An Improved RSU-based Authentication Scheme for VANET

Hongyuan Cheng, Yining Liu

Guangxi Key Laborabory of Trusted Software, School of Computer and Information Security,
Guilin University of Electronic Technology, China
hycheng649@163.com, ynliu@guet.edu.cn

Abstract

Vehicular Ad-hoc Networks (VANETs) plays an important role in improving traffic management. Due to the openness of wireless channels, how to ensure the security and privacy of communication has become a huge challenge for the VANETs. The tamper-proof based scheme has been proposed to solve the above problems, which requires stores system master key in the tamper-proof device (TPD) of vehicles to generate pseudonyms and signatures. For the sake of communication security, the system master key must be updated regularly. Recently, in order to update the master key more efficiently, the NERA scheme is proposed for secure vehicle communications. However, the NERA scheme is vulnerable against some security threats, such as impersonation attacks, identity privacy threats. Accordingly, an improved RSU-based authentication scheme with Elliptic Curve Cryptosystem (ECC) is proposed, in which the security of the proposed scheme is enhanced greatly to resist the security threats during pseudonym and private key generation process. Compared with the previous NERA, the improved scheme proved to be more secure and efficient.

Keywords: VANETs, Anonymous authentication, ECC, Conditional privacy, Batch verification

1 Introduction

Vehicle facilitates people's daily life; meanwhile, it brings us many problems, such as traffic congestion, traffic accidents, and complicated traffic conditions [1]. Therefore, it is necessary to design intelligent transportation systems (ITSs) in order to manage urban traffic effectively. As an important part of the ITSs, VANETs have attracted extensive attention from academia and industry [2]. The classic model of VANETs mainly consists of three parts: On-Board Units (OBU), Trust Authority (TA) and Roadside Unit (RSU). As a trusted third party, TA is responsible for registration of vehicles and RSUs and tracking the real identity of malicious vehicles. RSU acts as a bridge between TA and OBU. Each vehicle is equipped with OBU, which can broadcast messages to nearby vehicles and RSUs. The main goal of the VANETs is to improve road safety and driving conditions by sharing information among the vehicles [3].

There are two main communication models in VANETs: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. The model of V2V aims to exchange messages between different vehicles. V2I aims to exchange information between vehicles and RSUs. Both V2V and V2I are based on the Dedicated Short-range communication (DSRC) protocol, which applies the IEEE 802.11p standard for wireless communication [4]. In the DSRC protocol, the communication range is from 100 to 1000 *meters* [5], and the vehicle broadcasts messages every 100-300 *milliseconds* [6].

The openness of the communication environment in VANETs determines that it faces two challenges: (1) security [7], (2) privacy [8-9]. Firstly, the adversary easily launches various attacks, such as impersonation attack, and replay attack, by intercepting messages on the public channel. Thus, to ensure the recipient of the messages from legitimate vehicles can be authenticated and has not been modified by attackers, ensuring the security of data communication is the primary concern. Besides, privacy is also important [1]. If a vehicle directly sends its real identity to nearby RSU and other vehicles on the public channel, the attacker can track the vehicle's route through the identity of the vehicle. The leakage of the vehicle's route means that the user's privacy is exposed, which may cause serious consequences. Anonymous communication is an important way to protect privacy in VANETs, in which the vehicle uses a pseudonym instead of its own real identity when transmitting the messages. However, it is worth noting that anonymity is not completely anonymous. That is, TA can track the real identity of a vehicle when accidents occur. Thus, a malicious vehicle cannot use anonymity to avoidance of responsibility in the traffic accident. Conditional privacy is also required in the VANETs.

To enhance security and privacy in VANETs, various anonymous authentication schemes [10-14] are

*Corresponding Author: Yining Liu; E-mail: ynliu@guet.edu.cn
DOI: 10.3966/160792642020072104022

proposed, which are usually be roughly classified into three categories: (1) schemes based on public key infrastructure (PKI), (2) schemes based on identity-based signature (IBS), (3) schemes based on certificateless signature (CLS).

The main idea of PKI-based authentication scheme is that TA assigns multiple public-private key pairs, public key certificates, and anonymous certificates to each vehicle. In each communication, the vehicle picks a pair of public and private keys, and signs the message with the private key. Then the vehicle broadcasts the message, signature, and public key certificate. The verifier can authenticate the signature with public key certificate. Raya et al. [15] proposed a scheme based on PKI that achieves the goal of anonymous authentication. Then, Lu et al. [16] proposed a valid conditional privacy protocol. In Lu et al.'s scheme, the vehicle requests a short-term anonymous key from the RSU to complete the fast authentication of the message. PKI-based authentication scheme does not require the vehicle to store a large number of public-private key pairs. However, the vehicle needs to store a large number of anonymous certificates and TA must store anonymous certificates of all vehicles and maintain a tracking list for tracking the real identity of the vehicle. This puts TA and the vehicle under a huge storage burden. Since then, many lightweight certification schemes [17-18] have been proposed.

To solve the certificates management in PKI, some IBS schemes were proposed [19-26]. The vehicle does not need to store any public and private key pairs and anonymous certificates in advance. The vehicle's public key is calculated from its identity, and the corresponding private key is generated by the trusted third party called Private Key Generator (PKG). The message was signed by the private key of the vehicle, and the verifier authenticates the message with the corresponding public key. Shamir [19] first proposed an identity-based encryption and signature scheme in 1984. On this basis, many schemes are proposed. Zhang et al. [20] proposed an identity-based batch authentication scheme, in which the verifier can authenticate multiple received messages simultaneously. However, they still have some shortcomings, several schemes [21-22] tried to improve their weakness in replay attack and repudiation attack. Unfortunately, most of these schemes use complex bilinear pairing operations which are not suitable for vehicle wireless devices with limited computing power. Then He et al. [23] proposed a conditional privacy protection scheme that did not require pairing operations. In recent years, some lightweight authentication schemes [24-25] have been proposed to meet the requirements for fast certification of the VANETs. However, in some of these schemes, TA must store the system master key into the tamper-proof device (TPD) of the vehicle, which makes IBS have key escrow problems.

To deal with the key escrow problems, Al-Riyami et al. [27] first proposed a CLS scheme, which requires a key generation center (KGC) to generate a partial private key for each vehicle, and then the vehicle uses its private key and the partial private key to generate the final private key. Based on Al-Riyami et al.'s scheme, many related schemes have been proposed [28-31]. These schemes rely on TPD to store the partial private key. To make the assumption of TPD more practical, Zhong et al. proposed a privacy-protection authentication scheme [32]. However, Cui et al. [33] pointed out that Zhong et al.'s scheme authentication message was inefficient due to the complicated bilinear pairing operations. Then, Cui et al. proposed a certificateless aggregation signature (CL-AS) scheme without pairing operations. Although Cui rt al. Claim that proposal can resist various attacks. Kamil et al. [8] pointed out that Cui et al.'s scheme is insecure in the existing security model, and then they proposed an improved CL-AS scheme.

Many tamper-proof schemes are existing. In these schemes, the vehicle generates a pseudonym using the master key of TA stored in the vehicle's TPD. To ensure communication security in the VANETs, the system key should be updated regularly. However, the system key update efficiency is low due to the wireless communication protocol between TA and vehicle. Compared with the wireless communication method between TA and vehicle, the wired communication method between TA and RSU is more secure and efficient. The secure communication between RSUs and TA [33] makes the system master key update more efficient. Then, Bayat et al. [34] proposed a NERA scheme, in which TA stores the system master key into RSU's TPD instead of the vehicle's TPD. However, NERA maybe is vulnerable to impersonation attacks and reveal the privacy of users during the communication process. To remedy the weakness of the NERA scheme, an improved RSU-based authentication scheme with ECC for VANETs is proposed in this paper. The proposed scheme is based on ECC instead of bilinear pairing, thus avoiding complex pairing operations in the NERA scheme. The performance analysis shows that the proposed scheme owns a lower computational and communication burden.

The remainder of this paper is organized as follows. Section 2 describes the system model, and the security and privacy requirements. The review and analysis of the NERA scheme [34] are presented in Section 3. The proposed scheme is introduced in Section 4. The security and performance analysis are in Sections 5 and 6, respectively. Finally, the paper is concluded in Section 7.

2 Preliminaries

2.1 System Model

VANETs model mainly consists of three participants: RSU, TA and the OBUs, which is shown in Figure 1.

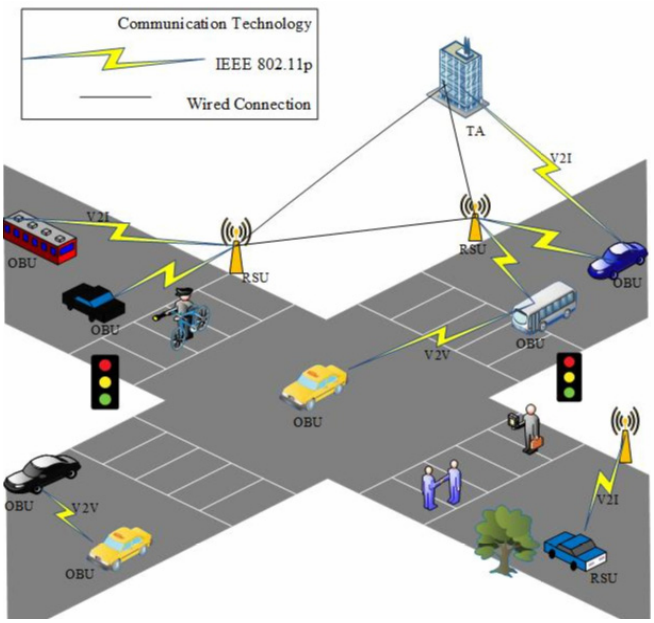

Figure 1. VANET model

RSU. Roadside Unit is usually installed in a fixed position along the roadsides, which has a large storage capacity and powerful communication capability [35] RSU is responsible for generating pseudonyms and private keys for the vehicle. RSU communicates with TA and vehicle via wired links or wireless channels respectively, and each RSU is equipped with a TPD for storing the system master key of TA. In this paper, we still use the TPD named ATSHA204 by Atmel Company [36], which allows read and write data operations.

TA. Trust Authority is usually a fully trusted third party. TA generates system parameters and is responsible for the registration of all vehicles and RSUs. TA is the only participant that can track the real identities of malicious vehicle.

OBU. Each vehicle is equipped with an OBU that communicates with RSU or nearby vehicles wirelessly. The data stored in the OBU will not be leaked. OBU periodically broadcast messages (driving status, congestion situation, etc.) in the VANETs.

2.2 Security and Privacy Requirements

The necessary security and privacy requirements include message integrity and authentication, identity privacy, traceability, unlinkability and resist several attacks.

Mutual authentication. mutual authentication is a security process in which both parties authenticate each other's identities before actual communication occurs. That is, a vehicle and an RSU prove their identities to each other before performing the communication-realated function.

Message authentication and integrity. Each message broadcast by the vehicle is authenticated to ensure that this message originated from a legitimate vehicle and has not been modified by an adversary.

Identity privacy. To guarantee the privacy of all vehicles, the real identity of the vehicle should keep anonymous from other vehicles and RSUs.

Traceability. Although the vehicles are anonymous, TA should have the ability to trace the real identity of the vehicles from its pseudonyms.

No-repudiation. When TA traces the real identity of the sender of a message, the sender cannot deny sending this message.

Unlinkability. It guarantees that an adversary cannot link any two or more received messages sent by the same vehicle. That is, an adversary cannot retrieve the real identity of a specific vehicle after analyzing multiple messages sent by it.

Resistance to attacks. The proposed scheme should resist several attacks, such as the impersonation attack, the replay attack, and the modification attack.

2.3 Elliptical Curve Cryptosystem and Assumptions

ECC [37] is widely used in authentication schemes for VANETs due to its capacity, providing a higher level of security with shorter keys [38]. $\mathbb{F}_n$ represents the finite field, which is determined by a large prime number n. Let a set of elliptic curve points E defined by the equation $y^2 = x^3 + ax + b \bmod n$, where $a, b \in \mathbb{F}_n$ and $(4a^3 + 27b^2) \bmod n \neq 0$. All the points on E and an infinity point O form an additive elliptic curve group G_1 with the order q and generator P.

Scalar point multiplication. The scalar multiplication of E is calculated as the repeated addition of a point. For instance, there is a point P on E, then mP is calculated as $mP = P + P + \cdots + P$ (m times), where $m \in Z_q^*$.

Elliptic Curve Discrete Logarithm Problem (ECDLP) assumption. Given two random points $P, Q \in G_1$, where $Q = x \cdot P$, $x \in Z_q^*$. The ECDLP is to found the integer $x \in Z_q^*$ satisfying $Q = x \cdot P$. ECDLP assumption is that the advantage of calculating $x \in Z_q^*$ in probability polynomial time is negligible.

Elliptic Curve Computational Diffie-Hellman Problem (ECCDHP) assumption. Given two random points Q, Y on E, where $Q = x \cdot P$, $Y = y \cdot P$ and x, y are two unknown values. The ECCDHP is to calculate the value $x \cdot y \cdot P$. ECCDHP assumption is that the advantage of calculating $x \cdot y \cdot P$ in probability

polynomial time is negligible.

3 Review and Analysis of NERA

3.1 Review of NERA

The NERA scheme [34] mainly contains five phases: system initialization, joining OBU to RSU group, message signing, verification, real identity tracking.

3.1.1 System Initialization

TA publishes the system parameters and registers RSUs and OBUs as follows.

TA selects a large prime number q and an elliptic curve $E: y^2 = x^3 + ax + b$, and P is a point on E which forms a cyclic additive group G_1 with order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$, where G_2 is a cyclic multiplicative group with order q. Then TA chooses a random $s \in Z_q^*$ as system master key and computes public key $P_{pub}^{TA} = s \cdot P$.

Step 1: TA preloads the public parameters $< G_1, G_2, q, P, P_{pub}^{RSU}, P_{pub}^{TA}, e(\cdot), H(\cdot), h(\cdot) >$ to RSU and stores the master key s on TPD of the RSU, where $P_{pub}^{RSU} = s \cdot H(ID_{RSU})$, $H(\cdot)$ is a map to point hash function and $h(\cdot)$ is a hash function.

Step 2: TA preloads the public parameters $< G_1, G_2, q, P, P_{pub}^{TA}, e(\cdot), H(\cdot), h(\cdot) >$ in OBU.

3.1.2 Joining OBU to RSU Group

The OBU completes mutual authentication with RSU and gets multiple pseudonyms from RSU.

Step 1: RSU broadcasts $< ID_{RSU}, P_{pub}^{RSU} >$.

Step 2: OBU certifies the RSU by checking the correctness of equation $e(P_{pub}^{RSU}, P) = e(H(ID_{RSU}), P_{pub}^{TA})$, then it sends its pseudo-ID $< PID_i^{(1)} \| PID_i^{(2)} >$ to the RSU, where $PID_i^{(1)} = r \cdot P$, $PID_i^{(2)} = RID_i \oplus h(r \cdot P_{pub}^{TA})$, $r \in Z_q^*$ and RID_i is the real identity of the OBU.

Step 3: RSU extracts the real identity RID_i by $RID_i = PID_i^{(2)} \oplus h(s \cdot PID_i^{(1)})$. Then it checks if there is RID_i in the local certificates revocation list (LCRL).

Step 4: If RID_i exists in the LCRL, RSU provides OBU with multiple pseudonyms. RSU chooses n random numbers $z_i \in Z_q^*$ and computes n pseudonyms $LPID = \{pid_1 \| pid_2 \| ... \| pid_n\}$ and corresponding private keys $LSK = \{sk_1 \| sk_2 \| ... \| sk_n\}$, where $pid_i = \{pid_i^{(1)} \| pid_i^{(2)}\} = \{z_i \cdot P, RID_i \oplus h(z_i \cdot P_{pub}^{TA})\}$, $sk_i = \{sk_i^{(1)} \| sk_i^{(2)}\} = \{s \cdot pid_i^{(1)} \| s \cdot H(pid_i^{(1)} \| pid_i^{(2)} \| T_j)\}$ and T_j is a timestamp. Then it selects a value $a \in Z_q^*$ and calculates $A = a \cdot P$, $R = a \cdot PID_i^{(1)}$, $k_{ij} = h(R \| RID_i)$, $Auth_{RSU} = HMAC_{k_{ij}}(LPID \| LSK \| T_j)$, $E_{RSU} = ENC_{k_{ij}}(LPID \| LSK \| T_j)$. It sends $< Auth_{RSU}, E_{RSU}, A, T_j >$ to OBU.

Step 5: OBU computes $R = r \cdot A$, $k_{ij} = h(R \| RID_i)$ and obtains $(LPID \| LSK \| T_j)$ from E_{RSU}. Then it checks that the equation $Auth_{RSU} = HMAC_{k_{ij}}(LPID \| LSK \| T_j)$ is hold. If it is true, the OBU get n pseudo-IDs.

3.1.3 Message Signing Phases

OBU signs the message M_i by $\sigma_i = sk_i^{(1)} + h(M_i) sk_i^{(2)}$. It broadcasts the messages $< \sigma_i, M_i, pid_i >$.

3.1.4 Verification Phases

Recipient verifies the equation $e(\sigma_i, H(ID_{RSU})) = e(pid_i^{(1)}, P_{pub}^{RSU}) e(h(M_i) \cdot H(pid_i^{(1)} \| pid_i^{(2)} \| T_j), P_{pub}^{RSU})$ and accepts the messages if it holds.

3.1.5 Real Identity Tracking

TA obtains the real identity of the vehicle by $RID_i = PID_i^{(2)} \oplus h(s \cdot PID_i^{(1)})$ with the help of RSU.

3.2 Cryptanalysis of NERA Scheme

NERA is claimed to meet all security requirements. However, it may be vulnerable against RSU spoofing attack, identity privacy threatens, and the malicious vehicle impersonation attack.

3.2.1 RSU Spoofing Attack

In the phase of joining OBU to RSU group, the RSU periodically broadcasts messages $< ID_{RSU_i}, P_{pub}^{RSU} >$ to all vehicles within its coverage. Upon receiving the message, the vehicle verifies the validity of RSU by checking whether equation $e(P_{pub}^{RSU}, P) = e(H(ID_{RSU_i}), P_{pub}^{TA})$ holds. Nevertheless, the identity ID_{RSU_i} of the RSU is public and P_{pub}^{RSU} is a public parameter, so it is very easy for an adversary to masquerade as a legal RSU.

3.2.2 Identity Privacy Threats

To satisfy the privacy requirement, none of the participants except TA in VANETs can extract the real identity of the vehicle from the intercepted messages. However, NERA does not provide sufficient anonymity and authenticity for users. The mutual

authentication between vehicle and RSU will reveal the vehicle's identity. The RSU can obtain the real identity RID_i of the vehicle by calculating the equation $RID_i = PID_i^{(2)} \oplus h(s \cdot PID_i^{(1)})$, where $< PID_i^{(1)} \| PID_i^{(2)} >$ is the pseudonym of the vehicle broadcast. RSU is a semi-trusted entity in their scheme. Therefore, it should not be overlooked that RSU may reveal the privacy of the vehicle. Therefore, the NERA scheme cannot meet the requirements of identity privacy protection and traceability.

3.2.3 Vehicle Impersonation Attack

There are two situations as follows.

Case 1 Adversary (malicious RSU) obtains the real identity RID_i of vehicle V_i from the intercepted message $< PID_i^{(1)} \| PID_i^{(2)} >$ by computes $RID_i = PID_i^{(2)} \oplus h(s \cdot PID_i^{(1)})$.

Then the adversary selects a random number $r^* \in Z_q^*$, computes pseudo-ID as $PID_i^{(1*)} = r^* \cdot P$, $PID_i^{(2*)} = RID_i \oplus h(r^* \cdot P_{pub}^{TA})$ and sends $< PID_i^{(1*)} \| PID_i^{(2*)} >$ to RSU.

When RSU receives the message $< PID_i^{(1*)} \| PID_i^{(2*)} >$, it first calculates $RID_i = PID_i^{(2*)} \oplus h(s \cdot PID_i^{(1*)})$ and then checks the validity of the RID_i.

Since RID_i is the real identity of a legal vehicle, RSU considers the adversary to be a legal vehicle.

Case 2 The adversary (unregistered vehicle with the identity of RID_i^*) first selects a random number $r \in Z_q^*$. Then, it calculates pseudo-ID as $PID_{i^*}^{(1)} = r \cdot P$, $PID_{i^*}^{(2)} = RID_i^* \oplus h(r \cdot P_{pub}^{TA})$ and sends message $< PID_{i^*}^{(1)} \| PID_{i^*}^{(2)} >$ to RSU.

When RSU receives messages $\{PID_{i^*}^{(1)} \| PID_{i^*}^{(2)}\}$, it first computes $RID_i^* = PID_{i^*}^{(2)} \oplus h(s \cdot PID_{i^*}^{(1)})$ and then checks the validity of the RID_i^*.

Likewise, since the identity RID_i^* of the unregistered vehicle does not appear in the Local Certificate Revocation List (LCRL), RSU considers the unregistered vehicle to be a legitimate vehicle.

3.2.4 Other Threats in NERA Scheme

There are still two threats in NERA scheme. Firstly, whenever a vehicle drives into the coverage area of a new RSU, it will discard the original pseudo-IDs, even if these pseudo-IDs do not expire. Then it performs the mutual authentication with the new RSU and gets new pseudo-IDs from this RSU. However, RSU is a device with a limited communication range (usually 1-3 *kilometer*) [35]. Therefore, not only the system resources are wasted, but also the calculation and communication burden of the RSU is increased. Secondly, in the verification phase, the receiver verifies the integrity of the message by checking whether $e(\sigma_i \cdot H(ID_{RSU_i})) = e(pid_i^{(1)}, P_{pub}^{RSU}) e(h(M_i) \cdot H(pid_i^{(1)} \| pid_i^{(2)} \| T_i), P_{pub}^{RSU})$ is true. In this case, the computation costs of scalar point multiplication and bilinear pairing operations are very huge. Therefore, their scheme fails to meet the fast authentication requirements.

4 The Proposed Scheme

4.1 Overview

In this paper, an enhanced RSU-based authentication scheme without pairing for VANETs is proposed, which not only inherits the advantages of NERA but also improves its security threatens. The proposed scheme includes the following five parts: the system initialization, pseudonym and private key generation, message signature, message verification, and malicious vehicle tracking. The process of updating the system master key stored in the RSU is not described in this paper.

4.2 System Initialization

All vehicles and RSUs register with TA before joining VANETs, and TA publishes system public parameters to all registered entities.

4.2.1 TA Setup

(1) TA selects a secure prime number n, an elliptic curve E which is defined by the equation: $y^2 = x^3 + ax + b \mod n$, where $a, b \in \mathbb{F}_n$.

(2) The TA picks a cyclic additive group G_1 generated by P with the prime order q.

(3) TA chooses three secure hash functions $h_1 : \{0,1\}^* \to Z_q^*$, $h_2 : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to Z_q^*$.

(4) The TA randomly selects $s \in Z_q^*$ as its master secret key and calculates the system public key $P_{pub}^{TA} = s \cdot P$.

(5) TA publishes system public parameters $param = \{G_1, q, n, P, P_{pub}^{TA}, h_1(\cdot), h_2(\cdot), H_1(\cdot)\}$ to all registered entities.

(6) TA maintains a private list ℓ_V and a list ℓ_R. The private list ℓ_V can only be accessed by TA for tracking the real identity of the vehicle. The list ℓ_R can only be accessed by registered RSUs. The contents of the two lists will be described later.

4.2.2 Vehicle Registration

The vehicle needs to register with TA as follows.

(1) Let V_i be the $i-th$ vehicle with real identity RID_i. The V_i selects a random number $a \in Z_q^*$, then it computes $A = a \cdot P$, $PID_i = H_1(RID_i \| a)$ and sends $< RID_i, PID_i, A >$ to TA via secure channel.

(2) Receiving messages $< RID_i, PID_i, A >$, TA computes $R = r \cdot P$, $B = r \cdot A$, $Q_i = H_1(B) \oplus H_1(PID_i)$, where $r \in Z_q^*$ is a random number chosen by TA. TA returns R to V_i, and V_i stores $< a, R >$ in its OBU.

(3) TA inserts tuple $< RID_i, H_1(PID_i), T_i >$ and $< H_1(B), Q_i, T_i >$ into list ℓ_V and ℓ_R respectively, where T_i denotes the valid period of the tuple.

4.2.3 RSU Registration

RSU registers to TA as follows.

(1) Let RSU_j be the $j-th$ RSU with identity ID_{RSU_j}. RSU_j submits its own identifier ID_{RSU_j} to TA for registration.

(2) When receiving the registration request of RSU_j, TA stores the system master key s into the tamper-proof device (TPD) of RSU.

4.3 Pseudonym and Private Key Generation

If pseudonyms and corresponding private keys of the vehicle V_i are expired, the vehicle executes mutual authentication with nearby RSU to get new pseudonyms and private keys from RSU.

(1) The OBU_i selects $d \in Z_q^*$, computes $D = d \cdot P$ and sends D to RSU_j.

(2) When the RSU_j receives D, it randomly selects $e \in Z_q^*$ and calculates $E = e \cdot P$, $X = \mathrm{s} \cdot D$. Then, RSU_j sends message $< ID_{RSU_j}, X, E >$ to the vehicle V_i.

(3) After receiving the message, vehicle V_i verifies whether equation (1) holds.

$$X = s \cdot D = s \cdot d \cdot P = d \cdot P_{pub}^{TA} \quad \textbf{(1)}$$

If the equation (1) holds, V_i successfully authenticates RSU_j, then V_i calculates $K = H_1(d \cdot E \| ID_{RSU_j})$, $B = a \cdot R$, $C_i = H_1(B) \oplus H_1(K)$. Vehicle V_i replies to RSU_j with message C_i.

(4) RSU_j calculates symmetric key $K = H_1(e \cdot D \| ID_{RSU_j})$, where a session key K ($K = H_1(d \cdot E \| ID_{RSU_j}) = H_1(e \cdot D \| ID_{RSU_j})$) is shared between V_i and RSU_j, and then it calculates $H_1(B) = C_i \oplus H_1(K)$. Next, RSU_j checks whether $H_1(B)$ exists in list ℓ_R. If such tuple does not exist or has expired, RSU_j terminates the session; otherwise RSU_j successfully authenticates V_i and the mutual authentication is completed.

(5) RSU_j chooses n random numbers $z_i \in Z_q^*$, $(i = 1, 2, ..., n)$, to generate pseudonym set as $LPID_i = \{pid_1, \cdots, pid_i, \cdots, pid_n\}$, where $pid_i = \{pid_{i,1} \| pid_{i,2}\}$, $pid_{i,1} = z_i \cdot P$, $pid_{i,2} = H_1(PID_i) \oplus H_1(z_i \cdot P_{pub}^{TA})$ and $H_1(PID_i) = H_1(B) \oplus Q_i$, and the corresponding private key $LSK_i = \{sk_1, \cdots, sk_i, \cdots, sk_n\}$ for vehicle V_i, where $sk_i = z_i + \alpha_i \cdot s \bmod q$, $\alpha_i = h_1(pid_i \| t_i)$ and t_i is a timestamp. RSU_j computes $A_{uth} = H_1(LPID_i \| LSK_i \| t_i)$, $E_{RSU} = ENC_K(LPID_i \| LSK_i \| t_i)$, and forwards messages $< A_{uth}, E_{RSU}, t_i >$ to vehicle V_i.

(6) Upon obtaining messages $< A_{uth}, E_{RSU}, t_i >$ from RSU_j, V_i first checks the freshness of t_i, then it utilizes the session key K to decrypt the cipher text E_{RSU} and obtains $(LPID_i \| LSK_i \| t_i)$. Then, it verifies if $H_1(LPID_i \| LSK_i \| t_i) = A_{uth}$ holds. If it is true, V_i stores $LPID_i$ and LSK_i.

4.4 Message Signature

A vehicle V_i signs its message M_i with its pseudonym pid_i and private key sk_i as follows.

(1) The vehicle V_i randomly selects a pseudonym pid_i from $LPID_i$, and get the corresponding private key sk_i from the LSK_i.

(2) The vehicle V_i generates a random number $f_i \in Z_q^*$. Then, it computes $F_i = f_i \cdot P$, $\beta_i = h_2(pid_i \| F_i \| M_i \| t_i')$ and $\sigma_i = sk_i + \beta_i \times f_i \bmod q$. Then, it broadcasts $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ to nearby vehicles and RSU, where t_i' and t_i are timestamps.

4.5 Message Verification

After receiving the message, the verifiers (vehicles or an RSUs or TA) check the validity of the received messages. To improve the efficiency of message verification, the batch verification of multiple signatures is used in this scheme.

4.5.1 Verification of One Message

After receiving message $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ sent by the vehicle V_i, the verifier uses the system

parameters $param=\{G_1,q,n,P,P_{pub}^{TA},h_1(\cdot),h_2(\cdot),H_1(\cdot)\}$ published by TA to execute the following steps.

(1) The verifier checks if $t_i^{'}$ and t_i are fresh. If so, it proceeds.

(2) The verifier checks whether the equation $\sigma_i \cdot P = pid_{i,1} + \alpha_i \cdot P_{pub}^{TA} + \beta_i \cdot F_i$ holds. If the equation holds, the verifier accepts the message; otherwise, the verifier rejects the message. The correctness of the single verification of one message can be proved using the equation (2).

$$\begin{aligned}\sigma_i \cdot P &= (sk_i + \beta_i \cdot f_i) \cdot P \\ &= (z_i + \alpha_i \cdot s + \beta_i \cdot f_i) \cdot P \\ &= z_i \cdot P + \alpha_i \cdot s \cdot P + \beta_i \cdot f_i \cdot P \\ &= pid_{i,1} + \alpha_i \cdot P_{pub}^{TA} + \beta_i \cdot F_i\end{aligned} \quad (2)$$

4.5.2 Batch Verification of Multiple Messages

Our scheme allows a verifier to verify a batch of messages. In this phase, in order to avoid man-in-the-middle attack, the small exponent test technology [39] is adopted to ensure the non-repudiation of signatures. Upon receiving a batch of messages $<M_1,pid_1,\sigma_1,F_1,t_1^{'},t_1>$, $<M_2,pid_2,\sigma_2,F_2,t_2^{'},t_2>$, …, $<M_n,pid_n,\sigma_n,F_n,t_n^{'},t_n>$ from n vehicles V_1, V_2, …, V_n respectively. The verifier performs the following steps.

(1) The verifier checks if t_i and $t_i^{'}$ are fresh, where $i=1,2,...,n$. If so, it proceeds.

(2) The verifier chooses a vector $v=\{v_1,v_2,v_3,...,v_n\}$, where v_i is random selected in $[1,2^t]$ and t is a very small integer. This process produces only a negligible computation cost. Next, the verifier checks whether the equation (3) holds. The correctness of the batch verification is as below.

$$\begin{aligned}&(\sum_{i=1}^{n} v_i \cdot \sigma_i) \cdot P \\ &= (\sum_{i=1}^{n} v_i \cdot (sk_i + \beta_i \cdot f_i)) \cdot P \\ &= (\sum_{i=1}^{n} v_i \cdot (z_i + \alpha_i \cdot s + \beta_i \cdot f_i)) \cdot P \\ &= \sum_{i=1}^{n} v_i \cdot z_i \cdot P + (\sum_{i=1}^{n} v_i \cdot \alpha_i) \cdot s \cdot P + (\sum_{i=1}^{n} v_i \cdot \beta_i \cdot f_i \cdot P) \\ &= \sum_{i=1}^{n} v_i \cdot pid_i + (\sum_{i=1}^{n} v_i \cdot \alpha_i) \cdot P_{pub}^{TA} + \sum_{i=1}^{n} v_i \cdot \beta_i \cdot F_i\end{aligned} \quad (3)$$

If equation (3) is true, all n messages are valid. Otherwise, it indicates that some of the messages in the batch are invalid. In this case, binary search technology [28] can be used for fetching invalid messages.

4.6 Malicious Vehicle Tracking

It is necessary to track the real identity of a malicious vehicle that broadcasts a controversial message M_i. Here, TA does this work.

(1) The receiver sends the pseudonym pid_i of the controversial message M_i to TA.

(2) After receiving the pseudonyms pid_i, TA calculates $H_1(PID_i) = pid_{i,2} \oplus H_1(s \cdot pid_{i,1})$. If there exists a valid tuple $<RID_i, H_1(PID_i), T_i>$ in the list ℓ_V, TA succeeds to trace the real identity RID_i of malicious vehicle V_i. Then, TA removes the tuple $<RID_i, H_1(PID_i), T_i>$ from the list ℓ_V to prevent the malicious vehicle from continuing to harm other vehicles.

5 Security Proof and Analysis

5.1 Security Proof

In this section, we present a formal proof, which shows that the proposed scheme can resist adaptive selection message attack based on ECDLP assumption in the random oracle model.

Theorem: The proposed scheme can resist the adaptive selection message attack under the random oracle model.

Proof: An instance $(P, Q = x \cdot P)$ of ECDLP is given, where P and Q are two points on the elliptic curve E. Suppose that an adversary A can forge a message $<M_i, pid_i, \sigma_i, F_i, t_i^{'}, t_i>$, and then we construct a challenger B and establish a game between challenger B and adversary A. The probability that B can solve ECDLP in polynomial time by running A as a subroutine is not negligible.

Setup: The challenger B select n random number $z_i \in Z_q^*, (i=1,2,...,n)$ to create an anonymous set $P_{ID}=\{pid_1,\cdots,pid_i,...,pid_n\}$ for the adversary A, where $pid_i=\{pid_{i,1} \| pid_{i,2}\}$. If $i=i^*$, then $pid_{i,1}=Q$, otherwise $pid_{i,1}=z_i \cdot P$. Then, the challenger B maintains three lists L_{H_1}, L_{h_1} and L_{h_2}, which store the query and answer of the list L_{H_1}, L_{h_1} and L_{h_2} respectively. Meanwhile, it selects random number k and computers its corresponding public key $K_{pub}=k \cdot P$. Then it generates system parameters $param=\{G_1,P,K_{pub},h_1(\cdot),h_2(\cdot),H_1(\cdot)\}$. Finally, the challenger B sends $param$ and P_{ID} to the adversary A.

H_1-query: A asks B for message φ, and then B checks if there is a tuple $<\varphi,\tau_{H_1}>$ in the list L_{H_1}

If so, returns $\tau_{H_1}=H_1(\varphi)$ directly to A, Otherwise, it chooses a random number $\tau_{H_1} \in Z_q^*$, stores the tuple $<\varphi,\tau_{H_1}>$ into the list L_{H_1} and sends $\tau_{H_1}=H_1(\varphi)$ to A.

h_1 **-query:** A asks B for message $< pid_i, t_i >$, and then B checks if there is a tuple $< pid_i, t_i, \tau_{h_1} >$ in the list L_{h_1} .If so, returns $\tau_{h_1} = h_1(pid_i \| t_i)$ directly to A; Otherwise, it chooses a random number $\tau_{h_1} \in Z_q^*$, stores the tuple $< pid_i, t_i, \tau_{h_1} >$ into list L_{h_1} and sends $\tau_{h_1} = h_1(pid_i \| t_i)$ to A.

h_2 **-query:** A asks B for message $< pid_i, F_i, M_i, t_i' >$, and then B checks if there is a tuple $< pid_i, F_i, M_i, t_i', \tau_{h_2} >$ in list L_{h_2}. If so, returns $\tau_{h_2} = h_2(pid_i \| F_i \| M_i \| t_i')$ directly to A; Otherwise, it chooses a random number $\tau_{h_2} \in Z_q^*$, stores the tuple $< pid_i, F_i, M_i, t_i', \tau_{h_2} >$ into list L_{h_2} and sends $\tau_{h_2} = h_2(pid_i \| F_i \| M_i \| t_i')$ to A.

Sign **-query:** A asks B for the signature of the messages $< M_i, pid_i >$ and B first checks if the tuple $< pid_i, t_i, \tau_{h_1} >$ is in list L_{h_1}. Then, B retrieves τ_{h_1} from the tuple $< pid_i, t_i, \tau_{h_1} >$. If $i = i^*$, B selects three random numbers $\sigma_i, \alpha_i, \beta_i \in Z_q^*$, chooses a random point $pid_{i,2}$, and computers $pid_{i,1} = \sigma_i \cdot P - \alpha_i \cdot K_{pub} - \beta_i \cdot F_i$. Then, B adds $< pid_i, t_i, \alpha_i >$ and $< pid_i, F_i, M_i, t_i', \beta_i >$ into L_{h_1} and L_{h_2} respectively, then sends a signature $< pid_i, F_i, M_i, \sigma_i, t_i', t_i >$ to A. Otherwise, if $i \neq i^*$, B has a valid signature $< pid_i, F_i, M_i, \sigma_i, t_i', t_i >$ and sends it directly to A.

Next, A sends the signature $< pid_i, F_i, M_i, \sigma_i, t_i', t_i >$ to B, and then B checks if the equation (4) is true

$$\sigma_i \cdot P = pid_{i,1} + \alpha_i \cdot K_{pub} + \beta_i \cdot F_i \quad \textbf{(4)}$$

If not, it discards this process. According to the Forgery Lemma [40], B can get another valid signature $< pid_i, F_i, M_i, \sigma_i^*, t_i', t_i >$ in polynomial time through A, where $\sigma_i \neq \sigma_i^*$. Similarly, we get an equation

$$\sigma_i^* \cdot P = pid_{i,1} + \alpha_i^* \cdot K_{pub} + \beta_i \cdot F_i \quad \textbf{(5)}$$

From equations (4) and (5), we can get the following equation (6)

$$\begin{aligned} &(\sigma_i - \sigma_i^*) \cdot P = \sigma_i \cdot P - \sigma_i^* \cdot P \\ &= pid_{i,1} + \alpha_i \cdot K_{pub} + \beta_i \cdot F_i - (pid_{i,1} + \alpha_i^* \cdot K_{pub} + \beta_i \cdot F_i) \\ &= (\alpha_i - \alpha_i^*) \cdot K_{pub} \\ &= (\alpha_i - \alpha_i^*) \times k \times P \bmod q \end{aligned} \quad \textbf{(6)}$$

In the end, B outputs $(\alpha_i - \alpha_i^*)^{-1}(\sigma_i - \sigma_i^*)$ as a solution to the ECDLP with a non-negligible probability. However, it is contradictory to the difficulty of the ECDLP. Hence, the proposed scheme can resist the adaptive selection message attack under the random oracle model. That is, the theorem is true.

5.2 Security Analysis

Our scheme is proved to achieve security and privacy goals.

Mutual authentication. The vehicle gets pseudonyms from RSU after mutual authentication with the RSU. In the proposed scheme, the vehicle authenticates RSU after receiving the message $< ID_{RSU_j}, X, E >$ submitted by RSU. Then the vehicle checks if the equation $X = d \cdot P_{pub}^{TA}$ holds. If the equation holds, RSU is a legal entity. Given D and P_{pub}^{TA}, an adversary has to solve ECCDHP to calculate $X = s \cdot D = d \cdot P_{pub}^{TA}$. Therefore, an adversary cannot imitate RSU. Similarly, RSU authenticates the vehicle after receiving the message C_i submitted by the vehicle. Then, RSU calculates $K = H_1(e \cdot D \| ID_{RSU_j})$, $H_1(B) = C_i \oplus H_1(K)$. RSU searches list ℓ_R for tuple $\{H_1(B), Q_i, T_i\}$. If such tuple does not exist, RSU aborts. Given D and E, an adversary has to solve ECCDHP to calculate $K = H_1(d \cdot E \| ID_{RSU_j}) = H_1(e \cdot D \| ID_{RSU_j})$. What's more, an adversary cannot calculates $B = a \cdot R$ without knowing a and R, where a and R are the two private parameters of the vehicle V_i. Therefore, an adversary cannot imitate the target vehicle V_i. In a word, the proposed scheme provides secure mutual authentication between RSU and vehicle.

Message authentication and integrity. According to the theorem, an attacker cannot forge a valid message $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ in polynomial time to satisfy the equation $\sigma_i \cdot P = pid_{i,1} + \alpha_i \cdot P_{pub}^{TA} + \beta_i \cdot F_i$, due to the intractability of ECDLP. Thus, the verifier could check the integrity and validity of the received message $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ by verifying whether the equation $\sigma_i \cdot P = pid_{i,1} + \alpha_i \cdot P_{pub}^{TA} + \beta_i \cdot F_i$ holds. Thus, this scheme provides message authentication and integrity.

Identity privacy. Each vehicle uses pseudonyms generated by RSU to communicate with others. When the vehicle sends a message $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$, its real identity RID_i is hidden in pseudonym $pid_i = \{pid_{i,1} \| pid_{i,2}\}$, where $pid_{i,1} = z_i \cdot P$, $H_1(PID_i) = pid_{i,2} \oplus H_1(z_i \cdot s \cdot P)$, $H_1(PID_i) = H_1(H_1(RID_i \| a))$. Suppose an adversary aims to obtain the real identity

RID_i of the vehicle, it has to calculate $z_i \cdot s \cdot P$ to obtain RID_i from $H_1(PID_i)$. According to ECCDHP assumption, it is difficult to calculate $z_i \cdot s \cdot P$. Besides, due to the one-way property of the hash function, it is difficult to calculate RID_i from $H_1(PID_i)$. Hence, the proposed scheme can protect the privacy of the vehicle.

Traceability. TA can trace the real identity of the vehicle that sent controversial messages. When the message $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ is considered controversial, TA can track the real identity of vehicle through its pseudonym $pid_i = \{pid_{i,1} \| pid_{i,2}\}$ and the tuple $< RID_i, H_1(PID_i), T_i >$ in list ℓ_V. TA calculates $H_1(PID_i) = pid_{i,2} \oplus H_1(s \cdot pid_{i,1})$ and then it retrieve the tuple $< RID_i, H_1(PID_i), T_i >$ in private list ℓ_V by $H_1(PID_i)$. Because only TA and RSU knows the system master key s, it is very hard for an adversary to calculate $H_1(PID_i)$ by $H_1(PID_i) = pid_{i,2} \oplus H_1(s \cdot pid_{i,1})$ without knowing s. Even if the RSU know $H_1(PID_i)$, it still cannot obtain the real identity RID_i of the vehicle from $H_1(PID_i) = H_1(H_1(RID_i \| a))$, due to the one-way property of hash function. The list ℓ_V only be accessed by TA in the proposed scheme. Therefore, only TA can track the real identity of the vehicle.

No-repudiation. In the proposed scheme, TA can track the real identity RID_i of the vehicle sending controversial messages $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$, thus all entities cannot deny its behavior of sending the controversial messages. Moreover, we adopt the small exponent test technology to ensure that none can deny its signature during the batch verification process. Because the verifier can verify the message by the equation (3). Thus, the proposed scheme provides no-repudiation.

Unlinkability. In our scheme, $pid_i = \{pid_{i,1} \| pid_{i,2}\}$, $F_i = f_i \cdot P$, $pid_{i,1} = z_i \cdot P$, $pid_{i,2} = H_1(PID_i) \oplus H_1(z_i \cdot P_{pub}^{TA})$, $\alpha_i = h_1(pid_{i,1}, pid_{i,2}, t_i)$, $sk_i = z_i + \alpha_i \cdot s \bmod q$, $\beta_i = h_2(pid_i, F_i, M_i, t_i')$, $\sigma_i = sk_i + \beta_i \cdot f_i \bmod q$, where $z_i \in Z_q^*$ and $f_i \in Z_q^*$ are randomly selected by RSU and vehicle respectively. Each pseudonym $pid_i = \{pid_{i,1} \| pid_{i,2}\}$ always uses a different random number $z_i \in Z_q^*$, and the pseudonym $pid_i = \{pid_{i,1} \| pid_{i,2}\}$ of each signature σ_i is indistinguishable. Therefore, an adversary cannot link any two or more signatures to a particular vehicle.

5.3 Resist Impersonation Attack

Case 1 If an adversary tries to imitate a legal RSU in the pseudonym and private key generation phase, it must gain the system master key s. However, s is stored in the TPD of RSU, so the adversary cannot forge the message $X = s \cdot D$ to fake the legal vehicles.

Case 2 In the pseudonym and private key generation phase, if adversary intents to imitate a legal vehicle, it must know a and R. Then, it computes $B = a \cdot R$. However, a and R are two private parameters of the vehicle V_i. It is infeasible for the adversary to imitate the legal vehicle without knowing a and R.

Case 3 In the message verification phase, an adversary wants to forge a legal message $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ to satisfy the equation $\sigma_i \cdot P = pid_{i,1} + \alpha_i \cdot P_{pub}^{TA} + \beta_i \cdot F_i$ or $(\sum_{i=1}^{n} v_i \cdot \sigma_i) \cdot P = \sum_{i=1}^{n} v_i \cdot pid_i + (\sum_{i=1}^{n} v_i \cdot \alpha_i) \cdot P_{pub}^{TA} + \sum_{i=1}^{n} v_i \cdot \beta_i \cdot F_i$, where $\alpha_i = h_1(pid_{i,1} \| pid_{i,2} \| t_i)$ and $\beta_i = h_2(pid_i \| F_i \| M_i \| t_i')$. However, an adversary cannot forge such a signature without knowing the current master key s according to the theorem. Even if the current master key s is obtained by the adversary, it is only valid until the next master key s is updated. Since the master key update in our scheme is more efficient, the leakage of the current master key will not have a permanent impact on the VANETs. Therefore, our scheme could withstand the impersonation attack.

Resist modification attack. In the proposed scheme, according to the theorem, if the messages $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ is modified, the verifier can easily discover the modification by detecting whether the equation $\sigma_i \cdot P = pid_{i,1} + \alpha_i \cdot P_{pub}^{TA} + \beta_i \cdot F_i$ or $(\sum_{i=1}^{n} v_i \cdot \sigma_i) \cdot P = \sum_{i=1}^{n} v_i \cdot pid_i + (\sum_{i=1}^{n} v_i \cdot \alpha_i) \cdot P_{pub}^{TA} + \sum_{i=1}^{n} v_i \cdot \beta_i \cdot F_i$ is true, where $\alpha_i = h_1(pid_{i,1} \| pid_{i,2} \| t_i)$, $\beta_i = h_2(pid_i \| F_i \| M_i \| t_i')$.

Resist man-in-the-middle attack. Suppose there is an adversary between the sender and verifier, and the goal of the adversary is to convince the sender and verifier that they are communication directly. Therefore, the adversary must to forge the signature of both the sender and verifier and then communicate with them. In the theorem, we have proved that no one can forge such a signature. Besides, we use the small exponent test technology to ensure that once the messages are forged, the verifier can detect it timely. Thus, our scheme can resist the man-in-the-middle attacks.

Resist replay attack. In our scheme, random number and timestamp mechanisms are used to cope with the replay attack. An adversary intercepts messages $< ID_{RSU_j}, E, X >, C_j$, $< A_{uth}, E_{RSU}, t_i >$, $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ on the public channel and then intents to forge RSU or vehicle by replaying these messages. The messages $< ID_{RSU_j}, E, X >$ and C_j contains the random numbers e and d. Then the receiver could detect the

replayed messages by checking the freshness of e and d. Similarly, the messages $< A_{uth}, E_{RSU}, t_i >$ and $< M_i, pid_i, \sigma_i, F_i, t_i', t_i >$ contain timestamps, and the verifier identifies the replayed messages by detecting the validity of timestamps. Therefore, our scheme resists replay attack.

6 Performance Evaluation

In this section, we evaluate the performance of the excellent schemes, such as NERA [34], Kumar et al.'s scheme [30], Zhong et al.'s scheme [32] and the proposed scheme in terms of computational and communication overhead for certificate and signature verification process. This paper constructs two cryptographic algorithms with a security level of 80 *bits*. The bilinear pairing operation is created as $\hat{e}: G_1 \times G_1 \to G_T$, where G_1 denotes an additive group with a generator of $\hat{P}$ and a prime order $\hat{q}$ on the super singular elliptic curve $\hat{E}: y^2 = x^3 + x \bmod \hat{p}$ with embedding degree 2. The length of the prime numbers $\hat{p}$ and $\hat{q}$ are 512-*bit* and 160-*bit* respectively. The ECC is created as following: G_a represents an additive group with a generator of P and a prime order q on non-singular elliptic curve $E: y^2 = x^3 + ax + b \bmod p$, where p, q are two 160-*bit* prime numbers and $a, b \in Z_q^*$.

6.1 Computation Overhead

This subsection mainly compares the computation overhead of the proposed scheme with the other three related VANETs-based schemes [30, 32, 34]. This paper refers to the running time of the cryptographic operations of the He et al.'s scheme [23], as shown in Table 1. For the sake of convenience, we use the following notations to indicate the running time of the cryptographic operations.

Table 1. Cryptographic operations and execution times

Cryptographic operation	Execution time (ms)
T_{bp}	4.211
T_{bp}^{m}	1.709
T_{bp}^{sm}	0.0535
T_{bp}^{a}	0.0071
T_{mtp}	4.406
T_{ecc}^{m}	0.442
T_{ecc}^{sm}	0.0138
T_{ecc}^{a}	0.0018
T_h	0.0001

T_{bp} : The time to perform one bilinear pairing $\hat{e}(P,Q)$, where $\hat{P}, \hat{Q} \in G_1$;

T_{bp}^{m} : The time to compute a scalar multiplication $x \cdot \hat{P}$ of the bilinear pairing, where $x \in Z_q^*$, $\hat{P} \in G_1$;

T_{bp}^{sm} : The time to compute a small multiplication operation $v_i \cdot \hat{P}$ of the bilinear pairing, where $v_i \in [1, 2^t]$, $\hat{P} \in G_1$;

T_{bp}^{a} : The time to compute a point addition operation $\hat{P} + \hat{Q}$ of the bilinear pairing, where $\hat{P}, \hat{Q} \in G_1$;

T_{mtp} The time to compute a Map-To-Point hash operation related to the bilinear pairing;

T_{ecc}^{m} : The time to perform one scalar multiplication $y \cdot P$ of the elliptic curve cryptography, where $y \in Z_q^*, P \in G_a$;

T_{ecc}^{sm} : The time to compute a small multiplication operation $v_i \cdot P$ of the elliptic curve cryptography, where $v_i \in [1, 2^t]$, $P \in G_a$;

T_{ecc}^{a} : The time to compute a point addition operation $P + Q$ of the elliptic curve cryptography, where $P, Q \in G_a$;

T_h : The time of one one-way hash operation.

We present the detailed analysis of Kumar et al.'s scheme [30], Zhong et al.'s scheme [32], the NERA scheme [34] and the proposed scheme in the pseudonym generation and message signing phase, the single verification of one message phase and the batch verification of n messages phase. The comparisons of the computation costs at each phase are shown in Table 2.

In our scheme, the pseudonym generation and message-signing phase contain three scalar multiplication operations of ECC, three one-way hash operations. Hence, the total computation cost of this phase is $3T_{ecc}^{m} + 3T_h \approx 1.3263$ *ms*. The single verification of one message phase requires three scalar multiplication operations of ECC, two addition operations of ECC and two one-way hash operations. Therefore, the total computation cost of this phase is $3T_{ecc}^{m} + 2T_{ecc}^{a} + 2T_h \approx 1.3298$ *ms*. Similarly, the batch verification of n messages phase needs $(n+2)$ scalar multiplication operations of the ECC, n small multiplication operations of ECC, $2n$ addition operations of ECC and $2n$ one-way hash operations.

Therefore, the total computation cost of this phase is $(n+2)T_{ecc}^{m} + nT_{ecc}^{sm} + 2nT_{ecc}^{a} + 2nT_h \approx (0.884 + 0.4596n)$ *ms*. The cost of computation of the other schemes [30, 32, 34] can be calculated in the same way.

Table 2. Comparison of computation cost

scheme	The pseudonym generation and message signing (ms)	The single verification of one message (ms)	The batch verification of multiple messages(ms)
Kumar et al. [30]	$4T_{bp}^{m}+2T_{bp}^{a}+2T_{mtp}$ $+3T_h \approx 15.6625$	$4T_{bp}+3T_{bp}^{m}+2T_{mtp}$ $+3T_h \approx 30.7833$	$4T_{bp}+3nT_{bp}^{m}+2nT_{mtp}+$ $3nT_h \approx 16.844+13.9393n$
Zhong et al. [32]	$7T_{bp}^{m}+2T_{bp}^{a}+3T_{mtp}$ $+1T_h \approx 25.1953$	$3T_{bp}+2T_{bp}^{m}+1T_{bp}^{a}+$ $2T_{mtp}+1T_h \approx 24.8702$	$3T_{bp}+2nT_{bp}^{m}+nT_{bp}^{a}+(n+1)T_{mtp}$ $+nT_h \approx 17.039+7.8312n$
NERA [34]	$3T_{bp}^{m}+1T_{bp}^{a}+1T_{mtp}$ $+2T_h \approx 9.5403$	$3T_{bp}+1T_{bp}^{m}+2T_{mtp}$ $+1T_h \approx 23.1541$	$3T_{bp}+nT_{bp}^{m}+(n+1)T_{mtp}+$ $nT_h \approx 17.039+6.1151n$
Proposed	$3T_{ecc}^{m}+3T_h$ ≈ 1.3263	$3T_{ecc}^{m}+2T_{ecc}^{a}+2T_h$ ≈ 1.3298	$(n+2)T_{ecc}^{m}+nT_{ecc}^{sm}+2nT_{ecc}^{a}$ $+2nT_h \approx 0.884+0.4596n$

Meanwhile, in the pseudonym generation and message-signing phase, the percentage improvement of our scheme is $(15.6625-1.3263)/15.6625 \approx 91.53\%$ higher than Kumar et al.'s scheme [30] and $(25.1953-1.3263)/25.1953 \approx 94.74\%$ higher than Zhong et al.'s scheme [32] and $(9.5403-1.3263)/9.5403 \approx 86.10\%$ higher than the NERA scheme [34]. In other phrases, the percentage of improvements in our scheme can be computed in the same way. Finally, the computational performance comparison between our scheme and other schemes are shown in Table 3.

Table 3. The computation cost of our scheme over other schemes

phase \ scheme	Kumar et al. [30]	Zhong et al. [32]	NERA. [34]
The pseudonym generation and message-signing (%)	91.53	94.74	86.10
The single verification of one message (%)	95.68	94.65	94.26
The batch verification of multiple (100) messages (%)	96.68	94.14	92.55

All vehicles in VANETs broadcast messages every 100 - 300 *ms*. During a peak traffic period, assume that the verifier receives messages from 180 vehicles every 300 *ms*, which requires the verifier to verify approximately 600-2000 messages within 1 *second*. To verify 600 messages, a verifier in our scheme takes 276.644 *ms* , while the other schemes [30, 32, 34] take 8380.424 *ms*, 4715.759 *ms* and 3686.099 *ms* respectively. Since the verification time of the other schemes [30, 32, 34] exceeds one second, only our scheme can meet the requirements of batch verification.

Figure 2 shows that when a single message is authenticated, the execution times of the proposed scheme is significantly smaller than other schemes. The relationship between the verification time and the number of messages is shown in Figure 3.

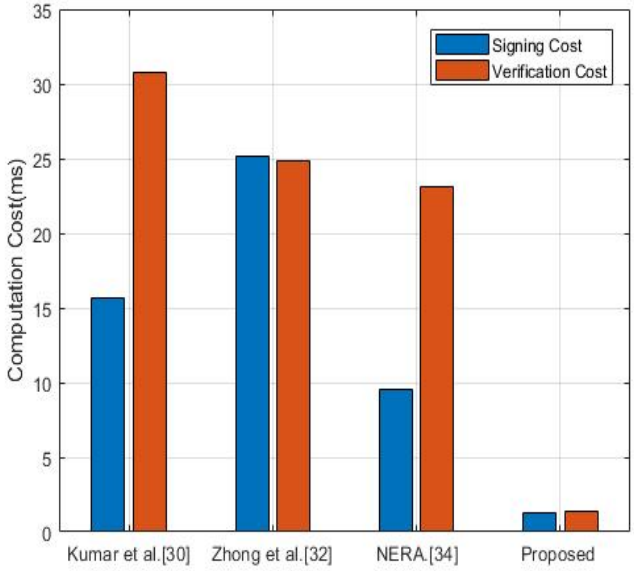

Figure 2. Computation overhead to sign and verify one message

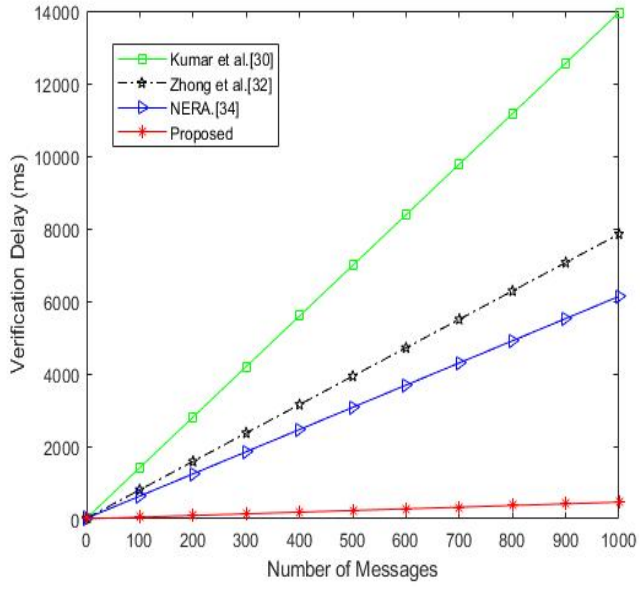

Figure 3. Verification delay with different number of messages

6.2 Communication Overhead

Since $\hat{p}$ and p are prime numbers of 64 *bytes* (512-*bits*) and 20 *bytes* (160-*bits*) respectively, the length of the elements in G_1 and G_2 are128 *bytes* and 40 *bytes* separately. We assume the length of the one-way hash function's output and timestamp are 20 *bytes* and 4 *bytes* respectively, and the length of the identity is 20 *bytes*. Therefore, we get the communication cost of our scheme and other schemes in Table 4.

Table 4. Comparison of communication cost

scheme	Sending a message (bytes)	Sending n messages (bytes)
Kumar et al. [30]	768	768n
Zhong et al. [32]	644	644n
NERA. [34]	384	384n
Proposed	148	148n

In the proposed scheme, a communication message is $\{pid_i, F_i, \sigma_i, t_i^{'}, T_j\}$, where $pid_i = \{pid_{i,1}, pid_{i,2}\}$, $\sigma_i \in Z_q^*$, $pid_{i,1}, pid_{i,2}, F_i \in G_a$ and $t_i^{'}$, T_j are the timestamps. Therefore, the total communication cost of our scheme is $40 \times 3 + 20 + 4 \times 2 = 148$ *bytes* and $148\,n$ bytes for n messages. The cost of communication of the other schemes [30, 32, 34] can be calculated in the same way. The relationship between communication overhead and the number of signatures is shown in Figure 4. Obviously, the proposed scheme has less communication costs than other schemes.

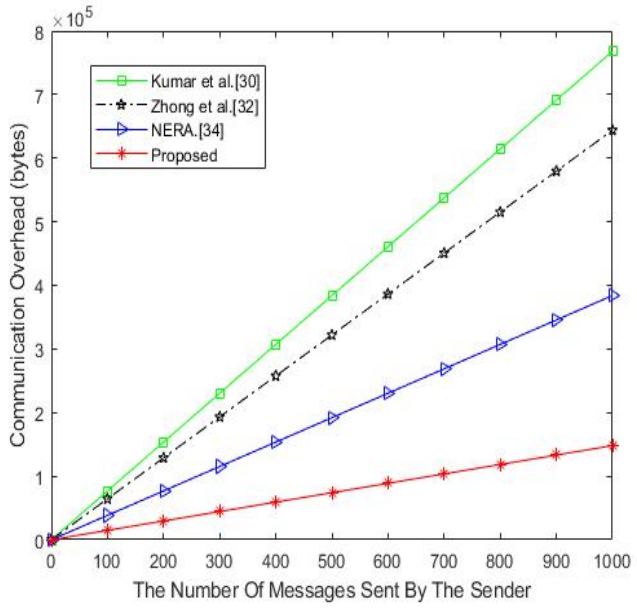

Figure 4. Communication overhead with the different number of messages

7 Conclusion

In order to address the weakness in NERA scheme, an improved RSU-based authentication scheme with ECC is proposed, in which RSU distributes the pseudonyms for the vehicle when the vehicle's pseudonyms are invalid. In the pseudonym and private key generation phase, the mutual authentication between vehicle and RSU does not leak the real identity of the vehicle. In this paper, the system master key is not stored in TPD of the vehicle, thus avoiding the risk of compromising TPD of one vehicle leading to the entire system failure. Besides, we demonstrated the security of the proposed scheme in the random oracle model under the Discrete Logarithm assumption. We demonstrated that the proposed scheme can satisfy all privacy and security requirements for VANETs. The proposed scheme requires less computation overhead due to the use of the elliptic curve cryptosystem instead of bilinear pairing. Extensive performance analysis showed that the proposed scheme in terms of computation cost and communication overhead is better than other related schemes.

Acknowledgements

This work was partly supported by National Natural Science Foundation of China under grant No. 61662016, Key projects of Guangxi Natural Science Foundation under grant No. 2018JJD170004 and Youth project of Guangxi Natural Science Foundation (2018GXNSFBA281019).

References

[1] S. O. Ogundoyin, An Autonomous Lightweight Conditional Privacy-preserving Authentication Scheme with Provable Security for Vehicular Ad-hoc Networks, *International Journal of Computers and Applications*, Vol. 42, No. 2, pp. 196-211, 2020.

[2] A. S. Salama, B. K. Saleh, M. M. Eassa, Intelligent Cross Road Traffic Management System (ICRTMS), *2010 2nd International Conference on Computer Technology and Development*, Cairo, Egypt, 2010, pp. 27-31.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges, *Telecommunication Systems*, Vol. 50, No. 4, pp. 217-241, August, 2012.

[4] Z. H. Mir, F. Filali, LTE and IEEE 802.11p for Vehicular Networking: A Performance Evaluation, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2014, No. 1, Article number 89, May, 2014.

[5] S. S. Manvi, and S. Tangade, A survey on Authentication Schemes in VANETs for Secured Communication, *Vehicular Communications*, Vol. 9, pp. 19-30, July, 2017.

[6] J. Cui, J. Zhang, H. Zhong, R. Shi, Y. Xu, An Efficient Certificateless Aggregate Signature Without Pairings for Vehicular Ad Hoc Networks, *Information Sciences*, Vol. 451-452, pp.1-15, July, 2018.

[7] A. Sari, O. Onursal, M. Akkaya, Review of the Security Issues in Vehicular Ad Hoc Networks (VANET), *International Journal of Communications, Network and System Sciences*, Vol. 8, No. 13, pp. 552-566, December, 2015.

[8] I. A. Kamil, S. O. Ogundoyin, An Improved Certificateless Aggregate Signature Scheme Without Bilinear Pairings for Vehicular Ad Hoc Networks, *Journal of information security and applications*, Vol. 44, pp. 184-200, February, 2019.

[9] Z. Zhang, B. Han, H. C. Chao, F. Sun, L. Uden, D. Tang, A New Weight and Sensitivity Based Variable Maximum Distance to Average Vector Algorithm for Wearable Sensor Data Privacy Protection, *IEEE Access*, Vol. 7, pp. 104045-104056, July, 2019.

[10] W. C. Chien, H. Y. Weng, C. F. Lai, Z. Fan, H. C. Chao, Y. Hu, A SFC-based Access Point Switching Mechanism for Software-defined Wireless Network in IoV, *Future Generation Computer Systems*, Vol. 98, pp. 577-585, September, 2019.

[11] W. Guo, Y. Liu, J. Wang, FPAP: Fast Pre-distribution Authentication Protocol for V2I, in: X. Sun, A. Liu, H. C. Chao, E. Bertino (Eds.), *International Conference on Cloud Computing and Security*, Springer, Cham, 2016, pp. 25-36.

[12] M. Kazemi, M. Delavar, J. Mohajeri, M. Salmasizadeh, On the Security of an Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks, *Iranian Conference on Electrical Engineering (ICEE)*, *IEEE*, Mashhad, Iran, 2018, pp. 510-514.

[13] X. Zhang, L. Mu, J. Zhao, C. Xu, An Efficient Anonymous Authentication Scheme with Secure Communication in Intelligent Vehicular Ad-hoc Networks, *KSII Transactions on Internet & Information Systems*, Vol. 13, No. 6, pp. 3280-3298, June, 2019.

[14] L. Zhang, X. Men, K. R. Choo, Y. Zhang, F. Dai, Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud, *IEEE Transactions on Dependable and Secure Computing*, pp. 1-14, January, 2018. http://doi.org/10.1109/TDSC.2018.2797190.

[15] M. Raya, J. P. Hubaux, Securing Vehicular Ad Hoc Networks, *Journal of Computer Security*, Vol. 15, No. 1, pp. 39-68, January, 2007.

[16] R. Lu, X. Lin, H. Zhu, P. H. Ho, X. Shen, ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, Phoenix, AZ, USA, 2008, pp. 1229-1237.

[17] Z. Zhou, H. Zhang, Z. Sun, An Improved Privacy-Aware Handoff Authentication Protocol for VANETs, *Wireless Personal Communications*, Vol. 97, No. 3, pp. 3601-3618, December, 2017.

[18] P. Wang, Y. Liu, S. Lv, An Improved Lightweight Identity Authentication Protocol for VANET, *Journal of Internet Technology*, Vol. 20, No. 5, pp. 1491-1504, September, 2019.

[19] A. Shamir, Identity-based Cryptosystems and Signature Schemes, in: G. R. Blakley, D. Chaum (Eds.), *Workshop on the Theory and Application of Cryptographic Techniques, CRYPTO 1984*, Springer, Berlin, Heidelberg, 1985, pp. 47-53.

[20] C. Zhang, R. Lu, X. Lin, P. Ho, X. Shen, An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks, *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, Phoenix, AZ, USA, 2008, pp. 246-250.

[21] T. W. Chim, S. M. Yiu, L. C. K. Hui, V. O. K. Li, SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs, *Ad Hoc Networks*, Vol. 9, No. 2, pp. 189-203, March, 2011.

[22] 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, August, 2013.

[23] D. He, S. Zeadally, B. Xu, X. Huang, 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, December, 2015.

[24] Y. Liu, S. Lv, M. Xie, Z. Chen, P. Wang, Dynamic Anonymous Identity Authentication (DAIA) scheme for VANET, *International Journal of Communication Systems*, Vol. 32, No. 5, e3892, March, 2019.

[25] J. Zhang, J. Cui, H. Zhong, Z. Chen, L. Liu, PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-preserving Authentication Scheme in Vehicular Ad-hoc Networks, *IEEE Transactions on Dependable and Secure Computing*, pp. 1-14, March, 2019. http://doi.org/10.1109/TDSC.2019.2904274.

[26] J. Song, Y. Liu, J. Shao, C. Tang, A Dynamic Membership Data Aggregation (DMDA) Protocol for Smart Grid, *IEEE Systems Journal*, Vol. 14, No. 1, pp. 900-908, March, 2020.

[27] S. S Al-Riyami, K. G. Paterson, Certificateless Public Key Cryptography, in: C. S. Laih (Ed.), *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Berlin, Heidelberg, 2003, pp. 452-473.

[28] J. Cui, J. Zhang, H. Zhong, Y. Xu, SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET With Cuckoo Filter, *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 11, pp. 10283-10295, November, 2017.

[29] J. Cui, L. Wei, J. Zhang, Y. Xu, H. Zhong, An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 20, No. 5, pp. 1621-1632, May, 2019.

[30] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, S. K. H. Islam, Secure CLS and CL-AS Schemes Designed for VANETs, *The Journal of Supercomputing*, Vol. 75, No. 6, pp. 3076-3098, June, 2019.

[31] J. Cui, D. Wu, J. Zhang, Y. Xu, H. Zhong, An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs, *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 3, pp. 2972-2986, March, 2019.

[32] H. Zhong, S. Han, J. Cui, J. Zhang, Y. Xu, Privacy-preserving

Authentication Scheme with Full Aggregation in VANET, *Information Sciences*, Vol. 476, pp. 211-221, February, 2019.

[33] J. Cui, J. Zhang, H. Zhong, R. Shi, Y. Xu, An Efficient Certificateless Aggregate Signature Without Pairings for Vehicular Ad Hoc Networks, *Information Sciences*, Vol. 451-452, pp. 1-15, July, 2018.

[34] M. Bayat, M. Pournaghi, M. Rahimi, M. Barmshoory, NERA: A New and Efficient RSU Based Authentication Scheme for VANETs, *Wireless Networks*, pp. 1-16, June, 2019. http://doi.org/10.1007/s11276-019-02039-x

[35] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET, *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 2, pp. 896-911, February, 2016.

[36] S. M. Pournaghi, B. Zahednejad, M. Bayat, Y. Farjami, NECPPA: A Novel and Efficient Conditional Privacy-Preserving Authentication Scheme for VANET, *Computer Networks*, Vol. 134, pp. 78-92, April, 2018.

[37] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, C. Chen, A Secure Three-Factor User Authentication Protocol with Forward Secrecy for Wireless Medical Sensor Network Systems, *IEEE Systems Journal*, Vol. 14, No. 1, pp. 39-50, March, 2020.

[38] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3599-3609, August, 2018.

[39] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, M. K. Khan, b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET, *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 11, pp. 1860-1875, November, 2013.

[40] D. Pointcheval, J. Stern, Security Arguments for Digital Signatures and Blind Signatures, *Journal of cryptology*, Vol. 13, No. 3, pp. 361-396, June, 2000.

Biographies

Hongyuan Cheng received the B. E. degree in Computer Science and Technology from Taishan University, Shandong, China, in 2018. She is graduate in School of Computer and Information Security, Guilin University of Electronic Technology, Guilin, China. Her research interest focuses on security and privacy in vehicular communication.

Yining Liu received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, China, in 1995, the M.S. degree in computer software and theory from the Huazhong University of Science and Technology, Wuhan, China, in 2003, and the Ph.D. degree in mathematics from Hubei University, Wuhan, in 2007. He is currently a professor with school of Computer and Information Security, Guilin University of Electronic Technology, Guilin, China. His research interests include the information security protocol and data privacy.