Research on Identity-based Batch Anonymous Authentication Scheme for VANET

Cheng Song[1], Xinan Gu[1*], Lei Wang[1], Zhizhong Liu[1] and Yuan Ping[2]
1. School of Computer Science and Technology, Henan Polytechnic University
Jiaozuo, Henan,454000, People's Republic of China
2. School of Information Engineering, Xuchang University,
Xuchang 461000, People's Republic of China
[e-mail: songcheng@hpu.edu.cn]
[e-mail: 18839101173@163.com]
*Corresponding author: Xinan Gu

Received March 17, 2019; revised May 13, 2019; accepted May 22, 2019; published December 31, 2019

Abstract

To slove the security and efficiency problem of anonymous authentication in vehicular ad-hoc network (VANET), we adopt the bilinear pairing theory to propose an identity-based batch anonymous authentication scheme for VANET. The tamper-proof device in the on-board unit and the trusted authority jointly realize the anonymity of vehicle identity and the signature of messages, which further enhances the security of this scheme, as well as reduces the overhead of trusted authority. Batch authentication can improve the efficiency of anonymous authentication for VANET. Security and efficiency analyses demonstrate that this scheme not only satisfies such security properties as anonymity, non-forgeability and non-repudiation, but also has advantage in time and space complexity. Simulation results show that this scheme can achieve good performance in real-time VANET communication.

Keywords: VANET; identity-based; anonymous authentication; random oracle model

1. Introduction

With the rapid development of science and technology, the number of vehicles has been increasing explosively, and vehicles are used more and more widely and frequently. However, the traffic situation is not satisfactory, and a series of transportation problems keeps emerging, like parking difficulty, traffic jam, traffic accidents, etc. As communication safety and security of vehicles are brought into focus, consequently, Intelligent Transport System (ITS) management is drawing more attention in particular. As its core, VANET [1-2] is a mobile network with vehicles as nodes, which is not only able to effectively solve or alleviate the present traffic problems, but also bring convenience to people in navigation, information entertainment and vehicle security. This enriches people's lifestyles and improves the intelligent and safe environment of the transportation system.

Nevertheless, due to the operation scenes and the wireless communication mode of VANET, attackers can easily manipulate the communication channel to intercept, revise, replay and delete the transmitted messages, thus making VANET vulnerable in terms of privacy, conspiracy and forgery [3-5]. Under real circumstances, the vehicle or RSU should verify that the received message is valid and intact prior to the next step. What's worse, the attacker may tamper with the original information, give the receiver a wrong message, and then tempt other vehicles to perform illegal operation, thus disrupting the traffic order. For example, an opponent may pretend to be a fire truck to broadcast a traffic signal in order to make others give way. Therefore, the messages received need to be authenticated to defend their integrity, while vehicle users' identities must be anonymized to guarantee the security of individual privacy [6-8].

To be specific, Our contributions in the paper are as follows:

1. Considering the security problem of avoiding error information and the conflict between privacy and trusted authorities, we propose an identity-based batch authentication scheme to ensure the vehicle is capable of anonymous authentication, maintaining message integrity together with privacy and traceability. The solution can communicate in different scenarios of the vehicle network.

2. The proposed batch anonymous authentication scheme based on bilinear pairings satisfies these security properties like anonymity, non-forgeability and non-repudiation etc.

3. Since the proposed scheme requires a small constant number of pairings and point multiplication computations in the batch verification process, the speed can be accelerated while the calculation cost can be reduced in the authentication process.

The overall structure of the paper is as follows: In Section 2, we introduce the necessary basic knowledge; in Section 3， we describe the batch anonymous authentication scheme for VANETs; the correctness, security and efficiency of the scheme is analyzed in Section 4; Section 5 draws a conclusion of the paper.

2. Related Work

In recent years, Security and privacy issues in the vehicle network have been a hot topic of research, scholars home and abroad have done massive research, and have achieved a series of results. For example, Raya and Hubaux[9] devised an appropriate security architecture to

hide the user's true identity with an anonymous certificate. In this scheme, vehicles on the road are pre-installed with a public key certificate and an anonymous public/private key pairs to avoid mobile tracking. A set of security protocols were provided to protect the privacy, so that once malicious messages are detected, trusted authorities must spend a lot of time and energy in huge databases to find the real identity associated with the leaked anonymous public key. Lin et al. [10] proposed a scheme based on group signature. In this scheme, the identical group public key is stored together with unique private key in each vehicle. Vehicles receiving information can only confirm the authenticity of the message signature via group public key, while the vehicle transmitting the message has no flag information to be recognized by the receiver, which reduces the overhead of anonymous keys. However, the scheme increases the computational cost, and the calculation cost of the verifying group signature is higher than other schemes. Zhang et al. [11], proposed an IBV scheme in VANETs for V2I and V2V communications. This scheme uses one-time identity-based signature in order to effectively reduce the cost of authentication and transmission of public key certificates, as well as the total delay of message signature verification and it functions to solve the traffic accident disputes and realize the security of conditional privacy in vehicular networks.

Sun et al. [12] devised an identity-based security system for user's privacy in VANET, which could only conduct authentication on a one-by-one basis, but attackers would disavow when tracing identities; Lee et al. [13] devised a batch authentication scheme for VANET based on bilinear pairing, which improves the efficiency, but still fails to satisfy these two security properties: non-repudiation and non-forgeability, and may cause vehicle's genuine identity to be easily leaked; Bayat et al. [14] put forward a batch authentication scheme for VANET based on elliptic curve in order to improve the security, in which, however, the complex algorithms lead to excessive computational cost, thus affecting the timeliness of vehicular communication. Liu et al. [15] proposed an efficient anonymous authentication protocol using batch operations for VANETs, but this scheme is unable to resist conspiracy attack; Azees et al. [16] suggested an efficient anonymous authentication with conditional privacy-preserving scheme for VANET, in which the signature procedure requires excessive complexity in space and communications. Vijayakumar et al. [17] proposed a computationally efficient privacy preserving anonymous mutual authentication scheme for VANETs (CPAV) to verify the authenticity of OBUs without revealing their real identities for V2V communications in IoT. Islam et al. [18] presents a password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) protocol for VANETs. Nevertheless, neither of the above two schemes is simulated in a specific scenario.

In view of the shortcomings of the existing schemes, this paper proposes an identity-based batch anonymous authentication scheme for VANET based on the bilinear pairing theory, aiming to effectively solve the problems of privacy and time efficiency that exist in previous schemes, reduce the communication overhead, and resist multiple attacks. Finally, a comparative analysis of the efficiency of the existing programs shows that the newly-proposed program has higher authtication efficiency. Simulation is conducted to compare this scheme to previous schemes, and the results prove that this scheme is possessed with better security and authentication efficiency.

3. Preliminaries

3.1 VANET Model

As is shown in **Fig 1**, the VANET model consists of three parts: Trust Authority, Roadside

Unit and On-Board Unit. The specific function of each part is as follows:

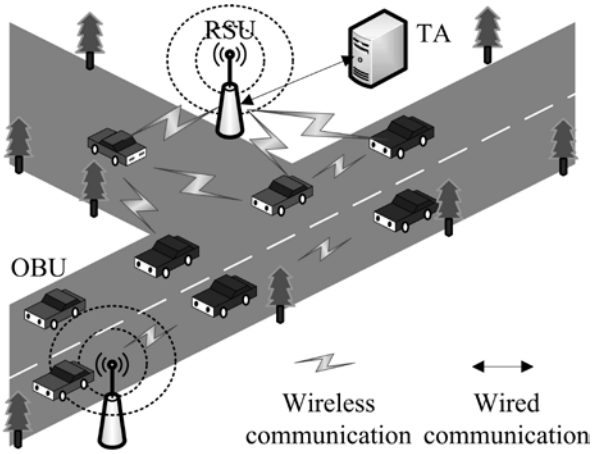

Fig. 1. VANET model

1) TA is the trusted authority management center of VANET, responsible for generating and publicizing security parameters, registering, managing and tracing vehicles. In general, TA is deployed in government agencies to manage traffic conditions.

2) RSU is the communication equipment installed on road sides, communicating with vehicles via DSRC protocol. It is responsible for network access of vehicles, information release of the management center, as well as sending and receiving the exchange messages of vehicles.

3) OBU is the wireless communication unit equipped for each vehicle in VANET, responsible for storing keys, and encrypting /decrypting messages. It communicates with RSU by DSRC protocol.

3.2 Bilinear pairing

Let G_1 and G_2 respectively be the addition and multiplication cyclic group of prime order q (q is a big prime number), then the bilinear pairing [19] $e: G_1 \times G_1 \to G_2$ satisfies the following properties:

1) Bilinearity: $\forall P, R, Q \in G_1$, $\forall a, b \in Z_q$, satisfies $e(aP_1, bP_1) = e(P_1, P_2)^{ab}$.

2) Non-degeneracy: $\exists P_1$, $P_2 \in G_1$, and $e(P_1, P_2) \neq 1$.

3) Computability: $\forall P_1$, $P_2 \in G_1$, there is efficient algorithm to compute $e(P_1, P_2)$.

4) Symmetry: $\forall P_1$, $P_2 \in G_1$, satisfies $e(P_1, P_2) = e(P_2, P_1)$.

3.3 Identity-based Cryptosystem

Firstly proposed by Shamir [20] in 1984, the identity-based encryption scheme attempts to use the unique identity of each user as the public key. This cryptosystem not only simplifies the key management in traditional public key cryptosystems, but also is more secure and efficient. In 2002, Malone-Lee [21] firstly adopted bilinear pairing to construct security model based on identity cryptosystem, and formalized the following definitions:

System initialization: input security parameter k, and the Trusted Authority (TA) outputs system parameter $params$ as well as master key r, then TA maintains the secrecy of master key r, and publicises system parameter $params$.

Key generation: input user's identiy ID, TA adopts master key r to compute user's private key SK, then transmit it to other users by a secure channel.

Signcryption: Signcryption is a cryptographic primitive that combines both the functions of digital signature and public key encryption in a logical single step , at lower computational costs and communication overheads than the traditional signature encryption approach. if ID_a signs and encrypts message M and send it to ID_b, SK_a, ID_b and M are input, then output signcryption message $\zeta = sig(M, SK_a, ID_b)$.

Decryption authentication: when receiving the signcryption message ζ sent by ID_a, ID_b decrypts and verifies this message; then input SK_b, ID_a and signcryption ζ, output $M = unsig(\zeta, SK_b, ID_a)$.

3.4 Elliptic curve cryptography algorithm

Elliptic Curve Cryptography (ECC) [22] is a public key cryptosystem based on algebraic curves, its security basis relying on point multiplication operation and Elliptic Curve Discrete Logarithm Problem (ECDLP).

Theorem 1 The elliptic curve in finite field: let p be a big prime number, F_p be the finite field of mode p, the elliptic curve equation in F_p is demonstrated as

$$y^2 = x^3 + ax + b \tag{1}$$

In which $a, b \in F_p$, and satisfies $4a^2 + 27b^3 \neq 0 \bmod p$; assume $x, y \in F_p$, if (x, y) satisfies equation (1), then (x, y) is the point of curve E, and $E(F_p)$ signifies the infinite point ∞ as well as all point sets in curve E, or is signified as $E_p(a, b)$.

Theorem 2 ECDLP: given a fixed point P with q as its order and the other point Q in elliptic curve, determine integer $x \in Z_q^*, 0 \le x \le q-1$, make $Q = xP \in G_1$ difficult.

Theorem 3 Computational Diffie- Hellman Problem (CDHP): given $xP, yP \in G_1$, in which $x, y \in Z_q^*$ is unknown integer, then computing $Q = xyP \in G_1$ is diffcult.

4. Identity-Based Batch Anonymous Authentication Scheme

The scheme proposed in this paper is composed of three phases: system initialization, anonymous identity generation and message signing, and message authentication.

4.1 System Initialization

In this phase, TA distributes system parameters for vehicle and RSU. The detatil is as follows:

Step 1: TA generates two cyclic groups G_1 and G_2 (order being q), in which G_1 is the addition cyclic group, G_2 the multiplication group, P and Q two generators of G_1; then randomly selects $r \in Z_q^*$ as the system's private key, and generates public key $P_{pub} = rP$.

Step 2: TA randomly selects three secure hash functions $h:\{0,1\}^* \to G_1$, $h_1:\{0,1\}^* \to Z_q^*$, $h_2:\{0,1\} \to Z_q^*$.

Step 3: TA secretly keeps r as the system's private key, and publishes $\{G_1, G_2, P, Q, q, e, P_{pub}, h(), h_1(), h_2()\}$ as system parameter.

4.2 Anonymous identity generation and message signing

In this phase, user registers and generates anonymous identity. The detail is as follows:

Step 1: Vehicle user submits to TA some identity information like UserName, E-mail, IDNumber, etc, to request registration.

Step 2: TA checks vehicle user's information to register, and distributes username R_{id}^i and password P_{wd}^i to this user, in which $R_{id}^i \in G_1$. Then R_{id}^i, P_{wd}^i and system's private key r are safely installed in the tamper-proofing device (TPD) of the vehicle.

Step 3: User inputs username R_{id}^i and password P_{wd}^i, TPD verifies the validity of user's information. If valid, the authentication succeeds; if not, cease the anonymous operation.

Step 4: TPD randomly selects $\sigma_i \in Z_q^*$, calculates vehicle's anonymous identity $ID = \{ID_1^i, ID_2^i\}$, and stores $\{\sigma_i, ID_i\}$ in TPD, in which, $ID_1^i = \sigma_i P$, $ID_2^i = R_{id}^i + h(\sigma_i P_{pub})$.

Step 5: TPD extracts system's private key r, calculates vehicle's private key $SK_i = rh_1(ID_1^i \| ID_2^i)$, and stores it together with $\{\sigma_i, ID_i\}$ in TPD. Vehicle user inputs M_i in TPD (M_i is the message that needs signature).

Step 6: After receiving message M_i, TPD calculates:

$$S_i = (SK_i + \sigma_i h_2(M_i \| T_i))Q \tag{2}$$

T_i is the time stamp of message signing. TPD delivers $\{ID_i, M_i, S_i, T_i\}$ as the signature of message M_i to vehicle.

4.3 Message authentication

In this phase, vehicle or RSU verifies the signature message it receives. It is divided into single vehicle authentication and batch authentication according to different amount of vehicle messages.

1) Single Vehicle Authentication

Step 1: Due to the timeliness of the message, when vehicle or RSU receives authentication message $\{ID_i, M_i, S_i, T_i\}$, inequality $\Delta T \overset{?}{\geq} T_r - T_i$ needs to be introduced, in which ΔT is the predicted time delay error, T_r the time point of receiving the message.

Step 2: Verify whether the inequality holds or not. If it holds, the signture message is valid; otherwise, the signature message is invalid, then ceases the authentication and discards the message.

Step 3: Verify the equation:

$$e(S_i, P) \overset{?}{=} e(h_1(ID_1^i \| ID_2^i)P_{pub} + h_2(M_i \| T_i)ID_1^i, Q) \tag{3}$$

If tenable, then the signature message is legal, and receive message m; if not, reject this message.

2）Batch Vehicle Authentication

In view of the authentication efficiency of signature messages in areas with large vehicle density and flow, this scheme realizes batch authentication of signature messages.

Step 1: Similar to single vehicle authentication, when receiving a signature message $\{ID_i, M_i, S_i, T_i\}$, firstly conduct timeliness authentication, i.e., verify whether $\Delta T \overset{?}{\geq} T_r - T_i$ holds or not. If it holds, the signature is valid; otherwise, discard this message.

Step 2: Based on small index testing method, RSU randomly selects n vectors $\{V_1, V_2 \cdots V_n\}$ for n signature messages that needs authentication in groups, so as to prevernt malicious user from replacing the signcryption value of the signature messages [8], in which $V_i \in [1-2^t]$, the value of t being a small integer.

Step 3: RSU computes:

$$A = e(\sum_{i=1}^{n} V_i S_i, P) \tag{4}$$

$$B = e(((\sum_{i=1}^{n} V_i h_1(ID_1^i \| ID_2^i))P_{pub} + \sum_{i=1}^{n} V_i h_2(M_i \| T_i) ID_1^i), Q) \tag{5}$$

then verify $A \overset{?}{=} B$, if tenable, accepts the signature.

5. Analyses and Simulation

In this section the scheme is analysed in terms of three aspects: correctness, security and efficiency.

5.1 Correctness Analysis

The correctness of this scheme is proved in single vehicle authentication and batch authentication.

In single vehicle authentication, on the premise of legal signature, the scheme's correctness depends on whether equation (3) is tenable or not, i.e., whether

$e(S_i, P) \overset{?}{=} e(SK_i + \sigma_i h_2(M_i \| T_i)Q, P)$ is tenable. Proof:

$$\begin{aligned}
&e(S_i, P) \\
&= e(SK_i + \sigma_i h_2(M_i \| T_i)Q, P) \\
&= e((rh_1(ID_1^i \| ID_2^i) + \sigma_i h_2(M_i \| T_i)Q), P) \\
&= e(Q, (rh_1(ID_1^i \| ID_2^i)P + \sigma_i h_2(M_i \| T_i)P)) \\
&= e(Q, h_1(ID_1^i \| ID_2^i)P_{pub} + h_2(M_i \| T_i)ID_1) \\
&= e(h_1(ID_1^i \| ID_2^i)P_{pub} + h_2(M_i \| T_i)ID_1^i, Q)
\end{aligned}$$

then the correctness is proved.

In batch authentication, on the premise of legal signature, the scheme's correctness depends on whether the equation $A \overset{?}{=} B$ is tenable, i.e., verify the equation

$$e(\sum_{i=1}^{n} V_i S_i, P) \overset{?}{=} e(((\sum_{i=1}^{n} V_i h_1(ID_1^i \| ID_2^i))P_{pub} + \sum_{i=1}^{n} V_i h_2(M_i \| T_i) ID_1^i), Q)$$

Proof:

$$
\begin{aligned}
& e(\sum_{i=1}^{n} V_i S_i, P) \\
&= e((\sum_{i=1}^{n} V_i r_i h_1(ID_1^i \| ID_2^i) + \sum_{i=1}^{n} V_i \sigma_i h_2(M_i \| T_i))Q, P) \\
&= e(Q, (\sum_{i=1}^{n} V_i r_i h_1(ID_1^i \| ID_2^i) + \sum_{i=1}^{n} V_i \sigma_i h_2(M_i \| T_i))P) \\
&= e(Q, \sum_{i=1}^{n} V_i r_i P h_1(ID_1^i \| ID_2^i) + \sum_{i=1}^{n} V_i \sigma_i P h_2(M_i \| T_i)) \\
&= e(Q, (\sum_{i=1}^{n} V_i h_1(ID_1^i \| ID_2^i))P_{pub} + \sum_{i=1}^{n} V_i h_2(M_i \| T_i) ID_1^i) \\
&= e((\sum_{i=1}^{n} V_i h_1(ID_1^i \| ID_2^i))P_{pub} + \sum_{i=1}^{n} V_i h_2(M_i \| T_i) ID_1^i, Q)
\end{aligned}
$$

Then, the correctness is proved.

5.2 Security Analysis

5.2.1 Non-forgeability

Theorem 1: If it is difficult to solve CDHP problem in polynomial time, this scheme is able to resist chosen-message attack in random oracle model, i.e., satisfies non-forgeability.

Proof: Let attacker be A, challenger be C. $\forall x, y \in Z_q^*$, x, y is unknown, and $P \in G_1$, (P, xP, yP) is known, then challenger C solves xyP, i.e., challenges CDHP problem. Assume attacker A is able to counterfeit the valid signature message $\{ID_i, M_i, S_i, T_i\}$, C performs the following steps:

Initialization: C resets system public parameter: $P_{pub} = xP, Q = yP$, then sends (P_{pub}, Q) to attacker A; meanwhile, construct and store three lists: L_h, L_{h1} and L_{h2}.

h-Oracle: C constructs list L_h of a tuple $\langle \alpha, \beta_h \rangle$, the initial stage being null. When C receives from A the query about message α, C checks whether record $\langle \alpha, \beta_h \rangle$ exists in the list L_h. If does, C replies to β_h; otherwise, C randomly selects $\beta_h' \in Z_q^*$, and adds $\langle \alpha, \beta_h' \rangle$ to the list, then replies to β_h'.

h_1-Oracle: challenger C keeps and maintains list L_{h1} of tuple $\langle ID_1^i, ID_2^i, \beta_{h1} \rangle$, with initial stage being null. When C receives from A query about message (ID_1^i, ID_2^i), C checks whether tuple $\langle ID_1^i, ID_2^i, \beta_{h1} \rangle$ exists in list L_{h1}. If does, C replies β_{h1}; otherwise, C randomly selects $\beta_{h1}' \in Z_q^*$, and adds $\langle ID_1^i, ID_2^i, \beta_{h1}' \rangle$ into the list, then replies to β_{h1}'.

h_2-Oracle: challenger C keeps and maintains list L_{h2} of tuple $\langle ID_1^i, ID_2^i, \beta_{h2} \rangle$, with initial stage being null. When C receives from A query about message (M_i, T_i), C checks whether tuple $\langle M_i, T_i, \beta_{h2} \rangle$ exists in the list. If does, answers β_{h2}; otherwise, C randomly selects $\beta_{h2}' \in Z_q^*$, and adds $\langle M_i, T_i, \beta_{h2}' \rangle$ into the list, then answers β_{h2}'.

Signature-Oracle: challenger C randomly generates $\gamma_i, h_{i,1}, h_{i,2} \in Z_q^*$, $ID_2^i \in G_1$, calculate $S_i = \gamma_i Q$, $ID_1^i = (\gamma_i P - h_{i,1} P_{pub}) / h_{i,2}$; add $\langle ID_1^i, ID_2^i, h_{i,1} \rangle$ and $\langle M_i, T_i, h_{i,2} \rangle$ to lists L_{h1} and L_{h2} to check whether $e(S_i, P) \stackrel{?}{=} e\left(h_1\left(ID_1^i \| ID_2^i\right) P_{pub} + h_2\left(M_i \| T_i\right) ID_1^i, Q\right)$ holds. If holds, the signature is valid; if not, the signature is invalid.

Output: A conducts two different queries, and in polynomial time C will get two valid signatures $\left\{ID_i, M_i^*, S_i, T_i\right\}$ and $\left\{ID_i, M_i^*, S_i^*, T_i^*\right\}$, while $S_i = \left(\gamma_i h_{i,1} + x h_{i,2}\right) Q$ and $S_i^* = \left(\gamma_i h_{i,1} + x h_{i,2}^*\right) Q$ can be satisfied. Thus C computes to get $\left(h_{i,2} - h_{i,2}^*\right)^{-1} \left(S_i - S_i^*\right) = xQ = xyP$, then CDHP problem is solved. However, this contradicts with the fact that CDHP problem is difficult, i.e., the scheme satisfies non-forgeability.

5.2.2 Non-repudiation

Non-repudiation is also called undeniability, i.e., in case of traffic accidents, proof can be obtained to verify and solve disputes as well as to ascertain the responsibility. When a certain vehicle has malicious acts, TA in this scheme is able to discover the true identity of this vehicle. The anonymous identity of the vehicle is $ID_i = \left(ID_1^i, ID_2^i\right)$, in which $ID_1^i = \sigma_i P$, $ID_2^i = R_{id}^i + h(\sigma_i P_{pub})$, TA adopts private key r to calculate $ID_2^i \oplus h\left(r \cdot ID_1^i\right)$ so as to discover the vehicle's tue identity R_{id}^i, i.e.:

$$\begin{aligned} & ID_2^i \oplus h\left(r \cdot ID_1^i\right) \\ &= ID_2^i \oplus h\left(\sigma_i \cdot r \cdot P\right) \\ &= ID_2^i \oplus h\left(\sigma_i \cdot P_{pub}\right) \\ &= R_{id}^i \end{aligned}$$

If the vehicle (with its identity discovered) denies its acts, this scheme introduces random vector V on the basis of small index testing method. When vehicles communicate with one another, a unique vector V is embedded in each signature. By means of batch authentication of signature messages, the malicious vehicle can not deny. Therefore, non-repudiation is satisfied.

5.2.3 Anonymity

The authentication scheme in this paper is recorded as ζ, the attacker as A, F_0 and F_1 denote two faithful vehicle users in the game.

Definition 1 Anonymity Game

Step 1: Attacker employs the key- generating algorithm to obtain public and private key pairs $\left(P_{pub}, r\right)$, and system's public parameter $\left\{G_1, G_2, P, Q, q, e, P_{pub}, h(), h_1(), h_2()\right\}$.

Step 2: Attacker selects two different messages m_0 and m_1.Select the random bit $b \in \{0,1\}$, then send m_b and m_{1-b} to F_0 and F_1. Plus, b is kept secret. F_0 and F_1 perform the proposed signature scheme ξ respectively.

Step 3: If F_0 and F_1 output two valid signatures τ_b and $\tau_{1\text{-}b}$ which are correspondent respectively with the message m_0 and m_1, then send τ_b and $\tau_{1\text{-}b}$ to attacker A in random order; otherwise, return invalid symbol $\perp$ to the attacker.

Step 4: Attacker A analyzes signature τ_b, outputs the guess b' of b, $b' \in \{0,1\}$. When $b' = b$, attacker A wins the game.

This article defines the advantage of attacker A winning the game as: $Adv_{\xi,A}^{Link}(A) = |2\Pr[b' = b] - 1|$, then $Pr[b' = b]$ represents the probability of $b' = b$.

Theorem 1: If attacker A is unable to use the signature scheme to win the anonymity game in polynomial time with a non-negligible probability, then the scheme satisfies anonymity.

A is the attacker in the anonymity game in Definition 1. If $\perp$ is received in step 5, then the message that A gets is invalid, and the probability of obtaining correct b is $\frac{1}{2}$. This is equivalent to the random guess of b.

Consider the other case: assume that attacker A completes the signature of the scheme and gets two signatures: (S_0, T_0, ID_0, M_0), (S_1, T_1, ID_1, M_1). Let $j \in \{0,1\}$, j as an instance of the signature scheme, (σ_j, P, SK_j) represents the parameter in the interaction process. To prove the anonymity of the scheme, for $\{(S,T,ID,M)\} \in \{(S_0,T_0,ID_0,M_0),(S_1,T_1,ID_1,M_1)\}$ and arbitrary parameter (σ_j, SK_j), $ID_1^i = \sigma_j P$, $ID_2^i = R_{id}^i + h(\sigma_j P_{pub})$, $SK_j = rh_1(ID_1^i \| ID_2^i)$, $j \in \{0,1\}$. Finally, get

$$\begin{aligned} S_i &= (SK_j + \sigma_j h_2(M_i \| T_i))Q \\ &= rh_1(\sigma_j P \| R_{id}^i \oplus h(\sigma_j P_{pub})) + \sigma_j h_2(M_i \| T_i)Q \\ &= rh_1(ID_1^i \| ID_2^i) + \sigma_j h_2(M_i \| T_i)Q \end{aligned}$$

So

$$\begin{aligned} & e(S,P) \\ &= e(SK_j + \sigma_j h_2(M_i \| T_i)Q, P) \\ &= e((rh_1(ID_1^i \| ID_2^i) + \sigma_j h_2(M_i \| T_i)Q), P) \\ &= e(h_1(ID_1^i \| ID_2^i)P_{pub} + h_2(M_i \| T_i)ID_1^i, Q) \end{aligned}$$

5.3 Efficiency Analysis

5.3.1 Computation Complexity

The computation complexity is compared with that of the representative schemes. Define T_p as the time for executing a single operation of bilinear pairing; T_{mp-bp} as the time for performing a single point multiplication operation in bilinear pairing; T_{mp-ec} as the time for performing a single point multiplication operation on elliptic curve; T_h as the time for conducting a hash computation; the time required to perform the exponentiation operation in G_1 is denoted as T_{ep}. The computational complexity in each scheme is shown in **Table 1** and **Table 2**. The operating system of this article is Windows 7, processor being intel i7 4GHz, and MIRACL encrypted database is applied to running a safe subgroup of 80-bit elliptic curves. The operation time: T_p is 4.21ms, T_{mp-bp} 1.71ms, T_{mp-ec} 0.44ms, T_h 4.41ms, and T_{ep} is 0.3ms.

Table 1. Execution time of single message authentication phase

Scheme	Total computation cost	Total execution time
In Ref.[13]	$3T_p + T_{mp-ec}$	13.07ms
In Ref.[14]	$3T_p + T_{mp-bp} + T_h$	18.75ms
In Ref.[15]	$2T_p + 2T_{mp-ec}$	9.3ms
In Ref. [16]	$2T_p$	8.42ms
In Ref.[17]	$2T_p + 2T_{ep} + T_h$	13.43ms
The proposed scheme	$2T_p + 2T_{mp-ec}$	9.3ms

Table 2. Execution time of batch message authentication phase

Scheme	Total computation cost	Total execution time
In Ref.[13]	$3T_p + T_{mp-ec}$	13.07ms
In Ref.[14]	$3T_p + nT_{mp-bp} + nT_h$	$6.12n + 12.63$ ms
In Ref.[15]	$2T_p + (n+1)T_{mp-ec}$	$0.44n + 8.86$ ms
In Ref. [16]	$(n+1)T_p$	$4.21n + 4.21$ ms
In Ref.[17]	$(1+n)T_p + 2nT_{ep} + nT_h$	$9.22n + 4.21$ ms
The proposed scheme	$2T_p + 2T_{mp-ec}$	9.3ms

As is shown in the **Table 1** and **Table 2**. In single signature authentication , the proposed scheme is obviously better than Ref.[13] Ref.[14] and Ref.[14], has similar time costs as Ref.[15], and is only slightly inferior to Ref. [16]. When it comes to batch signature authentication, the time costs in Ref.[14], Ref.[15],Ref.[16] and Ref.[17] increase with the increase of the quantity n of batch signature messages, while the time costs in this scheme and Ref.[13] is irrelevant to n, thus is apparently better than other schemes.

5.3.2 Communication complexity

Communication complexity refers to the traffic in communication, i.e., storage space, which is usually measured by byte. A single anonymous authentication scheme for VANET consists of signature message, pseudonym and other additional information. For example, in Ref.[13], signature message is 21 bytes, pseudonym 42 bytes, and timestamp 4 bytes; in Ref.[14], signature message is 42 bytes, pseudonym 234 bytes, timestamp 4 bytes; in Ref.[15], signature message is 53 bytes, pseudonym 42 bytes; in Ref.[16], signature message 60 bytes, pseudonym 40 bytes, timestamp 4 bytes; in Ref.[18], the size of the authentication message is 64 × 5 + 4 + 4 = 328 bytes; in the proposed scheme, signature message is 20 bytes, pseudonym 40 bytes, and timestamp 4 bytes. As is shown in **Table 4,** the proposed scheme has better communication complexity than other schemes.

Table 4. communication complexity comparison

scheme	storage space
In Ref.[13]	21+42+4=67B
In Ref.[14]	42+234+4=280B
In Ref.[15]	53+42=95B
In Ref. [16]	20+40+40+4=104B
In Ref. [18]	64×5+4+4=328B
The proposed scheme	20+40+4=64B

5.3.3 Simulation Analysis

The environment of simulation experiment in this scheme is as follows: operation system: Windows 10 (64 bit); CPU: Intel i5 processor; RAM: 4G; simulation software: NS-2.35, and wireless protocl is 802.11a. Assume the size of the simulation area as 1200m*1200m, the number of vehicular nodes is between 20-100, driving speed of vehicles is between 0-108km/h, and vehicular nodes are randomly distributed on the roads in the simulation area.

This simulation experiment verifies the scheme's efficiency and feasibility based on the rate of average message delay and lost. The rate of average message delay and loss message is denoted as AD and AL respectively.

$$AD = \frac{\sum_{i=1}^{N_V} \sum_{m=1}^{N_m^i} \left(T_{s\to m}^i + T_{t\to m\to r}^i + T_{r\to v\to m}^i \right)}{\sum_{i=1}^{N_v} N_m^i}$$

In which N_V is the number of vehicles in simulation area, N_m^i the amount of messages sent by vehicle i, $T_{s\to m}^i$ the signature time of vehicle i to message m, $T_{t\to m\to r}^i$ the time of sending message m to RSU from vehicle i, and $T_{r\to v\to m}^i$ is the time of RSU authenticating vehicle i.

$$AL = \frac{\sum_{i=1}^{N_V} N_m^i - \sum_{j=1}^{R_n} N_r^j}{R_n * \sum_{i=1}^{N_V} N_m^i}$$

In which R_n is the number of RSU, N_r^j the amount of messages received by the j th RSU. The simulation results are shown in **Fig. 2** and **Fig. 3**. In terms of average message delay, when the nodes is between 0-60, the proposed scheme is similar to other schemes; as the number of vehicular nodes increases, this scheme is apparently better than other schemes. When it comes to the rate of average messages loss, if nodes are between 0-20, this scheme is better than Ref.[14], Ref.[15], Ref.[16]and Ref.[18] and is similar to Ref.[13]; as the number of vehicular nodes increases, this scheme has advantage over other schemes.

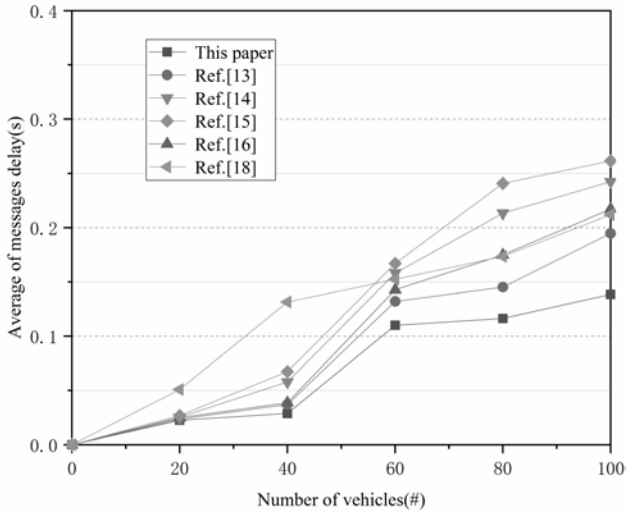

Fig. 2. The relationship between average message delay and vehicle nodes

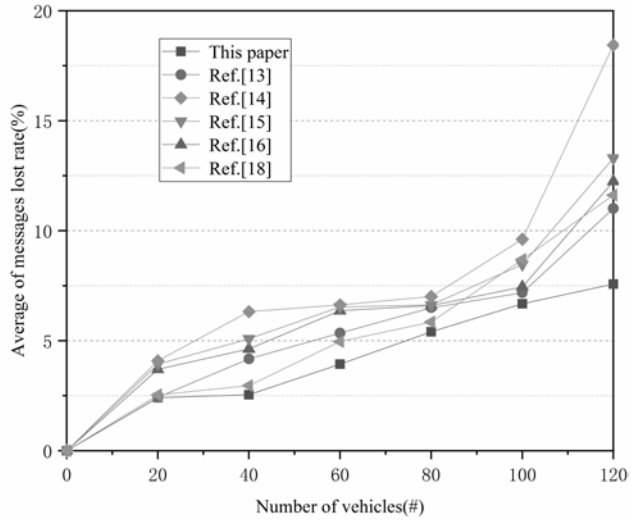

Fig. 3. The relationship between average message loss rate and vehicle nodes

6. Conclusions

Aiming at the problem of privacy protection and anonymous authentication efficiency in VANET, this paper proposes an identity-based batch anonymous authentication scheme based on the bilinear pairing property in elliptic curves and relevant problem assumptions. In this scheme, the anonymity of vehicle identity and the signature of messages are realized jointly by TPD in vehicular unit and TA, which not only enhances the security, but also reduces the computational overhead of TA. Random oracle model is employed to prove the scheme's anonymity and the non- forgeability of signature. Besides, the complexity of time and space of this scheme is also analysed, and simulation is also conducted to compare this scheme with the existing schemes based on the rate of average message delay and loss. The results demonstrate that the proposed scheme has certain advantage in terms of security, efficiency and feasibility.which makes it more suitable for deployment in VANET services and applications.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (61872126, 61772159, 61300216), the Program for Science & Technology Innovation Talents in Universities of He'nan Province (18HASTIT022) ; the Science and Technology Research Program of He Nan Province (182102110333, 172102310677). Doctoral Foundation of Henan Polytechnic University (B2012-057).

References

[1] R G Engoulou, M Bellaïche, S Pierre and A Quintero, "VANET security surveys," *Computer Communications* ,vol.44, pp. 1-13, 2014.Article (CrossRef Link).

[2] X Liu, Z Fang, L Shi. "Securing Vehicular Ad Hoc Networks," *International Conference on Pervasive Computing & Applications*, July.2007.Article (CrossRef Link).

[3] D He, S Zeadally, B Xu and X Huang, "An Efficient Identity-Based Conditional Privacy Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on*

Information Forensics & Security, vol. 10, no. 12, pp. 2681-2691, Dec. 2015. Article (CrossRef Link).

[4] J K Liu, T H Yuen, M H Au and W Susilo. "Improvements on an authentication scheme for vehicular sensor networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559-2564, April. 2014.Article (CrossRef Link).

[5] J Whitefield, L Chen, T Giannetsos, S Schneider and H Treharne, "Privacy-enhanced capabilities for VANETs using direct anonymous attestation," *Vehicular Networking Conference*, pp. 123-130, Feb. 2018.Article (CrossRef Link).

[6] Y Wang, H Zhong, Y Xu, J Cui and F Guo. "Efficient extensible conditional privacy preserving authentication scheme supporting batch verification for VANETs," *International Journal of Network Security*, vol. 9, no. 18, pp. 5460-5471, 2016.Article (CrossRef Link).

[7] C L Chen, J Shin, Y T Tsai, A Castiglione and F Palmieri, "Securing Information Exchange in VANETs by Using Pairing-Based Cryptography," *International Journal of Foundations of Computer Science*, vol. 28, no. 6, pp. 781-797, 2017.Article (CrossRef Link).

[8] C Zhang, R Lu, X Lin, P H Ho and X Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," in *Proc. of IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 246-250, 2008.Article (CrossRef Link).

[9] M Raya, J P Hubaux, "The security of vehicular ad hoc networks," in *Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 11-21, Nov. 2005. Article (CrossRef Link).

[10] X Lin, X Sun, P H Ho and X Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.Article (CrossRef Link).

[11] C Zhang, P H Ho and J Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851-1865, Nov. 2011. Article (CrossRef Link).

[12] J Sun, C Zhang, Y Zhang and Y Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Transactions on Parallel & Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, Jan. 2010.Article (CrossRef Link).

[13] C C Lee, Y M Lai. "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441-1449, Jan. 2013.Article (CrossRef Link).

[14] M Bayat, M Barmshoory, M Rahimi and M R Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1-11, Dec. 2014.

[15] Y Liu, Z He, S Zhao and L Wang, "An efficient anonymous authentication protocol using batch operations for VANETs," *Multimedia Tools & Applications*, vol. 75, no. 24, pp. 17689–17709 , Jun. 2016. Article (CrossRef Link).

[16] M Azees, P Vijayakumar and L J Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy Preserving Scheme for Vehicular AdHoc Networks," *IEEE Transactionson Intelligent Transportation Systems*, vol. 18, no. 9, pp. 1-10, Feb. 2017.Article (CrossRef Link).

[17] P Vijayakumara, V Changb, L J Deboraha, B Balusamy and P G Shynu, “Computationally Efficient Privacy Preserving Anonymous Mutual and Batch Authentication Schemes for Vehicular Ad Hoc Networks,” *Future Generation Computer Systems*, vol 78, pp. 943-955, Jan. 2018. Article(CrossRefLink)

[18] S H Islam, M S Obaidat, P Vijayakumar, E Abdulhay, F Li and M K C Reddy, “A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs,” *Future Generation Computer Systems*, vol 84, pp. 216-227, July. 2018. Article(CrossRefLink).

[19] F Brezing, A Weng, "Elliptic Curves Suitable for Pairing Based Cryptography," *Designs Codes & Cryptography*, vol. 37, no. 1, pp. 133-141, Oct. 2005.Article (CrossRef Link).

[20] A Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Proc. of Workshop on the theory and application of cryptographic techniques*, vol.196, no. 2, pp. 47-53, Aug. 1984. Article (CrossRef Link).

[21] L Chen, J Malone-Lee, "Improved identity-based signcryption," in *Proc. of International Workshop on Public Key Cryptography*, pp. 362-379, Jan. 2005.Article (CrossRef Link).

[22] Z Tong, H Lu, M Haenggi and C Poellabaure, "A Stochastic Geometry Approach to theModeling of DSRC for Vehicular Safety Communication," *IEEE Trans-actions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1448-1458, Feb. 2016.Article (CrossRef Link).

Cheng Song received his Ph.D. degree in Computer Science from the Beijing University of Posts and Telecommunications in 2011. He is now working as a lecture at the School of Computer Science and Technology in Henan Polytechnic University. His main research interests include Networking Security and Application, Privacy protection and Trusted Computing.

Xinan Gu is a graduate student at the School of Computer Science and Technology in Henan Polytechnic University. His main research interests include Networking Security and Application, Privacy Protection and Anonymous Authentication.

Lei Wang received his Ph.D. degree in control theory and engineering from Dalian University of Technology, China, in 2012. He is working as an associate professor in Henan Polytechnic University. His research interests include wireless Ad-hoc Networks, Embedded system, Networked control system, and Internet of things.

Zhizhong Liu received his Ph.D. degree in Computer Science from Hohai University in 2011. He did his post-doc at Harbin Institute of Technology from 2013 to 2017. He is currently an associate professor in Henan Polytechnic University. He has authored or coauthored more than 30 papers. His research interests include Service-oriented Computing and Artificial Intelligence.

Yuan Ping received his Ph.D. degree in information security from Beijing University of Posts and Telecommunications in 2012. He is an associate professor with Xuchang University and a visiting scholar with the School of Computing and Informatics, University of Louisiana at Lafayette. He was a visiting scholar with the Department of Computing Science, University of Alberta. His research interests include machine learning, public key cryptography, data privacy and security, cloud and edge computing.