Secure and Pairing-Free Identity-Based Batch Verification Scheme in Vehicle Ad-Hoc Networks

Xiaoming Hu[1(✉)], Jian Wang[1], Huajie Xu[2], Yan Liu[1], and Xiaojun Zhang[3]

[1] College of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai 201209, China
xmhu@sspu.edu.cn
[2] School of Computer and Electronic Information, Guangxi University, Nanning 530004, China
[3] E & A College, Hebei Normal University of Science and Technology, Hebei 066004, China

Abstract. Identity-based batch verification (IBBV) scheme is very desirable to solve efficiency, security and privacy preservation issues for vehicular ad hoc network (VANET). In 2015, Tzeng et al. proposed an IBBV scheme which was published in IEEE Transaction on Vehicular Technology. Their scheme has superior performance than other existing similar schemes in terms of security, computation cost and transmission overhead by performance evaluations. However, one time signature verification of their scheme needs two bilinear pairing operations. As it is well known, bilinear pairing is one of the most time-consuming operation in modern cryptography. Therefore, some efforts can be made to prevent the appearance of pairing and obtain better efficiency. In this paper, we propose an improved scheme of Tzeng et al.'s IBBV. Our improved IBBV scheme needs not use bilinear pairing without the lack of security and privacy-preserving. The total computation cost for signing and verifying is the constant 1.2 *ms* for single message and *n* messages respectively, which is far better performance than Tzeng et al. scheme and other similar schemes. So our improved IBBV scheme is more suitable for practical use. Finally, we apply the recovering technology of the vehicle's real identity of Tzeng et al.'s IBBV scheme to a public key authentication scheme for mobile Ad-hoc networks to address an improved pairing-free authentication scheme.

Keywords: Information security · Ad hoc network · Vehicular ad hoc network (VANET) · Identity-based batch verification · Authentication scheme · Pairing-free Diffie-Hellman

1 Introduction

Mobile ad hoc networks (MANETs) [1–4] have attracted many researchers' interests due to the nonexistence of fixed network infrastructure, but which increases the difficulty of providing security for MANETs. Vehicle ad hoc network (VANET) [5, 6] is a

D.-S. Huang et al. (Eds.): ICIC 2016, Part III, LNAI 9773, pp. 11–20, 2016.
DOI: 10.1007/978-3-319-42297-8_2

variant of MANETs which can improve the traffic safety and efficiency. In a VANET, vehicles are equipped with on-board units (OBUs) which can be used to communicate with road side units (RSU). The vehicles can also use OBUs to communicate each other. However, wireless communication mode makes the security of VANET is complex. Many attack issues need to be considered, including intercept, replay, delete and so on. A secure VANET ought to include the following properties [6]: unforgeagility, identity privacy preservation, traceability, message authentication, non-repudiation, unlinkability and replaying resistance. Recently, a lot of research [7–12] was made on security of VANET. However, most of them involved low efficiency and expensive deployment.

In 2008, an identity-based batch (IBBV) scheme was proposed by zhang et al. [13, 14]. In their scheme, a batch of messages to be signed can be verified together, which is greatly saving time. In 2013, Lee and Lai [15] pointed that there existed some drawbacks in Zhang et at.' IBBV scheme [14]. Lee and Lai also addressed an improved IBBV with high efficiency. Unfortunately, in 2015, Tzeng et al. [6] found out that Lee and Lai's IBBV scheme was vulnerable to some attacks, including forgeability and real identity extracting. As an improvement, Tzeng et al. [6] proposed a new IBBV scheme with enhancing security. They also made a concrete simulation evaluation that showed that their scheme had a superior performance in terms of computation cost and transmission overhead compared with other similar IBBV schemes. However, Tzeng et al.'s scheme [6] needed to use bilinear pairing operation which is one of the most consuming-time operations in modern cryptography. In this paper, we make a slight modification for Tzeng et al.'s scheme to propose an improved IBBV scheme. The improved scheme removes the bilinear pairing and make the computation cost be very low, i.e., constant 1.2 *ms* for any message signatures. Therefore, our scheme obtains a better performance than Tzeng et al.'s scheme and other similar schemes.

The rest of the paper is organized as follows. In second section, we give some preliminaries. In Sect. 3, we review the Tzeng et al.'s IBBV scheme. In Sect. 4, we present our improved scheme and the evaluation for security and performance of our scheme. In Sect. 5, an improved authentication scheme is presented. In Sect. 6, we conclude this paper.

2 Preliminaries

2.1 Bilinear Map

Let G1 and G2 be two groups with the same prime order q. Assume that P is a generator of G1 and e: G1 × G1 → G2 is a bilinear map if it holds the following properties:

- Bilinearity: $e(U^x, V^y) = e(U, V)^{xy}$ for all $U, V \in G_1$ and $x, y \in Z_q^*$.
- Non-degeneracy: $e(P, P) \neq 1$.
- Computability: for all $U, V \in G_1$, $e(U, V)$ can be computed efficiently.

2.2 Discrete Logarithm (DL) Problem

Given two random elements $P_1, P_2 \in G_1$, the DL problem is to find a which satisfies $P_2 = aP_1$.

3 Review of Tzeng et al.'s IBBV Scheme

In order to state conveniently and show the difference of our improved IBBV scheme and Tzeng et al.'s scheme clearly, here we briefly review Tzeng et al.'s IBBV scheme [6] for VANET.

Tzeng et al.'s IBBV scheme includes three parts: system setup (Syssetup), identity and signature generation (ID-SIGgeneration) and signature verification (SIGverification).

3.1 System Setup(Syssetup)

In this phase, a trust authority (TA) setups and publishes some system parameters as follows.

- TA selects two groups G_1 and G_2 with the same prime order q. Then choose two random generators of $G_1 : P_1$ and P_2. $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map as defined above. Define two one-way hash functions: $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : \{0,1\}^* \rightarrow Z_q^*$. Then, TA chooses a random element $s \in Z_q^*$ as the master private key and computes $P_{pk} = sP_1$ as the system public key. Next, the system public parameters are $params = \{G_1, G_2, q, e, P_1, P_2, P_{pk}, H_1, H_2\}$.
- TA generates a real identity *RID* and a secret password *PWD* for each vehicle when it makes the first registration. After that, TA preloads its identity *RID*, the password *PWD* and the master private key s into each vehicle's tamper-proof device. Then, TA publishes *params* to all RSUs and all vehicles.

3.2 Identity and Signature Generation (ID-SIGgeneration)

In this phase, the tamper-proof device of each vehicle performs the anonymous identity generation and signature generation. In order to do these works, the tamper-proof device of each vehicle consists of three modules: authentication module (AM), anonymous identity generation module (AIGM) and signature module (SM). Each module works as follows.

- Before making message signing, the vehicle C must pass the identity authentication which is performed by the authentication module of tamper-proof device. C first inputs its own *RID* and *PWD* into tamper-proof device. Then, the AM verifies the correctness of *RID* and *PWD*. If they are both not correct, the tamper-proof device ends the following operation. Otherwise, it performs the AIGM as follows.

- The AIGM picks up a random element $k \in Z_q^*$ and computes (ID_1, ID_2) where $ID_1 = kP_1$ and $ID_2 = RID \oplus H_1(kP_{pk})$. Then, (ID_1, ID_2) is an anonymous identity for vehicle C. Next, SM begins to work.
- The vehicle C constructs a message m and sends m to the SM of tamper-proof device. SM performs the following signature operations on m. First, the SM generates a current time stamp T. Then, it computes

$$V = (k + sH_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T).$$

Finally, the tamper-proof device obtains $\sigma = \{(ID_1, ID_2), m, V, T\}$ and the vehicle C sends σ to the neighbouring RSU and vehicles.

3.3 Signature Verification (SIGverification)

- Single signature verification. After RSU or a vehicle receives a message $\sigma = \{(ID_1, ID_2), m, V, T\}$, the RSU or vehicle verifies the message as follows. First, it checks if the time T is fresh. If T is fresh, it checks if

$$e(V, P_1) = e(ID_1 + H_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T)P_{pk}, P_2)$$

  If the above equation is satisfied, the RSU or vehicle accepts the message or rejects it.
- Batch signatures verification. In order to prevent a lot of messages congesting the RSU, batch verification is used as a very efficient method to improve the verification speed. Assume that the RSU receives l messages, such as $\{(ID_{1,1}, ID_{1,2}), m_1, V_1, T_1\}$, $\{(ID_{2,1}, ID_{2,2}), m_2, V_2, T_2\}, \ldots\ldots, \{(ID_{l,1}, ID_{l,2}), m_l, V_l, T_l\}$. RSU first checks if all time T_i is fresh for $1 \le i \le l$. Then, RSU uses the concept of small exponent test [6, 9] to check the following equation

$$e(\sum_{i=1}^{l} t_i V_i, P_1) = e(\sum_{i=1}^{l} t_i ID_{i,1} + \sum_{i=1}^{l} t_i H_2(ID_{i,1} \,||\, m_i \,||\, ID_{i,2} \,||\, T_i)P_{pk}, P_2)$$

  where $t_i (1 \le i \le l)$ is a random l-vector referring to [6, 9] for more information on t_i.

4 The Improved IBBV Scheme

From the above description of Tzeng et al.'s IBBV scheme, it can see that Tzeng et al.'s IBBV scheme needs two bilinear pairing operations for single signature verification. In this section, we make a slight modification for Tzeng et al.'s IBBV scheme to present an improved IBBV scheme which is pairing-free.

4.1 The Scheme

Our improved scheme consists of three phases as Tzeng et al.'s IBBV scheme: system setup (Syssetup), identity and signature generation (ID-SIGgeneration) and signature verification (SIGverification).

The Syssetup phase of our improved scheme is the same to that of Tzeng et al.'s scheme. The main difference is the ID-SIGgeneration and SIGverification phases.

ID-SIGgeneration

– After *RID* and *PWD* pass the authentication of the AM, the AIGM picks up a random element $k \in Z_q^*$ and computes (ID_1, ID_2) where

$$ID_1 = kP_1$$
$$ID_2 = RID \oplus H_1(kP_{pk}).$$

Then, (ID_1, ID_2) is an anonymous identity for vehicle C.
We can reduce the computation cost of anonymous identity by the following method. The AIGM generates a current time stamp T and computes

$$ID = RID \oplus H_1(T, s).$$

Then, *ID* is the anonymous identity which can be used to generate signature lately. It can be saw that a point multiplication operation is reduced than the previous method. When the real identity of vehicle needs to be recovered, TA computes

$$RID = ID \oplus H_1(T, s).$$

Then TA obtains the vehicle's real identity *RID*.

– After the anonymous identity generation, the vehicle C constructs a message m and sends m to the SM of tamper-proof device. The SM generates a current time stamp T. Then, it computes

$$r = k + sH_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T).$$

Finally, the tamper-proof device gets the signature $\{(ID_1, ID_2), m, r, T\}$ and the vehicle C sends $\{(ID_1, ID_2), m, r, T\}$ to the neighbouring RSU and vehicles.

Signature Verification (SIGverification)

– Single signature verification. After RSU or a vehicle receives a signature $\{(ID_1, ID_2), m, r, T\}$, the RSU or vehicle verifies the message as follows. First, it checks if the time T is fresh. If T is fresh, it checks if

$$rP_1 = ID_1 + H_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T)P_{pk}.$$

If the above equation is satisfied, the RSU or vehicle accepts the message or rejects it. The correctness of the above equation can be verified by the following method.

$$
\begin{aligned}
& rP_1 \\
&= (k + sH_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T))P_1 \\
&= kP_1 + sH_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T)P_1 \\
&= ID_1 + H_2(ID_1 \,||\, m \,||\, ID_2 \,||\, T)P_{pk}.
\end{aligned}
$$

– Batch signatures verification adopts the same technology as Tzeng et al.'s scheme. Assume that the RSU receives l messages, such as

$$
\begin{aligned}
&\{(ID_{1,1}, ID_{1,2}), m_1, r_1, T_1\}, \\
&\{(ID_{2,1}, ID_{2,2}), m_2, r_2, T_2\}, \\
&\ldots\ldots \\
&\{(ID_{l,1}, ID_{l,2}), m_l, r_l, T_l\}.
\end{aligned}
$$

RSU first checks if all time T_i is fresh for $1 \le i \le l$. Then, RSU checks the following equation

$$
\sum_{i=1}^{l} t_i r_i P_1 = \sum_{i=1}^{l} t_i ID_{i,1} + \sum_{i=1}^{l} t_i H_2(ID_{i,1} \,||\, m_i \,||\, ID_{i,2} \,||\, T_i) P_{pk}.
$$

where $t_i (1 \le i \le l$ is a random l-vector as that of Tzeng et al.'s scheme.

4.2 Performance and Security Evaluation

Performance Analysis

In order to facilitate comparison with other IBBV schemes, we adopt the same items to Tzeng et al.'s scheme and only consider the dominated operations, such as $T_{pairing}$ as the time for one bilinear pairing operation, $T_{multiple}$ as the time for one point multiplication operation on G_1. Then, from the Table 1, we can get that Tzeng et al.'s scheme needs $2T_{multiple} + 2T_{pairing}$ for single message signing and verifying, and at the same needs $(n+1)T_{multiple} + 2T_{pairing}$ for n messages signing and verifying. According to the simulation result from Tzeng et al.'s literature [6], $T_{pairing}$ is 4.5 ms and $T_{multiple}$ is 0.6 ms. So the total time for Tzeng et al.'s scheme is $4.5\,ms \times 2 + 0.6\,ms \times 2 = 10.2\,ms$ for single message and $4.5\,ms \times 2 + 0.6\,ms \times (n+1) = (9.6 + 0.6n)\,ms$ for n messages. Comparison with other schemes [14–18], Tzeng et al.'s scheme has the best efficiency.

However, from the Table 1, we can get that our improved IBBV scheme needs $2T_{multiple}$ for single message signing and verifying and $2T_{multiple}$ for n messages signing and verifying, and the total time is the constant $0.6\,ms \times 2 = 1.2\,ms$ for single message and n messages respectively. Therefore, our scheme has the constant time cost which does not increase with the number of message. So, by the above analysis, we can find that our improved scheme has better efficient than other schemes, including Tzeng et al.'s scheme [6, 14–18]. We will present the practical experiment data of our improved scheme in the further work.

Table 1. Computional comparison with scheme [6]

Scheme	Single signing + verifying	n signing + verifying
[6]	$2(T_{pairing} + T_{multiple})$	$(n+1)(T_{multiple} + 2T_{pairing})$
Our	$2T_{multiple}$	$2T_{multiple}$

Security Analysis

Our improved IBBV scheme is slight change of Tzeng et al.'s IBBV scheme. So, we can adopt the similar proof technology to prove the security of our improved scheme. Next we give a simple analysis on the unforgeability of our scheme, which is the main security property of IBBV scheme.

The unforgeability of our improved IBBV scheme can be deduced to the DL problem on G_1 in the random oracle model. The main idea on the unforgeability is as follows. Given a random instance of DL problem (P_1, Q) where $Q = aP_1$ and P_1, $Q \in G_1$, $a \in Z_q^*$. The aim of the challenger CH is to obtain a by the adversary AD by the following running.

Setup: In order to get a, CH sets

$$P_{pk} = aP_1$$

as the system public key and a as the master private key. The other system parameters are set as Tzeng et al.'s scheme.

Query: In this phase, AD can make the random oracle query and signature query. When AD submits a $U_i \in G_1$ for a H_1 random oracle query, CH chooses a random number $b_i \in G_1$ and returns b_i to AD as the value of $H_1(U_i)$. CH records the tuple (U_i, b_i). Namely,

$$b_i = H_1(U_i).$$

When AD submits a $\{(ID_{i,1}, ID_{i,2}), m_i, T_i\}$ for a H_2 query, CH selects randomly $c_i \in Z_q^*$ and returns c_i to AD as the value of $H_2(ID_{i,1} \| m_i \| ID_{i,2} \| T_i)$. Namely,

$$c_i = H_2(ID_{i,1}||m_i||ID_{i,2}||T_i).$$

When AD submits a message m_i for a signature query, CH chooses randomly k_i. $c_i \in Z_q^*, b_i \in G_1$ and sets

$$r_i = k_i,$$
$$ID_{i,2} = RID \oplus b_i.$$

Then, CH computes

$$ID_{i,1} = k_i P_1 - c_i P_{pk}.$$

$\{(ID_{i,1}, ID_{i,2}), m_i, r_i, T_i\}$ is a valid signature because

$$\begin{aligned} & r_i P_1 \\ &= ID_{i,1} + c_i P_{pk} \\ &= k_i P_1 - c_i P_{pk} + c_i P_{pk} \\ &= k_i P_1 = r_i P_1. \end{aligned}$$

Output: AD finally outputs a forged signature $\{(ID_1^*, ID_2^*), m^*, r^*, T^*\}$. Writing

$$h^* = H_2(ID_1^* \| m^* \| ID_2^* \| T^*).$$

Using the forking lemma [19], CH can obtain another signature $\{(ID_1^*, ID_2^*), m^*, r'^*, T'^*\}$. The two signatures satisfy

$$\begin{aligned} r^* &= k^* + ah^* \\ r'^* &= k^* + ah'^* \end{aligned}$$

Thus, CH can solve the given DL problem and obtain

$$a = (r^* - r'^*) \cdot (h^* - h'^*)^{-1}.$$

The other security properties (i.e., message authentication, identity privacy preservation, traceability and so on) for our IBBV scheme can be proved using the same analysis to Tzeng et al.'s scheme [6]. So we omit these descriptions. Therefore, our improvement scheme does not change the security properties of the original scheme, namely, the improved scheme still keeps the original security properties.

5 A Pairing-Free Authentication Scheme

In 2012, Tameem Eissa et al. [2] proposed an identity-based RSA authentication scheme for mobile ad hoc network (MANET). In their authentication scheme, the messages transmitted between mobile nodes were encrypted by RSA. In order to avoid RSA attacks, the public keys of RSA are secured and only the trust nodes can access. Due to the use of RSA, the efficiency of their authentication scheme is high. However, their scheme used bilinear pairing operation, so the computation cost still is high. Here, we use the recovering technology of the real identity of Tzeng et al.'s IBBV scheme (i.e., $RID = ID_2 \oplus H_1(kP_{pk})$ present an improved authentication scheme which is a very slight change of Tameem Eissa et al.' scheme. Due to the space, we only provide the main idea.

Assume that d_i and (e_i, N_i) is the private key and public keys on RSA for node $i \in \{A, B, CRSA\}$. When a node A submits (ID_B, P_A) to a coalition $CRSA$ for the public keys of B node where ID_B is the identity of B and

$$P_A = d_A P,$$

CRSA does as follows. *CRSA* computes

$$\begin{aligned} C &= e_B \oplus H_2(d_{CRSA} P_A \,||\, ID_A \,||\, ID_B), \\ U &= P_{CRSA} = d_{CRSA} P, \\ W &= e_B P, \\ Y &= N_B \oplus H_3(e_B). \end{aligned}$$

After A gets (U, C, W, Y), it can obtain the public key (e_B, N_B) by the following computing

$$\begin{aligned} e_B &= C \oplus H_d(d_A P_{CRSA} \,||\, ID_A \,||\, ID_B), \\ N_B &= Y \oplus H_3(e_B). \end{aligned}$$

6 Conclusion

In this study, we review Tzeng et al.'s identity-based batch scheme for VANET which has better efficiency than other similar schemes. As an improvement of Tzeng et al.'s scheme, we present a new IBBV scheme with pairing-free. We also make a performance evaluation between our scheme with other IBBV schemes. The comparison shows that our scheme is not only secure in the random oracle but also has constant computation cost which is independent of the number of messages. Therefore, our scheme has better performance and more practical than others.

Acknowledgements. This work was supported by the Innovation Program of Shanghai Municipal Education Commission (No.14ZZ167), the National Natural Science Foundation of China (No.61103213), the Guangxi Natural Science Foundation (No.2014GXNSFAA11838-2) and the Key Disciplines of Computer Science and Technology of Shanghai Polytechnic University under Grant No. XXKZD1604.

References

1. Ying, L., Yang, S., Srikant, R.: Optimal delay-throughput tradeoffs in mobile ad hoc networks. IEEE Trans. Inf. Theor. **54**(9), 4119–4143 (2008)
2. Eissa, T., Razak, S., Ngadi, M.: A novel lightweight authentication scheme for mobile ad hoc networks. Arab. J. Sci. Eng. **37**(8), 2179–2192 (2012)
3. Zhang, Y., Liu, W., Wei, W., et al.: Location-based compromise-tolerant security mechanisms for wireless sensor networks. IEEE J. Sel. Areas Commun. **24**(2), 247–260 (2013)

4. Shabnam, K., Mazleena, S.: A novel authentication scheme for mobile environments in the context of elliptic curve cryptography. In: Proceeding I4CT 2015, pp. 506–510. IEEE press, New York (2015)
5. Lin, X., Lu, R., Zhang, C., et al.: Security in vehicular ad hoc networks. IEEE Commun. Mag. **46**(4), 88–95 (2008)
6. Tzeng, S., Horng, S., Li, T., et al.: Enhancing security and privacy for identity-based batch verification scheme in VANET. IEEE Trans. Veh. Technol. **99**, 1–12 (2015)
7. Papadimitratos, P., Hubaux, J.: Report on the secure vehicular communications: results and challenges ahead workshop. ACM SIGMOBILE Mobile Comput. Commun. Rev. **12**(2), 53–64 (2008)
8. Chim, T., Yiu, S., Hui, C., et al.: SPECS: secure and privacy enhancing communications schemes for VANETs. Ad Hoc Netw. **9**(2), 189–203 (2011)
9. Horng, S., Tzeng, S., Pan, Y., et al.: b-SPECS+: batch verification for secure pseudonymous authentication in VANET. IEEE Trans. Inf. Forensics Secur. **8**(11), 1860–1875 (2013)
10. Nithya, D., Kumari, N.: A survey of routing protocols for VANET in Urban scenarios. In: Proceeding Pattern Recognition, Informatics and Mobile Engineering PRIME 2013, pp. 464–467. IEEE Press, New York (2013)
11. Mokhtar, B., Azab, M.: Survey on security issues in vehicular ad hoc networks. Alexandria Eng. J. **54**, 1115–1126 (2015)
12. Thenmozhi, T., Somasundaram, R.: Towards modelling a trusted and secured centralised reputation system for VANET's. Wireless Pers. Commun. **88**(2), 357–370 (2016)
13. Zhang, C., Lu, R., Lin, X., et al.: An efficient identity-based batch verification scheme for vehicular sensor networks. In: Proceeding INFOCOM 2008, pp. 816–824. IEEE Press, New York (2008)
14. Zhang, C., Ho, P., Tapolcai, J.: On batch verification with group testing for vehicular communications. Wireless Netw. **17**(8), 1851–1865 (2011)
15. Lee, C., Lai, Y.: Toward a secure batch verification with group testing for VANET. Wireless Netw. **19**(6), 1441–1449 (2013)
16. IEEE Trial-Use Standard for Wireless Access in Vehicular Environment-Security Services for Applications and Management Messages. In: IEEE standard 1609, 2 July 2006
17. Huang, J., Yeh, L., Chien, H.: ABAKA: an anonymous batch authenticated and key agreement scheme for value-add services in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **60**(1), 248–262 (2011)
18. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. J. Cryptology **17**(4), 297–319 (2004)
19. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptology. **13**(3), 361–396 (2000)