants to replace the original public key P_i of PID_i with a new public key $P_i^{'}$, if the list L_{sk} contains the identity PID_i, B sets $P_i = P_i^{'}$, $x_i = \perp$; Otherwise, B sets $P_i = P_i^{'}$, $x_i = \perp$,and adds it to L_{sk}.

Signature query: When B receives a signature query of identity-message-public key pair PID_i, m_i, P_i from A_1, B operates as follows:

1) if $PID_i \neq PID^*$, B chooses a random number $r_i \in Z_q^*$, calculates $R_i = r_i p$; B inquires the list L_{ppk}, H_2, H_3, H_4 and L_{sk} to get d_i, h_i, f_i, g_i and x_i, calculates $V_i = h_i r_i + x_i f_i + d_i g_i$, generates the signature $\sigma_i = R_i, V_i$ and returns it to the adversary A_1;
2) Otherwise, B gives up and terminates the simulation.

Forgery phase: After polynomial times of the above queries, A_1 outputs a forged aggregate signature $\sigma = R, V$ of the identity-message-public key pair PID_i, m_i, P_i $1 \leq i \leq n$, in which at least one of these identities PID_i $1 \leq i \leq n$ is equal to the challenging identity PID^*.

If the signature is successfully forged, the forged signature must satisfy the verification equation: $VP = P_{pub} \sum_{i=1}^{n} g_i Q_i + R + \sum_{i=1}^{n} P_i f_i$. Then $V = \sum_{i=1}^{n} h_i r_i + x_i f_i + \sum_{i=1, i \neq *}^{n} d_i g_i + d_i^* x g_i$

Finally, B outputs $x = (d_i^* g_i)^{-1} [V - \sum_{i=1}^{n} h_i r_i + x_i f_i - \sum_{i=1, i \neq *}^{n} d_i g_i]$ as the solution to the DLP problem.

Then the probability of B's success is analyzed. First define the following events:

1) E_1 is the event that at least one identity PID_i $1 \leq i \leq n$ doesn't execute partial key generation query;
2) E_2 is the event that B dose not exit during the single signature query.

3) E_3 is the event that the forgery phase has not been terminated, that is, the forged aggregate signature contains the challenging identity PID^* in the forgery phase.

The probability of E_1 is $\Pr[E_1] \geq \frac{1}{n}\left(1-\frac{q_{ppk}}{2^{\ell}}\right)$. In the case of E_1, the probability of E_2 is $\Pr[E_2 \middle| E_1] \geq (1-\theta)^{q_s}$, the probability of E_3 is $\Pr[E_3] \geq \theta$.

During the entire simulation, the probability that B does not terminate is at least $\frac{1}{n}\left(1-\frac{q_{ppk}}{2^{\ell}}\right)(1-\theta)^{q_s}\theta$. Because $\theta \in [\frac{1}{q_s+n}, \frac{1}{q_s+1}]$, when q_s is large enough, $(1-\theta)^{q_s}$ equals to $\frac{1}{e}$. Therefore, the probability that B does not terminate during the simulation is $\frac{1}{ne(q_s+n)}\left(1-\frac{q_{ppk}}{2^{\ell}}\right)$.

In summary, if an adversary can break down the new aggregate signature scheme in this article with non-negligible advantages ξ, then B can successfully solve the DLP difficulty problem with the advantages $Adv[B] \geq \frac{1}{ne(q_s+n)}\left(1-\frac{q_{ppk}}{2^{\ell}}\right)\xi$.

Theorem 3 Under the random oracle model, if there is an adversary A_2, who can break the unforgeability of the new aggregate signature scheme with non-negligible advantages ξ after making adaptive chosen message and identity attack queries in polynomial times, then there is a distinguisher B who can take polynomial times to solve a DLP difficulty problem with non-negligible advantages $Adv[B] \geq \frac{1}{ne(q_s+n)}\left(1-\frac{q_{sk}}{2^{\ell}}\right)\xi$ (wherein, q_{sk} and q_s are the maximum number of secret value query and single signature query respectively, n is the user number of the aggregate signature scheme.)

The proof process of Theorem 3 is similar to Theorem 2, so the proof process is omitted.

5 Discussion

5.1 Correctness analysis

$$
\begin{aligned}
VP &= (V_1+V_2+\cdots+V_n)P \\
&= P\sum_{i=1}^{n} d_i g_i + P\sum_{i=1}^{n} h_i r_i + P\sum_{i=1}^{n} x_i f_i \\
&= P\sum_{i=1}^{n} sQ_i g_i + \sum_{i=1}^{n} h_i R_i + \sum_{i=1}^{n} P_i f_i \qquad (2) \\
&= P_{pub}\sum_{i=1}^{n} Q_i g_i + \sum_{i=1}^{n} h_i R_i + \sum_{i=1}^{n} P_i f_i
\end{aligned}
$$

$$= P_{pub}\sum_{i=1}^{n} Q_i g_i + R + \sum_{i=1}^{n} P_i f_i$$

Since the equation $VP = P_{pub}\sum_{i=1}^{n} g_i Q_i + R + \sum_{i=1}^{n} P_i f_i$ holds, the verification equation of the new scheme is correct.

5.2 Security and performance analysis

The security of the existing VANET-based certificateless aggregate signature scheme is compared with the scheme proposed in this paper. The results are shown in Tab. 2, √ denotes resistance to such attacks, × denotes the scheme could not resist such attacks.

Table 2: Security contrast of several schemes

Schemes	Attack of type I attacker	Attack of type II attacker
Wang et al.	√	×
Zhong et al.	√	×
Cui et al.	√	×
Ismaila et al.	√	×
Kumar et al. in *Journal of Supercomputing*	×	√
Kumar et al.	√	√
Kumar et al. in *Sustainable Computing*	√	√
Our scheme	√	√

It can be seen from Tab. 2 that the first five schemes listed in the table are not secure. The scheme Kumar et al. [Kumar, Kumari, Sharma et al. (2018)] published in the Journal of Supercomputing is not safe for the Type I attacker, the schemes designed by Wang et al. [Wang and Teng (2018); Cui, Zhang, Zhong et al. (2018); Ismaila and Sunday (2019) and Zhong, Shunshun, Cui et al. (2019)] are not safe for the Type II attacker.

Then, we analyze the performance of the new solution and make comparison with several recently proposed certificateless aggregate signature schemes. We use the method of He et al. [He, Zeadally, Xu et al. (2015)] to evaluate the computational performance of these schemes. For the scheme used bilinear pairing, the bilinear pairing on the security level of 80 bits is created as follows $\bar{e}: G_1 \times G_2 \to G_T$, G_1 is an additive group generated by a point $\bar{P}$ with order $\bar{q}$ on the super singular elliptic curve $\bar{E}: y^2 = x^3 + x \bmod \bar{p}$ with embedding degree 2, where $\bar{p}$ is a 512-bit prime number and $\bar{q}$ is a 160-bit Solinas prime number [Ogundoyin (2018)]. For the scheme used ECC, the ECC on the security level of 80 bits is created as follows: G is an additive group with order q which is constructed on a non-singular elliptic curve $E: y^2 = x^3 + ax + b \bmod p$, where p, q are two 160-bit prime numbers. The execution time of different cryptographic operations is listed in Tab. 3.

Table 3: Execution time of different cryptographic operations

Notations	Cryptographic operations	Execution times (ms)
T_{bp}	The execution time of a bilinear pairing operation $\bar{e}(P,Q)$	4.211
T_{bp-m}	The execution time of a scale multiplication operation $x \cdot \bar{P}$	1.709
T_{bp-a}	The execution time of a point addition operation $\bar{P} + \bar{Q}$ related to the bilinear pairing	0.0071
T_H	The execution time of a MapToPoint hash operation related to the bilinear pairing	4.406
T_{e-m}	The execution time of a scale multiplication operation $x \cdot P$ related to the ECC	0.442
T_{e-a}	The execution time of a point addition operation $P + Q$ related to the ECC	0.0018
T_h	The execution time of a One-way hash function operation	0.0001

Using the value in Tab. 3, we can calculate the operation time of each scheme. The calculation overhead of each scheme is listed in Tab. 4. *n* is the number of users of the aggregate signature, and *L* is the bit length of the element on the group.

Table 4: Contrast of computation cost of several schemes

Scheme	Single signature	Aggregate signature verification	The length of aggregated signature
Wang et al.	$4T_{bp-m}+T_h$=6.8361	$3T_{bp}$+3nT_{bp-m}+2nT_h=12.633+5.1272n	(n+1)L
Zhong et al.	$3T_{bp-m}+T_h$=5.1271	$3T_{bp}$+2nT_{bp-m}+2nT_h=12.633+3.4182n	2L
Cui et al.	$T_{e-m}+T_{e-a}+T_h$=0.4439	(n+2)T_{e-m}+2nT_{e-a}+2nT_h=0.884+0.4458n	2L
Ismaila et al.	$3T_{e-m}$+2T_{e-a}+3T_h=1.3299	$2T_{e-m}$+nT_{e-a}+nT_h=0.884+0.0019n	2L
Kumar et al. in *Journal of Supercomputing*	$4T_{bp-m}+T_H$+2T_{bp-a}+2T_h=11.2564	$4T_{bp}$+3nT_{bp-m}+2nT_H+3nT_h=16.844+13.9393n	(n+1)L
Kumar and Sharma	$4T_{bp-m}$+2T_h=6.8362	$3T_{bp}$+3nT_{bp-m}+3nT_h=12.633+5.1273n	(n+1)L
Kumar et al. in *Sustainable Computing*	$3T_{bp-m}+T_h$=5.1271	$3T_{bp}$+nT_{bp-m}+2nT_h=12.633+1.7092n	(n+1)L
Our scheme	T_{e-m}+3T_h=0.4423	(n+2)T_{e-m}+3nT_h=0.884+0.4423n	2L

We have found from Tab. 2 that the first five schemes are not secure and therefore only the last three schemes are suitable for practical application. Although Kumar et al.'s scheme [Kumar and Sharma (2018)] and Kumar et al.'s scheme [Kumar, Kumari, Sharma et al. (2018)] which is published in Sustainable Computing are safe, but it could be seen from Tab. 4 that their computational overhead is obviously larger than that of our scheme. Moreover, the aggregate signature length of the new scheme is fixed as 2L, while that of the other two schemes [Kumar and Sharma (2018); Kumar, Kumari, Sharma et al. (2018)] is (n+1) L. Therefore, compared with the existing schemes in terms of storage overhead, the new scheme also has obvious advantages.

6 Conclusion

In VANET, the secure authentication of information transmitted between vehicles and vehicles, between vehicles and roadside infrastructures has been a research hotspot in the field of information security. Aiming at the shortcomings in the existing certificateless aggregate signature schemes in VANET, we propose a new scheme. The new solution does not use bilinear pairing operation, and the length of aggregate signature is constant which does not increase as the number of user increases. The new solution is secure under the attack of Type I and Type II attacker, and has lower computation, communication and storage overhead, which is suitable for resource-constrained VANET. The work in this manuscript provides ideas to design more secure and efficient certificateless aggregate signature scheme in VANET in the next step.

Acknowledgement: This work was supported by the National Science Foundation of China (No. 61872448) and the Natural Science Basic Research Plan in Shanxi Province of China (No. 2018JM6017). The authors are very grateful to the referees for their detailed comments and suggestions regarding this paper.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Al-Riyami, S. S.; Paterson, K. G. (2003): Certificateless public key cryptography. *Advances in Cryptology-ASIACRYPT*, pp. 452-473.

Boneh, D.; Gentry, C.; Lynn, B.; Shacham, H. (2003): Aggregate and verifiably encrypted signatures from bilinear maps. *Advances in Cryptology-EUROCRYPT*, pp. 416-432.

Cao, X.; Kou, W.; Du, X. (2010): A pairing-free identity-based authenticated key agreement scheme with minimal message exchanges. *Information Sciences*, vol. 180, no. 6, pp. 2895-2903.

Chen, H.; Wei, S. M.; Zhu, C. J.; Yang, Y. (2015): Secure certificateless aggregate signature scheme. *Journal of Software*, vol. 26, no. 5, pp. 1173-1180.

Chen, L.; Cheng, Z.; Smart, N. P. (2007): Identity-based key agreement prostocols from pairings. *International Journal of Information Security*, vol. 6, no. 4, pp. 213-241.

Cui, J.; Zhang, J.; Zhong, H.; Shi, R.; Xu, Y. (2018): An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks. *Information Sciences*, vol. 451, pp. 1-15.

Gong, Z.; Long, Y.; Hong, X.; **Chen, K. F.** (2007): Two certificateless aggregate signatures from bilinear maps. *Proceedings of the IEEE SNPD*, vol. 3, pp. 188-193.

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

Ismaila, A. K.; Sunday, O. O. (2019): An improved certificateless aggregate signature scheme without bilinear pairing for vehicular ad hoc networks. *Journal of Information Security and Applications*, vol. 44, pp. 184-200.

Kim, Y.; Lee, J. (2016): A secure analysis of vehicular authentication security scheme of RSUs in VANET. *Journal of Computer Virology and Hacking Techniques*, vol. 12, no. 3, pp. 145-150.

Kumar, P.; Kumari, S.; Sharma, V.; Li, X.; Arun, Kumar Sangaiah, A. et al. (2018): Secure CLS and CL-AS schemes designed for VANET. *Journal of Supercomputing*, vol. 75, no. 6, pp. 3076-3098.

Kumar, P.; Kumari, S.; Sharma, V.; Sangaiah, A. K.; Wei, J. et al. (2018): A certificateless aggregate signature scheme for healthcare wireless sensor network. *Sustainable Computing: Informatics and Systems*, vol. 18, pp. 80-89.

Kumar, P.; Sharma, V. (2018): On the security of certificateless aggregate signature scheme in vehicular ad hoc networks. *Soft Computing: Theories and Applications, Advances in Intelligent Systems and Computing*, vol. 583, pp. 715-722.

Malhi, A. K.; Batra, S. (2015): An efficient certificateless aggregate signature scheme for vehicular ad hoc networks. *Discrete Mathematics and Theoretical Computer Science*, vol. 17, no. 1, pp. 317-338.

Ogundoyin, S. O. (2018): An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular Ad-Hoc networks. *International Journal of Computer and Application*.

Shamir, A. (1976): Identity-based cryptosystems and signature schemes. *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654.

Shen, H.; Chen, J.; Shen, J.; He, D. (2016): Cryptanalysis of a certificateless aggregate signature scheme with efficient verification. *Security and Communication Networks*, no. 9, pp. 2217-2221.

Wang, D. X.; Teng, J. K. (2018): Probably secure certificateless aggregate signature algorithm for vehicular ad hoc network. *Journal of Electronics & Information Technology*, vol. 40, no. 1, pp. 11-17.

Wu, L. B.; Xu, Z. Y.; He, D. B.; Wang, X. M. (2018): New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment. *Security and Communication Networks*, vol. 2018.

Yang, X. D.; Wang, J. L.; Ma, T. C.; Li, Y. T.; Wang, C. F. (2018): A short certificateless aggregate signature against coalition attacks. *PLoS One*, vol.13, no. 12.

Zhang, H. (2016): Insecurity of a certificateless aggregate signature scheme. *Security and Communication Networks*, no. 9, pp. 1547-1552.

Zhong, H.; Han, S. S.; Cui, J.; Zhang, J.; Xu, Y. (2019): Privacy-preserving authentication scheme with full aggregation in VANET. *Information Sciences*, vol. 476, pp. 211-221.