An improved efficient authentication scheme for vehicular ad hoc networks with batch verification using bilinear pairings

Eko Fajar Cahyadi

Department of Computer Science and Information Engineering,
Asia University,
Taichung, 41354, Taiwan
and
Faculty of Telecommunication and Electrical Engineering,
Institut Teknologi Telkom Purwokerto,
Purwokerto, 53147, Indonesia
Email: ekofajarcahyadi@ittelkom-pwt.ac.id

Min-Shiang Hwang*

Department of Computer Science and Information Engineering,
Asia University,
Taichung, 41354, Taiwan
Email: mshwang@asia.edu.tw
and
Department of Medical Research,
China Medical University Hospital,
China Medical University,
Taichung, 40402, Taiwan
*Corresponding author

Abstract: Research related to the authentication schemes in vehicular ad hoc networks (VANETs) still becomes a hot issue to discuss. In 2019, Cui and Tu proposed an efficient authentication scheme for vehicular ad hoc networks (VANETs) with batch verification using bilinear pairings. Their scheme was designed to improve the utilisation of the double-secret key in the identity-based batch signature (IBS) scheme published by Jianhong et al. and Bayat et al. Unfortunately, we found that Cui and Tu's identity-based conditional privacy-preserving authentication (IBCPPA) scheme is also insecure against non-repudiation attack. By those defects, a malicious user can broadcast some wrong messages to mislead the roadside unit (RSU) and deny its behaviour when a trusted authority (TA) traces it. In this article, we address the issue and give our improvement to withstand the above security threat.

Keywords: batch verification; IBCPPA; non-repudiation attack; security; VANETs.

Reference to this paper should be made as follows: Cahyadi, E.F. and Hwang, M-S. (xxxx) 'An improved efficient authentication scheme for vehicular ad hoc networks with batch verification using bilinear pairings', *Int. J. Embedded Systems*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Eko Fajar Cahyadi is a Lecturer in the Faculty of Telecommunication and Electrical Engineering, Institut Teknologi Telkom Purwokerto, Indonesia. He is currently pursuing his PhD in the Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan, under the supervision of Professor Min-Shiang Hwang. He receives his BEng and MSc in Electrical Engineering from the Institut Sains dan Teknologi Akprind Yogyakarta in 2009, and Institut Teknologi Bandung in 2013, respectively. His research interest includes information security, VANETs, and WLANs.

Min-Shiang Hwang received his PhD in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He was the Chairman of the Department of Information Management, Chaoyang University of Technology, and National Chung Hsing University during 1999–2009. He was also a Visiting Professor with the University of California, Riverside and Davis (USA) during 2009–2010. He obtained the 1997–2001 Excellent Research Award of the National Science Council. He was the Dean of the College of Computer Science, Asia University (AU) during 2011–2015. He is currently the Chair Professor of AU. He has published over 200+ articles in international journals.

1 Introduction

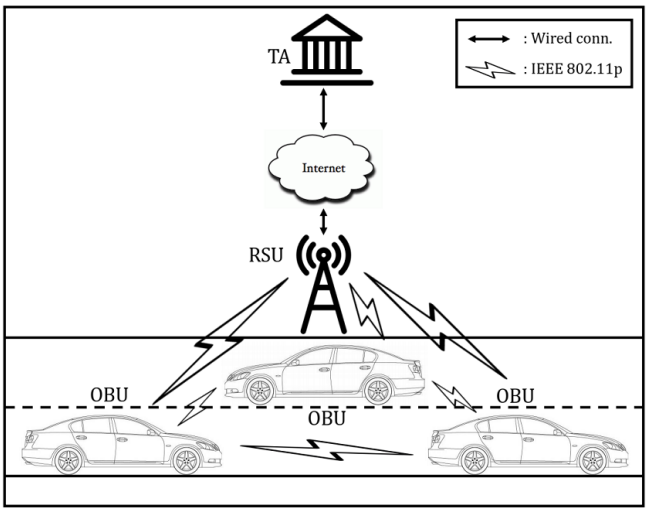
The vehicular ad hoc networks (VANETs) emerged from the existing mobile ad hoc network (MANET) concept (Faisal and Zaidi, 2020; Jindal and Bedi, 2018; Rodrigues et al., 2021). VANETs are made up of moving vehicles that represent nodes, fixed roadside units (RSUs) that allow vehicles to communicate with one another, and trusted authority (TA) (see Figure 1). VANETs is a mobile wireless network designed to help vehicle safety and traffic monitoring. To achieve these goals, Zhou et al. (2018) proposed a VANETs model based on immune network theory. One of the key issues of VANETs is how to use traffic lights to optimise vehicle mobility. Rodrigues et al. (2021) proposed a stochastic Petri net (SPN) model to evaluate the performance of collaborative intelligent traffic lights. In VANETs, communication between vehicles is called a vehicle-to-vehicle (V2V) communication, and vehicle to RSU is called a vehicle-to-infrastructure (V2I) communication.

Every vehicle must install an onboard unit (OBU) as a radio transceiver to communicate with other legal devices. They are also fitted with global positioning system (GPS) devices and sensors that detect and collect data then send it to other vehicles (Prado et al., 2018). RSU act as a bridge that allows OBU to communicate with TA. Communication between OBU and RSU is based on the dedicated short-range communications (DSRC) protocol (ASTM E2213-03, 2010). Meanwhile, TA acts as the trust and security management center of the entire VANETs entities. Its job, including registration and parameters generation for RSUs and OBUs after they join the network. It is also revoking nodes in the case of vehicles broadcasting fraud messages or performing malicious behaviour.

In this new environment, vehicles may broadcast a traffic-related message to hundreds of other vehicles (V2V) or RSUs (V2I) every 100–300 milliseconds (Prado et al., 2018). The OBU will broadcast information such as position, speed, and direction to improve the road environment, traffic safety, reduce traffic congestion, and vehicle mutual understanding of local traffic circumstances (Xie et al., 2020, 2021; Zhu et al., 2014). Despite all of the benefits, security, and privacy becomes significant concerns due to its unique properties, such as open wireless communication, quick topology shift, high mobility, time-critical, and many messages interchange. The most common way of ensuring the confidentiality of large message exchanges on VANETs is to sign each message with a digital signature. Meanwhile, a successful anonymous authentication technique for VANETs must consider the VANETs' tight time limitations.

Shamir (1991) proposed a new concept called ID-based public-key cryptography (ID-PKC) to simplify the complicated certificate management in traditional public key infrastructure (PKI) systems. An identity-based batch signature (IBS) scheme was proposed by Boneh and Franklin (2001) as a refinement of the PKI scheme for a secure and reliable authentication method. Their approach was based on advancements in elliptic curves using bilinear pairings like Weil and Tate. As a result, the cryptographic research community has paid close attention to the study of ID-based cryptography employing bilinear pairings (Yin et al., 2021). IBS utilises anonymous identities and corresponding private keys of the user for signing each traffic-related message. These pseudo-identities and users' private keys are generated by the tamper-proof device (TPD), installed in the OBU of every vehicle to satisfy the user identity privacy. IBS does not need any signature certificate, such as PKI and elliptic curve digital signature algorithm (ECDSA) for message authentication. Hence, the computation and communication overhead can be kept low. There is also no public key distribution with associated certificates and avoid the management of certificate revocation list (CRL) that causes a heavy overhead (Lu et al., 2019).

Figure 1 The topology of VANETs



For a better understanding, the rest of this article is arranged as follows. In Section 2, we provide the related work. Section 3 discusses the system model, concepts of bilinear maps, and the common security and privacy requirements in VANETs. Then, the review of Cui and Tu's (2019) IBDS and IBCPPA schemes are provided in Section 4 and Section 5, respectively. In Section 6, we discuss the cryptanalysis of Cui and Tu's (2019) scheme and our correction of their writing errors. The construction of our improved scheme is presented in Section 7, and its security analysis is described in Section 8. In Section 9, we provide the performance analysis. Finally, the conclusion is conveyed in Section 10.

2 Related work

A number of IBS schemes for VANETs (Zhang et al., 2008, 2011; Lee and Lai, 2013; Bayat et al., 2015; Jianhong et al., 2014; Tzeng et al., 2017; Cui and Tu, 2019; Wang et al., 2020; Ali et al., 2020; Liu and Wang, 2021) have been devised since the concept of IBS itself was

proposed by Boneh and Franklin (2001). Zhang et al. (2008) proposed a novel identity-based batch verification (IBV) scheme with bilinear pairing to deal with a bottleneck verification issue in vehicular sensor networks (VSNs). This method was updated in 2011 with an improvement in group testing to identify illegal signatures that could be appeared in the batch (Zhang et al., 2011). Lee and Lai (2013) published a paper that tries to point out the vulnerability of Zhang et al.'s (2011) IBV scheme. Lee and Lai (2013) revealed that Zhang et al.'s (2011) scheme suffered from a replaying attack and did not achieve the non-repudiation requirements. Success in addressing the security issue, Lee and Lai (2013) also improve the message verification (MV) process of Zhang et al. (2011), resulting in a more efficient computation cost.

Several improvements work towards the performance issue of Lee and Lai's (2013) scheme has been published in the following year (Jianhong et al., 2014; Bayat et al., 2015; Tzeng et al., 2017). Jianhong et al. (2014) showed that Lee and Lai's (2013) scheme was vulnerable to forgery attacks, traceability attacks, and message-signature repudiation. Bayat et al. (2015) also found if Lee and Lai's (2013) scheme suffers from an impersonation attack, where the adversaries can generate a valid signature on behalf of the legitimate user. They claimed that these flaws come from the private keys' weakness, so they make improvements in this area. Meanwhile, Tzeng et al. (2017) published a work that reveals the vulnerability of Lee and Lai's (2013) scheme towards identity privacy-preserving attack, forgery attack, and anti-traceability attack. Therefore, Tzeng et al. (2017) proposed a more secure and more efficient IBV scheme.

Recently, Cui and Tu (2019) published a bilinear pairing identity-based scheme that tries to improve Jianhong et al.'s (2014) and Bayat et al.'s (2015) IBV schemes. They stated that both Jianhong et al.'s and Bayat et al.'s schemes are very complicated and inefficient due to the utilisation of double-secret keys. Therefore, they construct a new identity-based digital signature (IBDS) scheme using bilinear pairings to form a new identity-based conditional privacy-preserving authentication (IBCPPA) scheme for VANETs without the need for a map-to-point hash function or double-secret keys.

However, we found that Cui and Tu's IBCPPA scheme also suffered a non-repudiation attack. A malicious user $\mathcal{M}$ can broadcast false information to deceive other drivers and dispute the action. So, the TA cannot trace him/her by signature. Therefore, this article proposes an improved Cui and Tu authentication scheme to withstand the attack.

3 Preliminaries

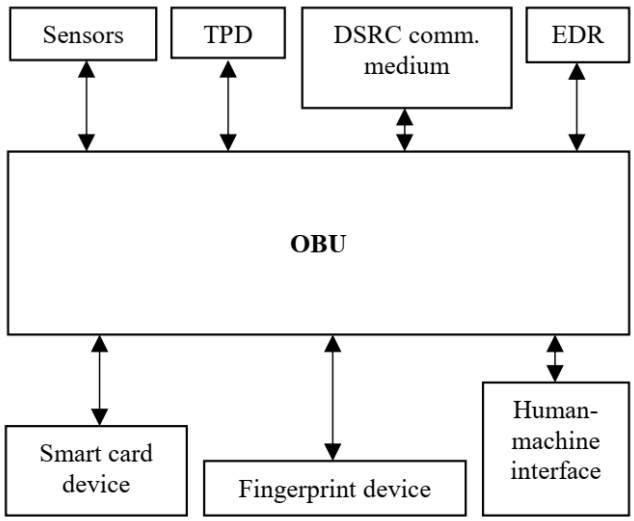
This section discusses the system model, concept of bilinear maps, complexity assumptions, and basic security and privacy requirements in VANETs.

3.1 System model

Zhang et al. (2008) established the two-layer concept in VANETs, with TA on top, while RSU and OBUs on the bottom layer, as shown in Figure 1. We have briefly described each entity's task and function in Section 1. To produce an effective decision movement, the OBU in the vehicle will have communication sensors, TPD, DSRC communication medium, event data recorder (EDR), smart card and fingerprint devices, and a human-machine interface (Vijayakumar et al., 2016). As we can see in Figure 2, the TPD and the OBU are different modules with different functionalities. TPD is where sensitive security materials such as master keys are kept. TPD is in charge of all cryptographic operations, such as message signing and key updates. As a result, legal OBUs have a difficult time extracting their master keys from their TPDs (Tzeng et al., 2017). In this paper, we will deal with both of them in the execution of several main parameters. We assume the following in our VANETs ecosystem (Cahyadi and Hwang, 2021):

- TA is uncompromised and fully trusted.
- Only TA that can reveal the real identity of RSUs and OBUs.
- TA-RSU communicates through a secured wireline network. Meanwhile, communication between RSU-vehicle is on the open wireless channel.
- RSUs are semi-trusted, which means they could be compromised.
- TPD is assumed to be credible, and no information about them has ever been revealed.

Figure 2 Components in vehicle's side



3.2 The bilinear maps

The bilinear map $\hat{e}$ can be obtained from the modified Weil pairing (Boneh and Franklin, 2001) or Tate pairing (Miyaji

et al., 2001) on elliptic curves. Its security and complexity lie on the computational Diffie-Hellman problem (CDHP), which is believed to be difficult to solve (Boneh et al., 2004). Let G_1 be denoted as a cyclic additive group generated by P, and G_2 is a cyclic multiplicative group with the same prime order q. Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear map if it satisfies the following properties:

1 Bilinear: For all P, Q, $R \in G_1$, we have $\hat{e}$ (Q, $P + R$) = $\hat{e}$ (P, $Q + R$) = $\hat{e}$ (Q, P) $\cdot$ $\hat{e}$ (Q, R). For any a, $b \in Z_q^*$, $\hat{e}$ (aQ, bP) = $\hat{e}$ (bQ, aP) = $\hat{e}$ (Q, P)^{ab}.

2 Non-degenerate: $\hat{e}$ (P, Q) $\neq$ 1.

3 Computable: For any P, $Q \in G_1$, there is an efficient algorithm to compute $\hat{e}$ (P, Q).

As G_1 is a cyclic additive group generated by P, given P, aP, $bP \in G_1$, and a, $b \in Z_q^*$ are unknown values. The CDHP is hard, because there is no polynomial time algorithm that can discover $abP \in G_1$.

3.3 Security and privacy requirements

Generally, the communication between entities in VANETs should meet the following security and privacy requirements: message authentication, non-repudiation, identity privacy-preserving, traceability, unlinkability, and replaying attack and impersonation attack resistance. The following are the detailed description of security and privacy requirements that must hold in VANETs (Cahyadi and Hwang, 2021).

1 Message authentication: The implementation of the message authentication method is intended to allow the vehicle or RSU to differentiate the original message from the bogus message. Furthermore, message authentication is also applied to resist modification and impersonation attacks.

2 Non-repudiation: This requirement will give the message receiver a guarantee about the integrity and authenticity of the information they receive. The sender of the message cannot deny the information they have sent.

3 Identity privacy-preserving: A sender of a message should be anonymous within a set of potential senders. In IBV, the vehicles' real identities will be converted to anonymous identities through TPD assistance. Therefore, without knowing the private master key of the TPD, an adversary cannot reveal the legitimate users' real identities. However, to reach accountability, only conditional anonymity is possible in VANETs, which are also related to traceability.

4 Traceability: The TA should be able to reveal the real identities of the users' anonymous identities in the case of a dispute. Traceability is also called conditional anonymity.

5 Unlinkability: An adversary vehicle (or RSU) should not link two or more subsequent pseudonym messages of the same vehicle.

6 Replaying attack resistance: The networks could endure a passive data capture and subsequent retransmission to produce an unauthorised message by the adversaries.

7 Impersonation attack resistance: The networks could endure towards the attacker trying to assume or impersonate the identity of the legitimate vehicles in VANETs, to generate the signature for any messages.

4 Review of Cui and Tu's IBDS scheme

This section elaborates on how Cui and Tu's (2019) authentication scheme works. Their batch verification authentication scheme is designed based on the IBCPPA schemes, initially proposed by Zhang et al. (2008). Meanwhile, the IBCPPA itself is constructed from their modified IBDS scheme, originally proposed by Schnorr (1991) and Boneh et al. (2004). To provide a clear understanding, notations throughout this paper are presented in Table 1.

Table 1 Notations of this paper

Notation	*Definition*
G_1	A cyclic additive group
G_2	A cyclic multiplicative group
$\hat{e}$	The bilinear map
P	Generator of cyclic group G_1
q	The prime order of G_1 and G_2
$h_1(\cdot)$, $h_2(\cdot)$	One-way hash functions
$H(\cdot)$	A map-to-point hash function
V_i	The i^{th} vehicle
σ_i	A signature of V_i
M_i	Original message sent by V_i
T_i	A timestamp generated by V_i
s	The master key of TA
P_{pub}	The public key of TA
RID_i	Real identity of V_i
PWD_i	Password of V_i
PID_i	Pseudo-identity of V_i
$\|$	Message concatenation operation
$\oplus$	Exclusive-OR operation

Cui and Tu's (2019) IBDS scheme consists of four phases: *setup*, *extract*, *sign* and *verification*.

4.1 Setup

In this phase, the key generator centre (KGC) generates some parameters.

1 KGC chooses a large prime number q, then generates additive and multiplicative groups of G_1 and G_2,

respectively. Afterwards, let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear map.

2 KGC chooses a random number $s \in Z_q^*$ as its master key, and subsequently computes $P_{pub} = sP$, as its public key.

3 KGC picks two one-way hash functions $h_1(\cdot)$, $h_2(\cdot) : \{0,1\}^* \rightarrow Z_q^*$, and a map-to-point hash function $H(\cdot) \rightarrow G_1$.

4 KGC publishes public parameters $\{q, G_1, G_2, \hat{e}, P, P_{pub}, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ to vehicles, and securely stores s.

4.2 Extract

KGC generates vehicles' private key sk_i after receiving their pseudo-identity PID_i.

1 KGC pick a random number $t_i \in Z_q^*$, and calculates $X_i = t_i P$.

2 KGC computes $h_i = h_1(PID_i \parallel X_i)$ and $s_i = t_i + h_i s \bmod q$.

3 KGC sends $sk_i = s_i + X_i$ to vehicle.

4.3 Sign

Vehicle generates a signature after receiving message M_i.

1 Vehicle selects a random number $r_i \in Z_q^*$, and computes $R_i = r_i P$.

2 Vehicle computes $k_i = h_2(PID_i \parallel R_i \parallel M_i \parallel X_i)$ and $S_i = (s_i + k_i r_i)Q$. Here Q is a base point on a curve as a generator.

3 Vehicle computes and sends $\sigma_i = \{X_i, R_i, S_i\}$ as the signature of M_i to verifier.

4.4 Verification

Since in Cui and Tu (2019) the communications done in V2I manners, so the verifier is RSU. Upon receiving a signature σ_i, RSU computes h_i, k_i, and $Q = H(P_{pub})$. Next, RSU will check whether,

$$\begin{aligned}\hat{e}(S_i, P) &= \hat{e}((s_i + k_i r_i)Q, P) \\ &= \hat{e}((t_i + h_i s + k_i r_i)Q, P) \\ &= \hat{e}((t_i + h_i s + k_i r_i)P, Q) \\ &= \hat{e}(t_i P + h_i sP + k_i r_i P, Q) \\ &= \hat{e}(X_i + h_i P_{pub} + k_i R_i, Q)\end{aligned}$$

holds or not. If the condition holds, then the message is legal and unaltered.

Meanwhile, in the batch verification, when number of signatures $\sigma_1 = \{X_1, R_1, S_1\}$, $\sigma_2 = \{X_2, R_2, S_2\}$, ..., $\sigma_n = \{X_n, R_n, S_n\}$ come to RSU, it will check whether,

$$\begin{aligned}\hat{e}\left(\sum_{i=1}^{n} S_i, P\right) &= \hat{e}\left(\sum_{i=1}^{n}(s_i + k_i r_i)Q, P\right) \\ &= \hat{e}\left(\sum_{i=1}^{n}(t_i + h_i s + k_i r_i)Q, P\right) \\ &= \hat{e}\left(\sum_{i=1}^{n}(t_i + h_i s + k_i r_i)P, Q\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} t_i P + h_i sP + k_i r_i P, Q\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} X_i + h_i P_{pub} + k_i R_i, Q\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} X_i + \left(\sum_{i=1}^{n} h_i\right) P_{pub} \right. \\ &\quad \left. + \left(\sum_{i=1}^{n}(k_i R_i), Q\right)\right)\end{aligned}$$

holds or not. If the condition holds, then the message is legal and unaltered.

5 Review of Cui and Tu's IBCPPA scheme

Using the IBDS scheme described in the previous section as a building block, Cui and Tu's IBCPPA scheme consists of three phases: *key generation and pre-distribution* (KGPD), *pseudo-identity generation and message signing* (PIDGMS), and *MV*.

5.1 KGPD phase

TA generates public system parameters for RSUs and vehicles. The first three steps are similar with the IBDS scheme in the previous section, followed by:

1 TA assigns a unique real identity RID, and password PWD to each vehicle. Then pre-loads $\{RID, PWD, s\}$ into every vehicles' TPD.

2 TA publishes public parameters $\{q, G_1, G_2, \hat{e}, P, Q, P_{pub}, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ to vehicles and RSUs, while $Q = H(P_{pub})$.

5.2 PIDGMS phase

To satisfy user privacy, the TPD of each vehicle performs the pseudo-identity generation and signature generation.

1 The vehicle V_i inputs its RID and PWD to the TPD. If both RID and PWD match the stored values, the request will proceed, otherwise refused.

2 After being verified, TPD picks a random number $t_i \in Z_q^*$, and computes pseudo-identity PID_i, where $PID_i = \{PID_{i,1}, PID_{i,2}\}$.

$$PID_{i,1} = t_i P$$

$PID_{i,2} = RID_i \oplus h_1(t_i P_{pub})$

With a current timestamp T_i, TPD also compute h_i and s_i with the similar operation to the IBDS scheme.

3 TPD generates a temporary private key $\{PID_i, s_i\}$, and sends it to OBU.

4 Given a message M_i, V_i chooses a random integer $r_i \in Z_q^*$ and compute R_i, k_i, and S_i with the similar operation to the IBDS scheme.

5 Finally, V_i sends the final message $\{PID_i, R_i, S_i, M_i, T_i\}$ to the nearest RSU.

5.3 MV phase

The MV process divided into single and batch verification process. When RSU receives a final message $\{PID_i, R_i, S_i, M_i, T_i\}$ from nearby vehicles, it will check the timestamp T_i. If $T_{RSU} - T_i \leq \Delta T$, RSU continues the verification process, otherwise reject the message. T_{RSU} denotes the received time of the message at RSU, while ΔT denotes the pre-defined endurable transmission delay.

In the single verification process, RSU checks $\{PID_i, R_i, S_i, M_i, T_i\}$ by verifying whether:

$$\begin{aligned}\hat{e}(S_i, P) &= \hat{e}((s_i + k_i r_i)Q, P) \\ &= \hat{e}((t_i + h_i s + k_i r_i)Q, P) \\ &= \hat{e}((t_i + h_i s + k_i r_i)P, Q) \\ &= \hat{e}(t_i P + h_i s P + k_i r_i P, Q) \\ &= \hat{e}(PID_i + h_i P_{pub} + k_i R_i, Q)\end{aligned}$$

If the equation holds, then the final message is legal and unaltered.

In the batch MV, if the RSU obtain number of messages, denoted as $\{PID_1, R_1, S_1, M_1, T_1\}$, $\{PID_2, R_2, S_2, M_2, T_2\}$, ..., $\{PID_n, R_n, S_n, M_n, T_n\}$, it can verifies the messages' validity simultaneously. When RSU obtains numbers of messages, it will verify them by checking if:

$$\begin{aligned}\hat{e}\left(\sum_{i=1}^{n} S_i, P\right) &= \hat{e}\left(\sum_{i=1}^{n}(s_i + k_i r_i)Q, P\right) \\ &= \hat{e}\left(\sum_{i=1}^{n}(t_i + h_i s + k_i r_i)Q, P\right) \\ &= \hat{e}\left(\sum_{i=1}^{n}(t_i + h_i s + k_i r_i)P, Q\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} t_i P + h_i s P + k_i r_i P, Q\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} T_i + h_i P_{pub} + k_i R_i, Q\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} PID_i + \left(\sum_{i=1}^{n} h_i\right) P_{pub} \right. \\ &\quad \left. + \left(\sum_{i=1}^{n}(k_i R_i), Q\right)\right)\end{aligned}$$

holds or not. If the equation holds, then the final messages are legal and unaltered.

6 Cryptanalysis of Cui and Tu's scheme

This section discusses the cryptanalysis of Cui and Tu's scheme, followed by our correction of their writing errors.

6.1 Problem in the non-repudiation attack

In this section, we show that Cui and Tu's scheme is vulnerable to signature non-repudiation attacks. As mentioned in Section 2, Lee and Lai (2013) pointed out Zhang et al.'s (2008) scheme did not achieve the signature non-repudiation. Here, we use the same method as described by Lee and Lai (2013) and Hwang et al. (2000, 2001). Since Cui and Tu's batch verification scheme did not employ a random vector to distinguish every message in it, a malicious user $\mathcal{M}$ can deny his/her signatures. According to Yoon et al. (2005), based on the number of signers and messages, batch verification could be classified into three following types:

Type 1 Multiple signatures on a single message generated by multiple signers.

Type 2 Multiple signatures on multiple messages generated by a single signer.

Type 3 Multiple signatures on multiple messages generated by multiple signers, where each message is signed by a different user.

We provide two methods to show that M can forge individual signatures and make a false batch verification valid. In this case, we consider a *type 2* batch verification classified by Yoon et al. (2005). We assume that $\mathcal{M}$ sends three pairs of messages $\{PID_1, R_1, S_1, M_1, T_1\}$, $\{PID_2, R_2, S_2, M_2, T_2\}$, $\{PID_3, R_3, S_3, M_3, T_3\}$ to RSU.

In the first method, $\mathcal{M}$ can swaps the contents of those messages to become $\{PID_1, R_1, S_2, M_1, T_1\}$, $\{PID_2, R_2, S_3, M_2, T_2\}$, $\{PID_3, R_3, S_1, M_3, T_3\}$. When RSU receives the messages, it will prove the correctness of the signature summation by checking:

$$\begin{aligned}\hat{e}\left(\sum_{i=1}^{n} S_i, P\right) &= \hat{e}(S_2 + S_3 + S_1, P) \\ &= \hat{e}(S_1 + S_2 + S_3, P) \\ &= \hat{e}\left(\sum_{i=1}^{3} PID_i + \left(\sum_{i=1}^{3} h_i\right) P_{pub} \right. \\ &\quad \left. + \left(\sum_{i=1}^{3}(k_i R_i), Q\right)\right)\end{aligned}$$

From the above operation, when RSU uses a batch verification process, it will consider that those changes are legal. Although the orders of those signatures have been changed, their sum remains the same. For this reason, $\mathcal{M}$ can deny his/her signatures.

In the second method, let $S_i^{'} = a_i \times S_i$, with i = 1, 2, ..., n, and $\sum_{i=1}^{n} a_i = 1$. Since $\mathcal{M}$ sends three messages $\{PID_1,\ R_1,\ S_1,\ M_1,\ T_1\}$, $\{PID_2,\ R_2,\ S_2,\ M_2,\ T_2\}$, $\{PID_3,\ R_3,\ S_3,\ M_3,\ T_3\}$ to RSU, and let $S_1^{'}$ = 0.3 S_1, $S_2^{'}$ = 0.5 S_2, and $S_3^{'}$ = 0.2 S_3, it will proves the correctness of the signatures summation by checking:

$$\begin{aligned}\hat{e}\left(\sum_{i=1}^{n} S_i, P\right) &= \hat{e}(0.3S_1 + 0.5S_2 + 0.2S_3, P)\\ &= \hat{e}(S_1 + S_2 + S_3, P)\\ &= \hat{e}\left(\sum_{i=1}^{3} PID_i + \left(\sum_{i=1}^{3} h_i\right) P_{pub}\right.\\ &\quad \left. + \left(\sum_{i=1}^{3} (k_i R_i), Q\right)\right)\end{aligned}$$

Since the above equation holds, RSU considers the signatures $S_1^{'}$, $S_2^{'}$, and $S_3^{'}$ are legal to $\{PID_1,\ R_1,\ S_1,\ M_1,\ T_1\}$, $\{PID_2,\ R_2,\ S_2,\ M_2,\ T_2\}$, $\{PID_3,\ R_3,\ S_3,\ M_3,\ T_3\}$. Although $\mathcal{M}$ has forged all the signatures by gives it a particular value, but their sum remains the same. By this scenario, $\mathcal{M}$ also can deny his/her signatures.

6.2 Corrections

In our opinion, some mistakes in Cui and Tu (2019) need to be addressed. We describe them in the following items:

1 In the *extract* phase (IBDS scheme) of the original paper (Cui and Tu, 2019), notation T_i has not seemingly interpret a timestamp, since it is made of $T_i = t_i P$. Therefore, for the sake of consistency, in Subsection 4.2, we change notation T_i of Cui and Tu's IBDS scheme into $X_i = t_i P$, only to differentiate it to T_i in the IBCPPA scheme. Meanwhile, notation T_i in the IBCPPA scheme is considered as a timestamp.

2 In the *extract* phase (IBDS scheme) of the original paper (Cui and Tu, 2019), the s_i is given as $s_i = t_i + h_i \bmod q$. However, referring to the s_i in the PIDGMS phase, it written as $s_i = t_i + h_i s \bmod q$. Hence, in Subsection 4.2 we write it as the latter mentioned.

3 Operation $S_i = (s_i + k_i r_i)Q$ in the IBDS scheme of the original paper (Cui and Tu, 2019) should be addressed earlier in the *sign* phase, not in the *verification* phase. Notation $k_i = h_2(PID_i \parallel R_i \parallel M_i \parallel T_i)$ also should be addressed before the *verification* phase, since it is used to compute S_i. In this paper, we have modified them in Subsection 4.3.

4 In the *sign* phase (IBDS scheme) of the original paper (Cui and Tu, 2019), the signature of the message M_i is confusingly written as $\sigma_j = \{T_j,\ R_j,\ S_j\}$. Since the subscript notation of "j" is not described before, so, it should be written as $\sigma_i = \{T_i,\ R_i,\ S_i\}$ (as shown in Subsection 4.3).

7 Our improvement

The robustness of security aspects in the VANETs information dissemination process strongly relies on its authentication scheme. The improved scheme is the same as the original Cui and Tu's IBCPPA scheme except for the batch verification phase. To resolve the aforementioned issue in Subsection 6.1, before the batch verification process begins, RSU should generate a random vector v_i, where i = 1, 2, ..., n, to ensure the non-repudiation of signatures. This concept is obtained from the small exponent test conducted in Bellare et al. (1998) and Horng et al. (2013). The value v_i ranges between 1 and 2^l, where l is a security parameter with a small value and does not make any computational overhead (Tzeng et al., 2017). Parameter l is set to the maximum probability of 2^{-l}, so even with a single signature in the batch is wrong, it still can be detected, except with the possibility 2^{-l}. Lee and Lai (2013) improve Zhang et al.'s (2011) scheme in such a similar way.

By implementing v_i, the malicious user cannot perform two operations in Section 6 to deceive the receiver. If

$$\begin{aligned}\hat{e}\left(\sum_{i=1}^{n} v_i S_i, P\right) &= \hat{e}\left(\sum_{i=1}^{n} v_i (s_i + k_i r_i)Q, P\right)\\ &= \hat{e}\left(\sum_{i=1}^{n} v_i (t_i + h_i s + k_i r_i)Q, P\right)\\ &= \hat{e}\left(\sum_{i=1}^{n} v_i (t_i + h_i s + k_i r_i)P, Q\right)\\ &= \hat{e}\left(\sum_{i=1}^{n} v_i t_i P + h_i s P + k_i r_i P, Q\right)\\ &= \hat{e}\left(\sum_{i=1}^{n} v_i T_i + h_i P_{pub} + k_i R_i, Q\right)\\ &= \hat{e}\left(\sum_{i=1}^{n} v_i PID_i + \left(\sum_{i=1}^{n} v_i h_i\right) P_{pub}\right.\\ &\quad \left. + \left(\sum_{i=1}^{n} v_i (k_i R_i), Q\right)\right)\end{aligned}$$

then the final messages are legal and unaltered.

8 Security analysis

This section analyses the improved Cui and Tu's (2019) IBCPPA scheme security, particularly in the batch

verification phase. Since our focus is to provide a vector parameter v_i in the batch verification process to prevent non-repudiation attacks, we first discuss this matter. Meanwhile, the other basic security requirements, including identity privacy-preserving, traceability, and resistance to replay attacks, are relatively the same.

8.1 Non-repudiation

As discussed in Section 7, we used a v_i to avoid user swap of the M_i and σ_i. If a malicious user wants to deny the signatures by swapping M_i and σ_i, his/her signatures will result in the batch MV failing. In Section 7, we perform the small exponent test that previously conducted in Bellare et al. (1998) and Horng et al. (2013). Givenly P is a generator in G_1, we have $\{S_1, y_1\}$, $\{S_2, y_2\}$, ..., $\{S_n, y_n\}$, with $S_i \in Z_q^*$ and $y_i \in G_1$, check if $\forall i \in \{1, 2, ..., n\}$: $\hat{e}(S_i, P) = \hat{e}(y_i, Q)$, by doing the following steps:

- Selects random parameter $l_1, l_2, ..., l_n \in \{0, 1\}^l$.
- Computes $A = \sum_{i=1}^{n} l_i y_i$ and $B = \sum_{i=1}^{n} l_i S_i$.
- If $\hat{e}(B, P) = \hat{e}(A, Q)$, then accepts, otherwise rejects.

The batch instance will be (S_1, y_1), (S_2, y_2), ..., (S_n, y_n), with $y_i = (PID_{i,1} + h_i P_{pub} + k_i R_i)$. The verification of the signature consists of checking operation that $\hat{e}(S_i, P) = \hat{e}(y_i, Q)$. If $\mathcal{M}$ wants to make some false multiple digital signatures S_i valid, he/she must make those operation holds. Since $\mathcal{M}$ did not know the values of l that leads to the value of v_i, it is difficult for $\mathcal{M}$ to make $\hat{e}(S_i, P) = \hat{e}(y_i, Q)$ holds.

8.2 Identity privacy-preserving

The improved protocol inherits the same measure of RID_i to PID_i conversion from the original (Zhang et al., 2008) IBV scheme, that also relatively similar to the latter (Lee and Lai, 2013; Jianhong et al., 2014; Bayat et al., 2015; Tzeng et al., 2017). To get a $PID_i = \{PID_{i,1}, PID_{i,2}\}$, user must input their RID_i and PWD_i, then verified by the TPD. Since $PID_{i,1} = t_i P$ and $PID_{i,2} = RID \oplus h_1(t_i P_{pub})$, so a malicious user $\mathcal{M}$ can try to retrieve RID_i by doing $RID_i = PID_{i,2} \oplus h_1(sPID_{i,1})$. However, since we believe that CDHP used in the bilinear pairing operation is hard (Zhang et al., 2008; Boneh et al., 2004), hence we argue that $\mathcal{M}$ cannot obtain any users' real identity RID easily.

8.3 Traceability

Related to the previous elaboration where $RID_i = PID_{i,2} \oplus h_1(sPID_{i,1})$, since only TA who know the value of s, so in the case of dispute, it is only TA who can reveal the RID_i of all vehicles in the network.

8.4 Resistance to replay attack

Since $k_i = h_2(PID_i \parallel R_i \parallel M_i \parallel T_i)$ and final message $\{PID_i, R_i, S_i, M_i, T_i\}$ in the PIDGMS phase employ a timestamp T_i, RSU will receive the latest message from vehicles, and get noticed when $\mathcal{M}$ try to replay the message by verifying the freshness of the T_i.

9 Performance analysis

In this section, we mainly discuss the comparison of computational complexity between Cui and Tu's and our improved scheme, as presented in Table 2. Let SC is scalar multiplication cost, PC is pairing operation cost, and HC is map-to-point hash function cost. Keep in mind, the pairing operation cost PC is higher than the other two (SC and HC).

Table 2 Comparison of the computational complexity

Scheme	*Single verification*	*Batch verification*
Cui and Tu (2019)	$3PC + 2SC$	$3PC + 2nSC$
Ours	$3PC + 2SC$	$3PC + 2nSC$

From Table 2, we can see both of Cui and Tu's and our improved scheme use the same $3PC + 2SC$ and $3PC + 2nSC$ operation in single and batch verification phases, respectively. In single verification phase, the $3PC$ calculation is obtained since in both schemes needs to calculate $\hat{e}(S_i, P) = \hat{e}(PID_i + h_i P_{pub} + k_i R_i, Q)$. We can divide $\hat{e}(PID_i + h_i P_{pub} + k_i R_i, Q)$ into $\hat{e}(PID_{i,1}) \cdot \hat{e}(h_i P_{pub}) \cdot \hat{e}(k_i R_i, Q)$, hence it is $3PC$ (pairing operation cost). Meanwhile, the $2SC$ calculation is resulted from $h_i P_{pub}$ and $k_i R_i$.

In the batch verification process, the number of pairing operation cost is the same of $3PC$. Meanwhile, the scalar multiplication cost is based on the number of n in $\hat{e}(\sum_{i=1}^{n} v_i PID_i + (\sum_{i=1}^{n} v_i h_i) P_{pub} + (\sum_{i=1}^{n} v_i (k_i R_i), Q))$. Although our improved scheme has to compute $v_i S_i$, $v_i PID_i$, $v_i h_i$, and $v_i (k_i R_i)$, as mentioned in Section 7, the range of v_i is very small, hence its computation is negligible.

10 Conclusions and future work

In this paper, we show that the IBCPPA scheme proposed by Cui and Tu (2019) is vulnerable to the non-repudiation attack. Two approaches described in Subsection 6.1 show that a malicious user can broadcast wrong messages to mislead the RSU and deny its behaviour. To overcome the threat, we include a random vector v_i to distinguish every message and signature in the batch without any computational overhead effect. Therefore, by preserving the performance efficiency of the original paper, we have given the scheme an extra security feature. For our future work, we'd like to improve the feature of the batch verification

mechanism for VANETs, such as the illegal signatures identification mechanism. We want to improve efficiency by this technique, mainly when the batch's sum of illegal signatures appears.

Acknowledgements

This research is partially supported by The Ministry of Science and Technology, Taiwan 288 (ROC), under contract no. MOST 108-2410-H-468-023 and MOST 108-2622-8-468-001-TM1.

References

Ali, I., Lawrence, T. and Li, F. (2020) 'An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs', *Journal of Systems Architecture*, Vol. 103, p.101692.

ASTM E2213-03 (2010) *Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems 8212; 5 GHz Band Dedicated Short Range Communications DSRC Medium Access Control (MAC) and Physical Layer (PHY) Specifications* [online] http://www.astm.org/Standards/E2213.htm.

Bayat, M., Barmshoory, M., Rahimi, M. and Aref, M.R. (2015) 'A secure authentication scheme for VANETs with batch verification', *Wireless Networks*, Vol. 21, pp.1733–1743.

Bellare, M., Garay, J.A. and Rabin, T. (1998) 'Fast batch verification for modular exponentiation and digital signatures', in Nyberg, K. (Ed.): *Advances in Cryptology – Eurocrypt'98, LNCS*, Vol. 2139, pp.213–229.

Boneh, D. and Franklin, M. (2001) 'Identity-based encryption from the weil pairing', in Kilian, J. (Ed.): *Advances in Cryptology – CRYPTO 2001, LNCS*, Vol. 2139, No. 19, pp.213–229.

Boneh, D., Lynn, B. and Shacham, H. (2001) 'Short signatures from the Weil pairing', *Journal of Cryptology*, Vol. 17, pp.297–319.

Cahyadi, E.F. and Hwang, M-S. (2021) 'An improved efficient anonymous authentication with conditional privacy-preserving scheme for VANETs', *PLoS ONE*, Vol. 16, No. 9, p.e0257044.

Cui, J. and Tu, H. (2019) 'Efficient authentication scheme for vehicular ad-hoc networks with batch verification using bilinear pairings', *International Journal of Embedded Systems*, Vol. 11, No. 3, pp.363–373.

Faisal, S.M. and Zaidi, T. (2020) 'Timestamp based detection of sybil attack in VANET', *International Journal of Network Security*, Vol. 22, No. 3, pp.399–410.

Horng, S-J., Tzeng, S-F., Pan, Y., Fan, P., Wang, X., Li, T. and Khan, M.K. (2013) 'B-SPECS+: batch verification for secure pseudonymous authentication in VANET', *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 11, pp.1860–1875.

Hwang, M-S., Lin, I-C. and Hwang, K-F. (2000) 'Cryptanalysis of the batch verifying multiple RSA digital signatures', *Informatica*, Vol. 11, No. 1, pp.15–19.

Hwang, M-S., Lee, C-C. and Tang, Y-L. (2001) 'Two simple batch verifying multiple digital signatures', in Qing, S., Okamoto, T. and Zhou, J. (Eds.): *Information and Communications Security, ICICS 2001, LNCS*, Vol. 2229, pp.233–237.

Jianhong, Z., Min, X. and Liying, L. (2014) 'On the security of a security batch verification with group testing for VANET', *International Journal of Network Security*, Vol. 16, No. 4, pp.313–320.

Jindal, V. and Bedi, P. (2018) 'High performance adaptive traffic control for efficient response in vehicular ad hoc networks', *Int. J. Computational Science and Engineering*, Vol. 16, No. 4, pp.390–400.

Lee, C-C. and Lai, Y-M. (2013) 'Toward a secure batch verification with group testing for VANET', *Wireless Networks*, Vol. 9, pp.1441–1449.

Liu, F. and Wang, Q. (2021) *An Identity-based Batch Verification Scheme for VANETs Based on Ring Signature with Efficient Revocation*, arXiv preprint arXiv:2103.07653.

Lu, Z., Qu, G. and Liu, Z. (2019) 'A survey on recent advances in vehicular network security, trust, and privacy', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 20, No. 2, pp.760–776.

Miyaji, A., Nakabayashi, M. and Takano, S. (2001) 'New explicit conditions of elliptic curve traces for FR-reduction', *IEICE Transactions on Fundamentals*, Vol. E84, No. A, pp.1234–1243.

Prado, A., Ruj, S., Stojmenovic, M. and Nayak, A. (2018) 'Applying transmission-coverage algorithms for secure geocasting in VANETs', *International Journal of Computational Science and Engineering*, Vol. 16, No. 1, pp.17–26.

Rodrigues, L., Neto, F., Gonçalves, G., Soares, A. and Silva, F.A. (2021) 'Performance evaluation of smart cooperative traffic lights in VANETs', *International Journal of Computational Science and Engineering*, Vol. 24, No. 3, pp.276–289.

Schnorr, C.P. (1991) 'Efficient signature generation by smart cards', *Journal of Cryptology*, Vol. 4, pp.161–174.

Shamir, A. (1984) 'Identity-based cryptosystem and signatures schemes', in Blakley, G.R. and Chaum, D. (Eds.) *Advances in Cryptology, CRYPTO 1984, LNCS*, Vol. 196, pp.47–53.

Tzeng, S-F., Horng, S-J., Li, T., Wang, X., Huang, P-H. and Khan, M.K. (2017) 'Enhancing security and privacy for identity-based batch verification scheme in VANETs', *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 4, pp.3235–3248.

Vijayakumar, P., Azees, M., Kannan, A. and Deborah, L.J. (2016) 'Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, No. 4, pp.1015–1028.

Wang, C., Dai, Z., Zhao, D. and Wang, F. (2020) 'A novel identity-based authentication scheme for IoV security', *International Journal of Network Security*, Vol. 22, No. 4, pp.627–637.

Xie, P.S., Han, Feng, T., Yan, Y. and Ma, G.Q. (2020) 'A method of constructing arc edge anonymous area based on LBS privacy protection in the internet of vehicles', *International Journal of Network Security*, Vol. 22, No. 2, pp.275–282.

Xie, P.S., Fu, C., Wang, X., Feng, T. and Yan, Y. (2021) 'Malicious attack pevention model of internet of vehicles based on IOV-SIRS', *International Journal of Network Security*, Vol. 23, No. 5, pp.835–844.

Yin, S., Li, H., Karim, S. and Sun, Y. (2021) 'ECID: elliptic curve identity-based blind signature scheme', *International Journal of Network Security*, Vol. 23, No. 1, pp.9–13.

Yoon, H., Cheon, J.H. and Kim, Y. (2005) 'Batch verification with ID-based signature', in Park, C. and Chee, S. (Eds.): *Information Security and Cryptology – ICISC 2004, LNCS*, Vol. 3506, pp.233–248.

Zhang, C., Lu, R., Lin, X., Ho, P.H. and Shen, X. (2008) 'An efficient identity-based batch verification scheme for vehicular sensor networks', in *IEEE INFOCOM 2008 – The 27th Conference on Computer Communications*, Phoenix, USA, 13–18 April, pp.816–824.

Zhang, C., Ho, P-H. and Tapolcai, J. (2011) 'On batch verification with group testing for vehicular communications', *Wireless Networks*, Vol. 17, pp.1851–1865.

Zhou, Y. and Peng, D. (2018) 'A new model of vehicular ad hoc networks based on artificial immune theory', *International Journal of Computational Science and Engineering*, Vol. 16, No. 2, pp.153–161.

Zhu, X., Jiang, S., Wang, L. and Li, H. (2014) 'Efficient privacy-preserving authentication for vehicular ad hoc network', *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 2, pp.907–919.