Available online at http://www.cnki.net

The Journal of China Universities of Posts and Telecommunications

February 2018, 25(1): 85 – 94

http://jcupt.bupt.edu.cn

Efficient pairing-based batch anonymous authentication scheme for VANET

Song Cheng, Zhang Mingyue (✉), Peng Weiping

School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China

Abstract

To solve the efficiency problem of batch anonymous authentication for vehicular Ad-hoc networks (VANET), an improved scheme is proposed by using bilinear pairing on elliptic curves. The signature is jointly generated by roadside unit (RSU) node and vehicle, thus reducing the burden of VANET certification center and improving the authentication efficiency, and making it more difficult for attacker to extract the key. Furthermore, under random oracle model (ROM) security proof is provided. Analyses show that the proposed scheme can defend against many kinds of security problems, such as anonymity, man-in-the-middle (MITM) attack, collusion attack, unforgeability, forward security and backward security etc., while the computational overheads are significantly reduced and the authentication efficiency is effectively improved. Therefore, the scheme has great theoretical significance and application value under computational capability constrained Internet of things (IoT) environments.

Keywords bilinear pairing, anonymous authentication, privacy protection, vehicular Ad-hoc networks, random oracle model

1 Introduction

With the popularity of vehicles in modern society, parking, traffic congestion, traffic accidents and other related traffic problems occur frequently. More and more people are paying attention to the problems of traffic management, driving safety and traffic information exchange. In order to manage a large number of vehicles, intelligent transportation system (ITS) [1] has been widely used at home and abroad. The VANET [2] based on mobile Ad-hoc network (MANET) [3] has drawn much attention from enterprises and academia aimed to build the next generation transportation system. The vehicle can obtain information concerning real-time traffic, weather and entertainment by communicating with the RSU, thus improving the driving safety and experience in VANET. So, the application of vehicle network brings a great convenience to people.

However, there are some security threats in VANET. On the one hand, the inherent characteristics of VANET wireless communication often make the data easily to be monitored, altered and forged. On the other hand, since vehicles are located in open physical space, so privacy (such as driver's license number, identity, position, route or distance of driving) leakage may endanger the lives and property of drivers and passengers. So, user's privacy protection [4] becomes

Received date: 17-07-2017

Corresponding author: Zhang Mingyue,
E-mail: zhangmingyue0118@163.com

DOI: 10.19682/j.cnki.1005-8885.2018.0010

one of the most basic security requirements in VANET. The basic method of privacy protection is anonymous authentication. The computation overheads of traditional anonymous authentication algorithms are relatively large. In addition, the properties of wireless communication and the rapid change of the topology make the efficiency of anonymous authentication in VANET become people's top concern. Therefore, enhancing the security of the existing schemes and improving the efficiency of anonymous authentication turns out to be an urgent topic in researching privacy protection for VANET.

Now, many scholars have proposed some VANET anonymous authentication schemes [5 – 7], but most of them are based on traditional digital signature technology of public key infrastructure (PKI). The computation and storage overheads of these schemes are high, the performance requirements being strict. In order to solve the problems, the idea of batch authentication has attracted much attention in recent years. Shao et al. [8] proposed a threshold anonymous authentication protocol based on group signature, but it cannot realize nonrepudiation, what's more, the communication overheads remain quite high. In Ref. [9], Zhang et al. proposed an efficient batch verification scheme which is used to communicate between RSU and on board unit (OBU). In the scheme, RSU can simultaneously verify lots of vehicles and reduce the total time overheads, but the scheme is totally dependent on the anti-tampering device. To improve security and privacy, in Ref. [10], Chim et al. introduced a batch authentication protocol, in which, after executing a batch authentication, one vehicle can form a group with any other vehicle to communicate securely without the participation of RSU. But Horng et al. [11] confirmed that the SPECS scheme is unable to defend the impersonation attack, and attacker can disguise as a legitimate vehicle to issue fake messages and even communicate securely with other vehicles. Liu et al. [12] proposed a batch VANET anonymous authentication protocol in which the message cannot be forged, but the update problem of the members in VANET remains unsolved. Fiat designed a batch verification scheme based on the RSA scheme [13], and Harn proposed a digital signature algorithm based (DSA-based) batch verification scheme [14]. However, both of them only solve Type 1 attack. To overcome the shortcomings of the existing schemes, an improved batch anonymous authentication scheme for VANET based on bilinear pair is proposed.

The rest of paper is organized as follows: in Sect. 2 some preparation knowledge are introduced. The proposed protocol is described in detail in Sect. 3. In Sect. 4, the correctness, security and efficiency analyses of the proposed scheme are presented. The last section concludes the paper.

2 Preparation knowledge

2.1 VANET model

Different from the traditional Internet, VANET mainly adopts wireless communication mode, and the communication entity is vehicle. The system model includes three parties: trust authority (TA), RSU and vehicle unit OBU. There are two types of communication: communication between OBU and RSU and communication between vehicle and vehicle. The system network model is shown in Fig. 1.

1) TA

In order to ensure the normal operation of the

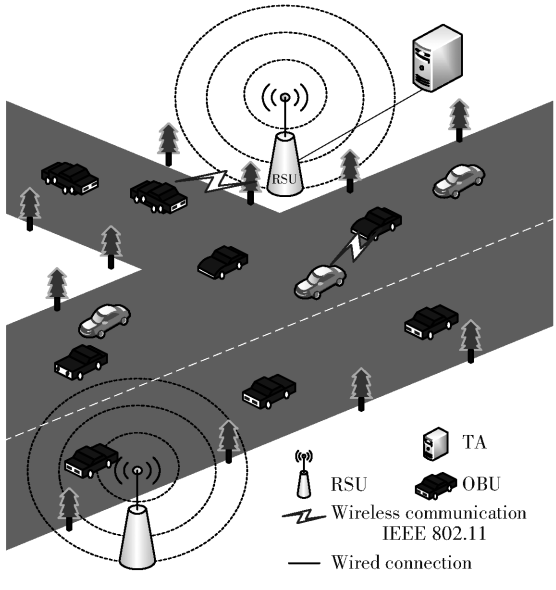

Fig. 1 VANET network model

system, TA is required to store the privacy information for all authenticated vehicles, generating the overall security parameters. In general, vehicle manufacturer or transportation management department acts as TA.

2) RSU

Similar to the access nodes of wireless sensor networks, RSU is the infrastructure installed on both sides of the road, capable of communicating wirelessly with vehicles. RSU communicates with vehicles using the dedicated short range communications (DSRC) protocol [15], which enables RSU to validate the request information sent by the vehicle.

3) Vehicle unit OBU

In VANET, each vehicle is equipped with wireless communication module OBU, through which vehicles can communicate with RSU or other vehicles equipped with OBU.

2.2 Bilinear pairing

Bilinear pairing [16] theory is the foundation of this paper. The following is a brief introduction to bilinear pairings.

Let G_1 be an addition cycle group of prime order q, G_2 be an multiplication cycle group of prime order q, a bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

1) Bilinear. $\forall P,R,Q \in G_1, \forall a,b \in Z_q, e(aP,bQ) = e(P,Q)^{ab}, e(P,Q+R) = e(P,Q)e(P,R), e(P+Q, R) = e(P,R)e(Q,R)$.

2) Non degeneracy. $\exists P,Q \in G_1$, satisfy $e(P,Q) \neq 1$.

3) Computability. $\forall P, Q \in G_1$, the existing algorithm can compute $e(P, Q)$ in the polynomial time.

4) Symmetry. $\forall P,Q \in G_1, e(P,Q) = e(Q,P)$.

2.3 Batch authentication

Assume every step of the scheme goes well, then the authentication parameter is $\text{Verify}(s_i, M_i, G_i)$, where $i \in \{1,2,\ldots,n\}$, the batch authentication parameter is $\text{BatchVerify}((s_1,M_1,C_1),(s_1,M_2,C_2),\ldots,(s_n,M_n,C_n))$. If that $(s_i,M_i,C_i) = 0$, then $\text{BatchVerify}((s_1,M_1,C_1),(s_2,M_2,C_2),\ldots,(s_n,M_n,C_n))$ is 0. That is, if each signature in n signatures is valid, the batch authentication succeeds, otherwise it means that one or more signatures are invalid, and the batch authentication fails.

According to the sources of the signature message, batch authentication is divided into three types:

Type 1 Batch authentication of different messages for the same user.

Type 2 Batch authentication of the same message for different users.

Type 3 Batch authentication of different messages for different users.

3 Anonymous authentication scheme based on bilinear pairings

The scheme includes five processes: the registration process, the initialization process, the signing process, the verification process and the update process.

3.1 Registration process

In the registration process, the vehicle node OBU and the RSU node send registration request to TA, and TA issues corresponding authentication information and generates system parameters. Specific steps are as follows:

Step 1 TA randomly generates a $m \times n$ matrix $\boldsymbol{A}$, $2 \leqslant m < n$ and a m-dimensional column vector $\boldsymbol{w}$ which satisfy $R(\boldsymbol{A}) = R(\overline{\boldsymbol{A}})$ (the rank of the coefficient matrix $\boldsymbol{A}$ is equal to the rank of the augmented matrix $\overline{\boldsymbol{A}}$) and $R(\boldsymbol{A}) < n$. Obviously, the linear equations $\boldsymbol{Ad} = \boldsymbol{w}$ have infinite solutions.

Step 2 TA generates a unique n dimension vector $\boldsymbol{d}_i$ for each corresponding vehicle node V_i. $\boldsymbol{d}_i$ satisfies $\boldsymbol{Ad}_i = \boldsymbol{w}$, and it is the true identity information of V_i. TA randomly selects a n dimension column vector $\boldsymbol{a}$, then calculate the identity of V_i

$$\text{ID}_i = \boldsymbol{a}^{\text{T}} \cdot \boldsymbol{d}_i \tag{1}$$

TA sends ID_i to V_i and sends $\boldsymbol{A}, \boldsymbol{D}$ and $\boldsymbol{w}$ to RSU through secure channel as shared secrets between RSU and TA.

Step 3 Let be an additive group of prime order q, G_2 denotes a multiplicative group of prime order q. Let P be a generator of G_1, RSU generates its own private key x_1 in finite field Z_q^* and a m dimension column

vector $\boldsymbol{D}$, and calculate another private key:

$$x_2 = (\boldsymbol{D}^{\mathrm{T}} \cdot \boldsymbol{w}) \bmod q \tag{2}$$

The public key is $K_{\mathrm{P1}} = x_1 P, K_{\mathrm{P2}} = x_2 P$.

Step 4 The common parameters of the system are: $(q, H, G_1, G_2, e, P, K_{\mathrm{P1}}, K_{\mathrm{P2}})$, where H: $\{0,1\}^* \rightarrow G_1$ is a one-way Hash function for cryptography and e is the bilinear pairing e: $G_1 \times G_1 \rightarrow G_2$.

3.2 Initialization process

In initialization process, RSU authenticates vehicle nodes and makes preparations for the next stage. Specific steps are as follows:

Step 1 Before communicating with other vehicles, vehicle V_i sends a request to RSU.

Step 2 After receiving the request from vehicle V_i, RSU randomly selects a m dimension column vector $\boldsymbol{Q}$ and calculates authentication parameter:

$$\boldsymbol{R} = \boldsymbol{Q}^{\mathrm{T}} \boldsymbol{A} \tag{3}$$

$$\boldsymbol{s} = \boldsymbol{Q}^{\mathrm{T}} \boldsymbol{w} \tag{4}$$

RSU sends $(t_1, \boldsymbol{R}, h(\boldsymbol{s} \parallel \mathrm{ID}_{R_p} \parallel t_1))$ to V_i, where ID_{R_p} is the identity of RSU, t_1 stands for the time associated with the message transmission.

Step 3 After receiving the message $(t_1, \boldsymbol{R}, h(\boldsymbol{s} \parallel \mathrm{ID}_{R_p} \parallel t_1))$, V_i calculates

$$\boldsymbol{r} = \boldsymbol{R} \cdot \boldsymbol{x}_i \tag{5}$$

And then verifies $h(\boldsymbol{r} \parallel \mathrm{ID}_{R_p} \parallel t_l) \stackrel{?}{=} h(\boldsymbol{s} \parallel \mathrm{ID}_{R_p} \parallel t_1)$, V_i sends $(t_2, h(\boldsymbol{r} \parallel \mathrm{ID}_{R_p} \parallel t_1 \parallel t_2))$ to RSU, where t_2 is the timestamp related to the message transmission.

Step 4 After receiving the message, RSU verifies $\boldsymbol{h}(r \parallel \mathrm{ID}_{R_p} \parallel t_1 \parallel t_2) = h(\boldsymbol{s} \parallel \mathrm{ID}_{R_p} \parallel t_1 \parallel t_2)$. If the verification is valid, RSU selects $y_i \in {}_R Z_q^*$, calculates $\rho_i = y_i P$, and sends ρ_i to V_i.

In the same communication range of RSU, when RSU communicates with vehicle for the first time, RSU must authenticate the vehicle's identity before conducting the message signature. After the authentication is executed, if the vehicle communicates with other vehicles, the vehicle and RSU need not execute the authentication again.

3.3 Signing process

At this stage, RSU and OBU jointly generate a signature, and the signature is used to authenticate between the vehicles. Detailed steps are as follows:

Step 1 V_i selects three random numbers u_i, r_{i1}, r_{i2}, lets $C_i = u_i \rho_i$, RID_i is $\mathrm{ID}_i t_2$, where RID_i is randomly generated by calculates:

$$\beta_i = r_{i1} H(\mathrm{RID}_i \parallel C_i \parallel M_i) + r_{i2} P \tag{6}$$

$$\gamma_i = r_{i1} u_i (\bmod q) \tag{7}$$

then V_i sends (β_i, γ_i) to RSU.

Step 2 After receiving (β_i, γ_i), RSU calculates:

$$T_i = x_1 \beta_i + x_2 y_i \gamma_i P \tag{8}$$

Then sends it to V_i.

Step 3 After receiving T_i, V_i calculates:

$$S_i = r_{i1}^{-1} (T_i - r_{i2} K_{\mathrm{P1}}) \tag{9}$$

Finally, V_i gets the signature for message M_i: $\sigma_i = (S_i, C_i, \mathrm{RID}_i, M_i)$. The signature process is shown in Fig. 2.

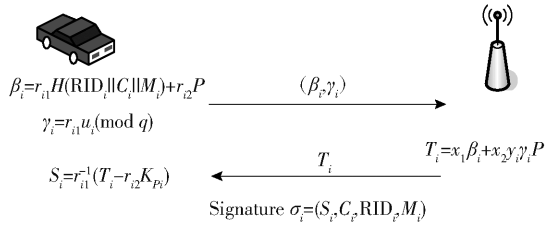

Fig. 2 Signature generation process

3.4 Verification process

At this stage, the verification is executed between vehicles. It is divided into single vehicle verification and batch verification.

1) Single vehicle verification

If vehicle A wants to communicate with vehicle B, A first sends its own signature to B, then B verifies

$$e(S_i P) \stackrel{?}{=} e(H(\mathrm{RID}_i \parallel C_i \parallel M_i), K_{\mathrm{P1}}) e(C_i, K_{\mathrm{P2}}) \tag{10}$$

If it is valid, the identity of vehicle A is legal, and vehicle B accepts the subsequent messages. Otherwise, vehicle B refuses them. The verification process is shown in Fig. 3:

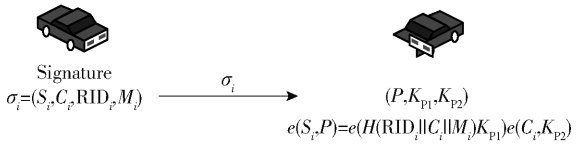

Fig. 3 Verification process

2) Batch verification stage

The signature is jointly generated by RSU and V_i.

RID_i is randomly generated by V_i, C_i is a random attribute generated by RSU. S_i is the final signature. So, each signature is unique. The specific verification is as follows:

Given the signature $\sigma_1 = (S_1, C_1, \mathrm{RID}_1, M_1), \sigma_2 = (S_2, C_2, \mathrm{RID}_2, M_2), \ldots, \sigma_i = (S_i, C_i, \mathrm{RID}_i, M_i), \ldots, \sigma_n = (S_n, C_n, \mathrm{RID}_n, M_n)$ (the $M_1, M_2, \ldots, M_n$ may be the same or different). If the equation

$$e\left(\sum_{i=1}^{n} S_i, P\right) = e\left(\sum_{i=1}^{n} H(\mathrm{RID}_i \| C_i \| M_i), K_{\mathrm{P1}}\right) \cdot e\left(\sum_{i=1}^{n} C_i, K_{\mathrm{P2}}\right) \tag{11}$$

is valid, then the signature is accepted.

3.5 Update process

If a member wants to withdraw from the group, the public key K_{P2} will change. Known equation group:

$$\left.\begin{aligned} \boldsymbol{A}\boldsymbol{d}_1 &= \boldsymbol{w} \\ \boldsymbol{A}\boldsymbol{d}_2 &= \boldsymbol{w} \\ &\cdots \\ \boldsymbol{A}\boldsymbol{d}_n &= \boldsymbol{w} \end{aligned}\right\} \tag{12}$$

Given $\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_n$, to get new $\boldsymbol{A}$ and $\boldsymbol{w}$. $\boldsymbol{A}$ is an $m \times n$ dimension matrix and $\boldsymbol{w}$ is m dimension vector. The number of unknown variables in the equation group is $m \times n + m$, but the number of equations is only $m \times n$. Obviously, there are infinite solutions for $\boldsymbol{A}$ and $\boldsymbol{w}$. If a member revokes or a new member joins, the register server can recalculate $\boldsymbol{A}$ and $\boldsymbol{w}$ by the existing vehicle node $\boldsymbol{d}_i$. Then the register server sends $\boldsymbol{A}$ and $\boldsymbol{w}$ to RSU. Finally, RSU recalculates K_{P2} and distributes it to group members. If a vehicle revokes from a group, K_{P2} in the Eqs. (10) and (11) will be updated. So, the in-group and out-group vehicles cannot be authenticated. The update process is shown in Fig. 4.

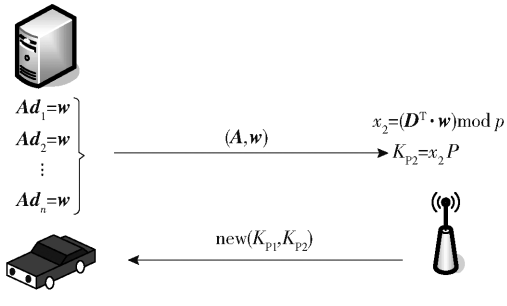

Fig. 4 Update process

4 Scheme analysis

In this section we present the correctness, security and efficiency analyses of the proposed scheme.

4.1 Correctness analysis

The correctness of single vehicle authentication and the correctness of batch certification are proved.

4.1.1 The correctness of single vehicle authentication

In single vehicle verification process, the validity of the signature is determined by judging whether the verification is right.

Because:

$$\begin{aligned} e(S_i, P) &= e(r_{i1}^{-1}(T_i - r_{i2}K_{\mathrm{P1}}), P) = \\ &\quad e(r_{i1}^{-1}(x_1\beta_i + x_2 y_i \lambda_i P - r_{i2}K_{\mathrm{P1}}), P) = \\ &\quad e(x_1 H(\mathrm{RID}_i \| C_i \| M_i) + x_2 y_i u_i P, P) = \\ &\quad e(x_1 H(\mathrm{RID}_i \| C_i \| M_i), P)\, e(x_2 y_i u_i P, P) = \\ &\quad e(H(\mathrm{RID}_i \| C_i \| M_i), x_1 P)\, e(y_i u_i P, x_2 P) = \\ &\quad e(H(\mathrm{RID}_i \| C_i \| M_i), K_{\mathrm{P1}})\, e(C_i, K_{\mathrm{P2}}) \end{aligned}$$

So, it is correct.

4.1.2 The correctness of batch vehicle authentication

In batch verification, the signature's validity is determined by judging whether the verification Eq. (11) is right.

Because:

$$\begin{aligned} e\left(\sum_{i=1}^{n} S_i, P\right) &= e(r_{i1}^{-1}(T_1 - r_{i2}K_{\mathrm{P1}}) + r_{i1}^{-1}(T_2 - \\ &\quad r_{i2}K_{\mathrm{P1}}) + \ldots + r_{i1}^{-1}(T_n - r_{i2}K_{\mathrm{P1}}), P) = \\ &\quad e(r_1^{-1}(x_1\beta_1 + x_2 y_1 \lambda_1 P - r_2 K_{\mathrm{P1}}) + \\ &\quad r_1^{-1}(x_1\beta_2 + x_2 y_2 \lambda_2 P - r_2 K_{\mathrm{P1}}) + \ldots + \\ &\quad r_1^{-1}(x_1\beta_n + x_2 y_n \lambda_n - \\ &\quad r_2 K_{\mathrm{P1}}), P) = e(x_1 H(\mathrm{RID}_1 \| C_1 \| M_1) + \\ &\quad x_1 H(\mathrm{RID}_2 \| C_2 \| M_2) + \ldots + \\ &\quad x_1 H(\mathrm{RID}_n \| C_n \| M_n) + x_2 y_1 u_1 P + \\ &\quad x_2 y_2 u_2 P + \ldots + x_2 y_n u_n P, P) = \\ &\quad e\left(x_1 \sum_{i=1}^{n} H(\mathrm{RID}_i \| C_i \| M_i), P\right) \cdot \\ &\quad e\left(\sum_{i=1}^{n} x_2 y_i u_i P, P\right) = \\ &\quad e\left(\sum_{i=1}^{n} H(\mathrm{RID}_i \| C_i \| M_i), x_1 P\right) \cdot \\ &\quad e\left(\sum_{i=1}^{n} y_i u_i P, x_2 P\right) = \end{aligned}$$

$$e\left(\sum_{i=1}^{n} H(\mathrm{RID}_i \parallel C_i \parallel M_i), K_{\mathrm{P1}}\right) \cdot$$
$$e\left(\sum_{i=1}^{n} C_i, K_{\mathrm{P2}}\right)$$

So, it is correct.

4.2 Security analysis

4.2.1 Anonymity

Suppose η as the symbol for the proposed scheme, the challenger as A, B_0 and B_1 denote two trusted vehicle users, the signer RSU is ζ.

Definition 1 The link game

Step 1 Challenger A generates public and private key pairs (SK, PK) by key generation algorithm KeyGen(k), meanwhile, gets the system's public parameters $(q, H, G_1, G_2, e, P, K_{\mathrm{P1}}, K_{\mathrm{P2}})$.

Step 2 The challenger chooses two completely different messages M_0 and M_1.

Step 3 Select the random bit $b \in \{0,1\}$, then M_b send M_{1-b} and to B_0 and B_1 secretly, b is not public for the challenger.

Step 4 The signer ζ performs the signature scheme with B_0 and B_1 respectively.

Step 5 If B_0 and B_1 output two valid signatures δ_b and δ_{1-b} corresponding to message M_0 and M_1 respectively, then δ_b and δ_{1-b} will be sent to the challenger in random order. Otherwise return $\perp$ to the challenger.

Step 6 Challenger guesses that δ_b comes from b', if $b' = b$, the challenger wins the game.

This article defines the advantages of the challenger winning the game as: $A_{\eta,\mathrm{A}}^{\mathrm{Link}}(\mathrm{A}) = |2\Pr[b' = b] - 1|$, $\Pr[b' = b]$ represents the probability of $b' = b$.

Theorem 1 If challenger A wins the linked game using the signature scheme with a non-negligible probability, then the scheme satisfies unlinkability and anonymity.

A is the challenger for the link game in Definition 1, and if it receives $\perp$ in Step 5, then A cannot get any useful information, and $\Pr[b' = b] = 1/2$. This is equivalent to A's random guess.

In another case, we assume that the attacker A performs the scheme's signature and gets two signatures: $(S_0, C_0, \mathrm{RID}_0, M_0)$, $(S_1, C_1, \mathrm{RID}_1, M_1)$. $j \in \{0,1\}$, j as an instance of the signature scheme, and $(y_jP, \beta_j, \gamma_j, T_j)$ representing the parameters in the interaction process. In order to prove the unlinkability of the scheme, for arbitrary $\{(S, C, \mathrm{RID}, M)\} \in \{(S_0, C_0, \mathrm{RID}_0, M_0)\}$, $(S_1, C_1, \mathrm{RID}_1, M_1)\}$, and any $(y_jP, \beta_j, \gamma_j, T_j)$, $j \in \{0,1\}$, always exist (r'_{j1}, r'_{j2}, u'_j),

$$C = u'_j y_j P$$
$$\beta_j = r'_{j1} H(\mathrm{RID}_i \parallel C_i \parallel M_i) + r'_{j2} P$$
$$\gamma_j = r'_{j1} u'_j (\mathrm{mod}\ q)$$
$$T_j = x_1 \beta_j + x_2 y_j \gamma_j P$$

available:

$$\begin{aligned} S_i &= r'^{-1}_{j_1}(T_j - r'_{j2} K_{\mathrm{P1}}) = \\ &\quad r'^{-1}_{j_1}(x_1\beta_j + x_2 y_j \gamma_j P - r'_{j2} K_{\mathrm{P1}}) = \\ &\quad r'^{-1}_{j_1}(x_1 r'_{j1} H(\mathrm{RID}_i \parallel C_i \parallel M_i) + x_2 y_j u'_j P) = \\ &\quad x_1 H(\mathrm{RID}_i \parallel C_i \parallel M_i) + x_2 y_j u'_j P = \\ &\quad x_1 H(\mathrm{RID}_i \parallel C_i \parallel M_i) + x_2 C \end{aligned}$$

It can be concluded that:

$$\begin{aligned} e(S, P) &= e(r_{i_1}^{-1}(x_1\beta_i + x_2 y_i \lambda_i P - r_{i2} K_{\mathrm{P1}}), P) = \\ &\quad e(x_1 H(\mathrm{RID}_i \parallel C_i \parallel M_i) + x_2 y_i u_i P, P) \end{aligned}$$

4.2.2 MITM attack

In a MITM attack, the attacker maintains communication links with two parties that communicate with each other, and let two parties believe they are directly communicating with each other. Then the attacker obtains useful information for the purpose of attack. In this scheme, a random number will be generated in each communication between RSU and V_i, whereas the random number used by attacker in establishing connection with RSU (or V_i) is different from the random number generated in the communications between RSU and V_i. So, the attacker cannot establish a communication connection via MITM attack to achieve the purpose of attack.

4.2.3 Collusion attack

1) Vehicles collude to obtain the identity of another vehicle

Assume that V_i communicates with n vehicles in the same field, and those vehicles have received V'_i's signature. Collusion attack can be divided into two kinds:

Case 1 Send identical message to each vehicle. In this case the message M in each signature is the same,

assume that the signatures are $(S_1, C_1, \mathrm{RID}_1, M)$, $(S_2, C_2, \mathrm{RID}_2, M)$, ..., $(S_j, C_j, \mathrm{RID}_j, M)$, ..., $(S_n, C_n, \mathrm{RID}_n, M)$, where $j \in (1, n)$, $S_j = r_{j1}^{-1}(T_j - r_{j2}K_{\mathrm{P1}})$, $C_j = u_j\rho_j$.

In the formula $S_j = r_{j1}^{-1}(T_j - r_{j2}K_{\mathrm{P1}})$, $C_j = u_j\rho_j$, r_{j1}, r_{j2}, u_j are randomly generated in each signature process. The random parameters are irrelevant, and RSU generates different ρ_j for each vehicle. Therefore, according to the signature generated by each vehicle, the attacker cannot get any useful information and then cannot know the true identity of V_i.

Case 2 Send different messages to each vehicle. in this case, the message M in each signature is different, assume that the signatures are $(S_1, C_1, \mathrm{RID}_1, M_1)$, $(S_2, C_2, \mathrm{RID}_2, M_2)$, ..., $(S_j, C_j, \mathrm{RID}_j, M_j)$, ..., $(S_n, C_n, \mathrm{RID}_n, M_n)$, $j \in (1, n)$, $S_j = r_{j1}^{-1}(T_j - r_{j2}K_{\mathrm{P1}})$, $C_j = u_j\rho_j$. Same as Case 1, there are some irrelevant random numbers in each phase of the signature, and the random numbers are from RSU and V_i respectively. Even if some vehicles collude, they cannot get useful information and then cannot get the true identity of V_i.

2) RSUs collude to track the true identity of the vehicle

Because a temporary identity RID_i is used during the communication between V_i and RSU, RSU cannot get the true identity of the vehicle, even by collusion.

In summary, the proposed scheme is able to resist collusion attacks.

4.2.4 Unforgeability

A Hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$ satisfying the following properties is called a ROM [17].

1) Uniformity. The output of the oracle is evenly distributed in $\{0,1\}^n$.

2) Determinism. For the same input, the output value is the same.

3) Validity. Given an input x, the calculation of $H(x)$ can be done in the low order polynomial time with respect to the length x.

It is proved that the security of ROM is based on the three properties above.

In ROM, if an attacker can forge a valid signature in a polynomial time t with a probability ε that cannot be ignored, there exists a polynomial time algorithm which can solve the computational Diffie-Hellman (CDH) difficult assumption.

Definition 2 One-more forgery [18]

There is a signature scheme for any integer l is polynomial (k, k is a security parameter). $(l, l+1)$ forgery means that there is a probability polynomial time algorithm which can compute $l+1$ valid signatures with the probability that cannot be ignored after l interactions with the signer.

Definition 3 The chosen-target CDH assumption [19]

P is the generator of G with prime order q, (P, aP) is given to the adversary A, where $a \in_R Z_q$. A can query the following two kinds of oracles:

1) Target oracle

i) Randomly select Z in G.

ii) Z as output.

2) Help oracle

i) Given element $Z \in G$ as an input, calculate $V = aZ$.

ii) V as output.

A wins the game if A can output l pairs $\{(V_1, Z_1), (V_2, Z_2), \ldots, (V_l, Z_l)\}$, $q_{\mathrm{h}} < l \leqslant q_{\mathrm{t}}$, such that $V_i = aZ_i (1 \leqslant i \leqslant l)$, after making $q_{\mathrm{t}} T_1$ queries q_{h} and H_2 queries, $q_{\mathrm{h}} < l \leqslant q_{\mathrm{t}}$.

There exists no probabilistic polynomial-time adversary A which can win the above game with non-negligible probability.

It is shown that the scheme is secure under the random blind signature scheme.

Proof Assume that attacker A can solve chosen-target CDH problem in this scheme, and the other attacker F has the same ability as A. The scenes can be described as follows:

Initialization phase $(q, H, G_1, G_2, e, P, K_{\mathrm{P1}}, K_{\mathrm{P2}})$ is the system parameter of this scheme, $K_{\mathrm{P1}} = aP$, let (P, aP) be a challenge to chosen-target CDH assumption. Also, F is given the parameters x_2, $K_{\mathrm{P2}} = x_2P$. Attacker F is able to query the help oracle H_2 and the target oracle T_1 under chosen-target CDH assumption.

Oracle query phase F can access the target oracle T_1 to get a random element $Z \in G_1$, and the help oracle H_2 to obtain aZ for some input $Z \in G_1$, respectively, in the chosen-target CDH assumption. Then F will

simulate O_h and O_s oracle query.

A can make two kinds of oracle queries: Hash query from the oracle O_h and signing queries from oracle O_s. The detailed process is as follows:

1) Detect (M, RID, C)

Detect is a procedure used to check whether there exists a record with a prefix (M, RID, C) as the input, in the list L_h.

If there is a record prefixed by (m, RID, C), it will return 1. Otherwise, it returns 0.

2) O_h query

Attacker A queries O_h for the Hash value on the input (M, RID, C), F will call a detecting procedure to check whether (M, RID, C) has been queried or not.

If (M, RID, C) has been queried, retrieve Z from the list L_h by taking (M, RID, C) as the search index.

Otherwise, F will query T_1 to obtain a random element $Z \in G_1$ and stores (M, RID, C, Z) in L_h for preserving consistency.

Return Z to A.

3) O_s query

In order to get the signature, the attacker A uses β_1, γ_1 as input. F inputs β_1 to H_2 to get the output $T_1 = \alpha\beta_1$.

F calculates $T = T_1 + x_2 y_i \gamma_1 P$.

Send the output T to A.

Forgery and problem solving After q_r and q_s queries to O_h and O_s respectively. If A can output l valid signature-message triples $(S_1, C_1, \mathrm{RID}_1, M_1)$, $(S_2, C_2, \mathrm{RID}_2, M_2), \ldots, (S_l, C_l, \mathrm{RID}_l, M_l)$, $q_s < l \leqslant q_r$, then F can calculate $V_i = S_i - x_2 C_i = aZ_i, 1 \leqslant i \leqslant l$ and output l valid signatures $(V_1, Z_1), (V_2, Z_2), \ldots, (V_l, Z_l)$ under the chosen-target CDH assumption, and $q_h = q_s < l \leqslant q_r = q_t$, where q_h and q_t are the number of the queries to T_1 and H_2. This contradicts with the chosen-target CDH assumption, so this paper can meet the requirements of non-forgery.

4.2.5 Forward security and backward security

Forward security and backward security ensure that before and after the verification phase the information will not affect each other. Forward confidentiality means that even if attacker obtains the secret information of the current authentication, it cannot infer the relevant information of the previous authentication message. Backward confidentiality is on the contrary, even if attacker receives the current verification's relevant information, it cannot infer the following verification information to track the vehicle. That is, the user's current authentication information does not expose the user's authentication information beforehand and afterward.

In the scheme, the generation of authentication messages depends on the random characteristics which guarantee that each authentication message contains random parameters $C_i = u_i \rho_i$ is not identical in each authentication message. So, a malicious attacker who has obtained any information about the current signature verification process cannot infer the previous authentication information or the subsequent authentication information.

The security of the scheme is compared with the existing schemes [7-8,12], the results are shown in Table 1.

Table 1 Security performance comparison

Performance	Security scheme			
	In Ref. [7]	In Ref. [8]	In Ref. [12]	The proposed scheme
Authentication	√	√	√	√
Anonymity	√	√	√	√
Anti-MITM attack	-	-	-	√
Anti-collusion attack	-	-	√	√
Unforgeability	-	√	√	√
Renewable	-	√		√
Forward security	-	-	-	√
Backward security	-	-	-	√

The analyses show that the security is further improved, and such problems as the MITM attack, forward and backward security are solved, too.

4.3 Efficiency analysis

4.3.1 Computational complexity analysis

Let T_{mul} be the time costs for performing the point multiplication operation on elliptic curve, T_{par} be the time costs for executing a bilinear pair of operation, and T_{exp} be the time costs for performing a modular

exponentiation operation. Other operations are ignored here for being relatively simple and lower time consumption. As is shown in Table 2.

Table 2 Comparison of computational complexity

Scheme	Authenticate one message	Authenticate n messages
In Ref. [7]	$3T_{par}+2T_{mul}$	$3T_{par}+(n+1)T_{mul}$
In Ref. [8]	$10T_{par}+4T_{exp}$	$(n+6)T_{par}+4nT_{exp}$
In Ref. [12]	$2T_{par}+2T_{mul}$	$2T_{par}+(n+1)T_{mul}$
The proposed scheme	$3T_{par}$	$3T_{par}$

In the experiment of Ref. [20], the 2 GHz CPU 4 GB RAM processor was selected and analyzed in 100 random simulation operations. The average operation time was: T_{exp} is 0.6 ms, T_{par} is 1.6 ms. The computational complexity of the proposed scheme is compared with the existing schemes, as is shown in Fig. 5. With the increase of the number of certification messages, the advantage of the proposed scheme turns to be more and more obvious, for the time costs of authentication always keep constant.

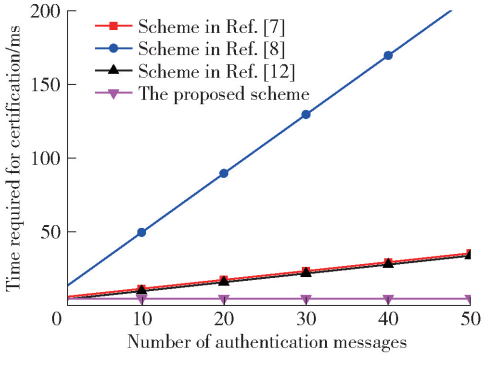

Fig. 5 Comparison of computational complexity

4.3.2 Communicational complexity analysis

Communicational complexity takes into account the number of bytes in communication. In VANET authentication schemes, the total communicational complexity mainly includes the identity information, signature, and the message itself.

Set the original message size as 20 B. In Ref. [7], the original message size is 20 B, signature is 60 B, pseudo-ID is 41 B, timestamp is 4 B, and ID is 4 B. In Ref. [8], the original message size is 20 B, signature is 826 B, timestamp is 4 B, and ID is 3 B. In Ref. [12], the signature size of the recoverable message is 53 B, and pseudo-ID is 42 B. In the proposed scheme, the original message size is 20 B, while signature is 60 B. As is shown in Table 3.

Table 3 Comparison of communicational complexity

Scheme	Authenticate one message/B
In Ref. [7]	20+60+41+4+4=129
In Ref. [8]	20+826+4+3=853
In Ref. [12]	53+42=95
The proposed scheme	20+60=80

This scheme is based on the elliptic curve cryptosystem. Compared with the traditional digital signature system based on the factoring of large integers and discrete logarithm, the signature length is relatively short. As can be seen from Table 3, this scheme has a clear advantage over other schemes.

5 Conclusions and further work

To solvethe low efficiency problem of anonymous authentication for VANET, an improved batch anonymous authentication scheme based on bilinear pairing is proposed. The correctness of the scheme can be proved, and analyses show that the scheme not only solves such security problems as authentication, unforgeability, anonymity, forward and backward security, MITM attack, and collusion attack, but also meets three kinds of batch authentication. Compared with the existing schemes, the security of the scheme is obviously enhanced, whereas the computational complexity and the space complexity is obviously reduced. So, the proposed scheme has great significance in theoretical research and practical applications for vehicle networking.

Despite the proposed scheme has made improvement and optimization on the basis of the existing schemes, with the rapid development of vehicle networking technology, it is difficult for anonymous authentication schemes under traditional VANET models to meet the requirements of privacy protection in vehicle anonymous authentication in various communication environments. Therefore, it remains to be tackled for

the author to further improve and optimize the proposed scheme so as to satisfy the growing demands of communication of VANET in various conditions.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61300124, 61300216), the Science and Technology Research Program of Henan Province (132102210123).

References

1. Giovanna C, Giuseppe M, Antonio P, et al. Transport models and intelligent transportation system to support urban evacuation planning process. IET Intelligent Transport Systems, 2016, 10(4): 279 – 286
2. Chouhan P, Kaushal G, Prajapat U. Comparative study MANET and VANET. International Journal of Advanced Trends in Computer Science and Engineering, 2016, 5(4): 16079 – 16083
3. Rizvi M, Pasha S, Tamrakar S. MANET parameter analysis and its impact on next generation network. Proceedings of the 2nd International Conference on Recent Trends in Computer Science and Electronics Engineering (RTCSE'17), Jan 2 – 3, 2017, Kuala Lumpur, Malasiya. 2017
4. Diep P T N, Yeo C K. A trust-privacy framework in vehicular ad hoc networks (VANET). Proceedings of the Wireless Telecommunications Symposium (WTS'16), Apr 18 – 20, 2016, London, UK. Piscataway, NJ, USA: IEEE, 2016: 7p
5. Yao L, Lin C, Wu G W, et al. An anonymous authentication scheme in data-link layer for VANETs. International Journal of Ad Hoc and Ubiquitous Computing, 2016, 22(1): 1 – 13
6. Huang J L, Yeh L Y, Chien H Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 2011, 60(1): 248 – 262
7. Shim K A. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874 – 1883
8. Shao J, Lin X D, Lu R X, et al. A threshold anonymous authentication protocol for VANETs. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1711 – 1720
9. Zhang C X, Lu R X, Lin X D, et al. An efficient identity-based batch verification scheme for vehicular sensor networks. Proceedings of the 27th Conference on Computer Communications (INFOCOM'08), Apr 13 – 18, 2008, Phoenix, AZ, USA. Piscataway, NJ, USA: IEEE, 2008: 246 – 250
10. Chim T W, Yiu S M, Hui L C K, et al. SPECS: secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks, 2009, 9(2): 189 – 203
11. Horng S J, Tzeng S F, Pan Y, et al. B-SPECS +: batch verification for secure pseudonymous authentication in VANET. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1860 – 1875
12. Liu Y W, He Z J, Zhao S J, et al. An efficient anonymous authentication protocol using batch operations for VANETs. Multimedia Tools and Applications, 2016, 75(24): 17689 – 17709
13. Fiat A. Batch RSA. Journal of Cryptology, 1997, 10(2): 75 – 88
14. Harn L. Batch verifying multiple DSA-type digital signatures. Electronics Letters, 1998, 34(9): 870 – 871
15. Tong Z, Lu H S, Haenggi M, et al. A stochastic geometry approach to the modeling of DSRC for vehicular safety communication. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5): 1448 – 1458
16. Lam T, Rietsch K. Total positivity, schubert positivity, and geometric satake. Journal of Algebra, 2012, 460: 284 – 319
17. Haitner I, Omri E, Zarosim H. Limits on the usefulness of random oracles. Journal of Cryptology, 2016, 29(2): 283 – 335
18. Cheon J H. Security analysis of the strong Diffie-Hellman problem. Advances in Cryptology: Proceedings of the 25th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'06), May 28 – Jun 1, 2006, St Petersburg, Russian. LNCS 4004. Berlin, Germany: Springer-Verlag, 2006: 11p
19. Herranz J, Laguillaumie F. Blind ring signatures secure under the chosen-target-CDH assumption. Proceedings of the 9th International Conference on Information Security (ISC'06), Aug 30-Sep 2, 2006, Samos Island, Greece. LNCS 4176. Berlin, Germany: Springer-Verlag, 2006: 117 – 130
20. Azees M, Vijayakumar P, Deboarh L J. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467 – 2476

(Editor: Wang Xuying)