Security Analysis of Efficient Anonymous Authentication With Conditional Privacy Preserving Scheme for Vehicular Ad Hoc Networks

Rui Qiao
Shaanxi International Business College
18220857680@163.com

Qinglong Wang*
Chang’an University
*qlwang@chd.edu.cn

Zongtao Duan
Chang’an University
ztduan@chd.edu.cn

Na Fan
Chang’an University
fnsea@chd.edu.cn

ABSTRACT

Protecting a driver’s privacy is one of the major concerns in vehicular ad hoc networks (VANETs). Currently, Azees et al. has proposed an efficient anonymous authentication protocol (EAAP) for VANETs. The authors claim that their scheme can implement conditional privacy, and that it can provide resistance against impersonation attack and bogus message attack from an external attacker. In this paper, we show that their scheme fails to resist these two types of attack as well as forgery attack. By these attacks, an attacker can broadcast any messages successfully. Further, the attacker cannot be traced by a trusted authority, which means their scheme does not satisfy the requirement of conditional privacy. The results of this article clearly show that the scheme of Azees et al. is insecure.

KEYWORDS

Vehicular ad hoc networks (VANETs), Impersonation attack， Bogus message attack, Forgery attack, Conditional privacy.

1 INTRODUCTION

As a special case of mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs) have become a key part of intelligent transportation system (ITS) frameworks [1]. VANETs can improve driving experience, reduce traffic accidents, and provide rich infotainment services for drivers and passengers, making driving more comfortable and safe [2]. Generally, there are three kinds of entities involved in a typical VANET system: a trusted agency (TA), which is the builder and manager of the VANET system; the on board unit (OBU) with which each vehicle is equipped; and the road side unit (RSU), assumed to be a fixed device located on the road side. Both OBUs and RSUs are dedicated short-range communication (DSRC) devices that are used to provide vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communication [3]. The communication between an RSU and the TA is assumed to occur through wired channels.

According to the IEEE802.11P standard, vehicles are required to periodically broadcast messages every 300 ms. The message includes not only general traffic conditions such as weather conditions and emergent events but also data about the vehicle’s condition, such as its identity, location, and speed. In order to guarantee the authenticity and reliability of these messages, the receivers have to authenticate the sender’s identity to ensure that the messages are from a legal vehicle. Moreover, there are many VANET applications that also need to send the vehicle’s identity to an RSU or other vehicles. However, a vehicle’s identity has much to do with the driver’s privacy, which is sensitive information [4]. For example, an adversary is able to reconstruct a vehicle’s trajectory if they can distinguish messages broadcasted by the vehicle from those broadcasted by other vehicles, which is called privacy-related attack. From the vehicle’s trajectory, an adversary can acquire a lot of privacy information about the driver (or user) of the vehicle, such as the driver’s home address, workplace, and living habits. Furthermore, the adversary can potentially derive the driver’s real identity from this privacy information, which is truly a threat to the driver. It is well known that VANETs could not have been deployed at large scales unless driver privacy is protected. In practice, anonymous identity is widely used to protect the vehicle driver’s real identity. However, some malicious vehicle operators may broadcast fraudulent messages for their own benefit. In this case, a VANET system must have the ability to trace the real identity of these malicious vehicle operators, which means that the anonymity is conditional. The challenge is how to efficiently make a trade-off between anonymity and traceability.

2 RELATED WORKS

In recent years, many conditional privacy-preserving authentication (CPPA) schemes have been advanced for protecting driver privacy in VANETs. Usually, various methods are used to design CPPA schemes, such as the following.

The first method is use of a group signature mechanism[5-8], which achieves conditional privacy based on the anonymity and traceability of the group signature itself. However, the size of a group signature is several times larger than traditional signatures, making them more expensive in terms of transmission and verification cost. In addition, efficiently overcoming the dynamic changes associated with a group member requires significant effort.

The second method is based on the ring signature mechanism[9-10]. The main difference between a ring signature and group signature is that a group creator is not required in a ring signature. The critical problem inherent in this method is that it is difficult to achieve traceability effectively. In both Refs. [9] and [10], the TA cannot trace the malicious member without the collaboration of all ring members, which is an unrealistic expectation.

The third method is based on the public key infrastructure (PKI)[11–13], in which a TA needs to issue many anonymous certificates for each vehicle. Although the anonymous certificates have nothing to do with the real identity of a vehicle, each certificate can only be used a limited number of times in order to avoid privacy-related attacks. Therefore, vehicles must update their certificates before current certificates expire, and the TA has to store all issued certificates in order to implement traceability. Moreover, a vehicle needs to check the certificate revocation list (CRL) before verifying the integrity of received messages in cases of communicate with vehicles with revoked certificates. This places a heavy certificate management burden on the TA, and the efficiency of this methods decreases with the growing size of the CRL.

The fourth method is based on the ID-based public key cryptosystem[14]. For some schemes in this method[15-16], the TA stores the master key of the VANET system in a tamper-proof device (TPD), with which each vehicle is equipped. By using the master key, each vehicle is able to generate valid anonymous certificates itself. Thus, no complex certificate management problem exists, as with the third method. However, the assumption of total security of TPDs in these schemes is too high to be practical. Actually, the adversary can acquire substantial information from a TPD by using various side attacks[18]. In 2017, Zhang et al.[17] presented an improved CPPA scheme based on the scheme presented in [16]. In the scheme presented in [17], there is no need to store the master key for a TPD. However, the main problem of [17] is that the RSU requires the assistance of the TA when a RSU authenticates a vehicle at the first time. Considering the number of vehicles in a VANET, the TA might become an authentication bottleneck. In 2016, based on their ID-based signature, Lo et al.[19] presented a CPPA scheme without time-consuming pairings. However, in order to provide privacy, they assumed that each vehicle already had sufficient anonymous certificates from the TA. This means that the same problems of the third method must be overcome [19].

In 2014, Zhu et al.[20] proposed an efficient CPPA scheme. The notable property of the scheme presented in [20] is that it does not apply an anonymous certificate, but instead employs the hash message authentication code(HMAC) technique to verify both authenticity and integrity. In this scenario, TA publishes a group public key for each domain. Each vehicle in a RSU's area will get its own group secret key after it is authenticated by this RSU. The drawback of the scheme presented in [20] is that a vehicle must send its unique identity to RSU during the authentication process. This constitutes a leak of vehicle privacy since the RSU is not a trusted party. In 2016, a CPPA scheme[21] based on HMAC was presented by Jiang et al., but this scheme also implied use of anonymous certificates issued by a TA. Hence, the scheme presented in [21] suffers from the similar certificate management burden discussed above Azees et al. published a new CPPA scheme [22]. In their scheme, in order to prevent an external vehicle from entering the VANET system, each vehicle must register required information with the local TA. In [22], when a vehicle wants to broadcast a message, it generates an anonymous certificate by itself and signs the message with this certificate. Differing from the schemes discussed in context of the fourth method above, the advantages of [22] are that it neither stores the master key in a TPD nor does the local TA takes part in the vehicle's authentication directly. In addition, the scheme presented in [22] purports to protect a RSU's privacy, which is rarely considered in many existing CPPA schemes. This means that a RSU also uses anonymous certificates to authenticate itself to vehicles. Five theorems were provided in [22]: Theorem 1 shows that their scheme is semantically secure against impersonation attack, theorem 2 claims that the scheme can withstand bogus message attack, and theorem 4 proves that the privacy of the scheme is conditional. However, we have found that these three theorems are incorrect.

2.1 Our Contribution

We executed some concrete attacks on the scheme presented in [22] that revealed serious security problems. In the proof of theorem 1, the authors of [22] assumed that an adversary has no way of mounting an impersonation attack because the adversary cannot obtain any one of the secret values embedded in messages broadcasted by registered vehicles. Again, we prove that their assumption is incorrect, since an adversary is able to impersonate a vehicle successfully even without the corresponding secret key. In the proof of theorem 2, the authors assumed that a vehicle cannot obtain a valid dummy identity unless it completed the registration. However, we show that an unregistered malicious vehicle is able to generate many dummy identities and can produce valid signatures for any messages. Furthermore, a TA cannot trace the real identity of the malicious vehicle because the TA does not store any information about the unregistered vehicle, which shows that theorem 4 of [22] is also incorrect.

2.2 Organization of this paper

The rest of this article is organized as follows. In Section 3, we briefly introduce the CPPA scheme of Azees et al., and in Section 4 we provide the results of different attacks executed against it. Section 5 concludes the article.

3 INTRODUCTION OF CPPA SCHEME OF AZEES *et al.*

Owing to length considerations, we omit descriptions of the system model, attack model, and security analysis of their scheme; for details, refer to [22] directly.

3.1 System Initialization

A TA generates and publishes the system parameters as $param = (q, e, g_1, g_2, G_1, G_2, G_T, A_1, B_1, H)$, where q is a large prime; G_1, G_2, G_T are three groups that have the same order q ; g_1, g_2 are generators, respectively, for G_1 and G_2 ; $H: \{0,1\}^* \to Z_q^*$ is a secure cryptographic hash function; $e: G_1 \times G_2 = G_T$ is a bilinear map (the definition of which is also omitted here); and $A_1 = g_1^a$, $B_1 = g_1^b$, where $a, b \in Z_q^*$. Unless otherwise specified, all of the arithmetic are modulo q operations.

3.2 Anonymous Authentication of Vehicles

3.2.1 Registration and Key Generation. The vehicle users first need to register their real information to the TA. The TA then generates the original identity (OID_{u_i}) and computes the dummy identity $DID_{u_i} = g_1^{n_i + a}$ and $T_i = g_1^{\frac{1}{v_i + a + b}}$, as well as $E_i = g_1^{-n_i}$ for each ser u_i , where $n_i, v_i \in Z_q^*$. Finally, the TA stores $(OID_{u_i,} DID_{u_i}, T_i^b)$ in its tracking list and sends an authorization key $AK = (DID_{u_i}, T_i, E_i)$ to u_i .

3.2.2 Anonymous Certificate Generation. u_i randomly selects $r_k, \mu, k_1, k_2 \in Z_q^*$ and computes $Y_k = g_2^{r_k}$, $\gamma_U = B_1^{\mu}$, $\gamma_V = T_i \cdot A_1^{\mu}$, $\lambda_1 = \gamma_U^{\mu + k_1}$, $\lambda_2 = \frac{\gamma_U^{\mu + k_1}}{\gamma_V^{\mu + k_2}}$, $\lambda = (\mu + r_k) \bmod q\text{-}1$, $\delta_1 = (r_k - k_1) \bmod q\text{-}1$, and $\delta_2 = (r_k - k_2) \bmod q\text{-}1$ [in [22], the authors incorrectly describe these as $\lambda = (\mu + r_k) \bmod q$, $\delta_1 = (r_k - k_1) \bmod q$, and $\delta_2 = (r_k - k_2) \bmod q$]. u_i further computes the challenger $c = H\left(DID_{u_i} \| A_1 \| B_1 \| E_i \| \gamma_u \| \gamma_v \| Y_k \| \lambda_1 \| \lambda_2\right)$ and generates the anonymous certificate $Cert_k = \left\{Y_k \| E_i \| DID_{u_i} \| \gamma_U \| \gamma_V \| c \| \lambda \| \delta_1 \| \delta_2\right\}$.

3.2.3 Signature Generation. For message M , u_i produces the signature as $sig = g_1^{\frac{1}{r_k + H(M)}}$, and broadcasts the anonymous message $msg = \left(M \| sig \| Y_k \| Cert_k\right)$.

3.2.4 Verification. After receiving the message $msg = \left(M \| sig \| Y_k \| Cert_k\right)$, the receiver first computes $N_i = E_i \times DID_{ui}$, $\lambda_1^{'} = \frac{\gamma_U^{\lambda}}{\gamma_U^{\delta_1}}$, $\lambda_2^{'} = \frac{\gamma_U^{\lambda} \cdot \gamma_V^{\sigma_2}}{\gamma_U^{\delta_1} \cdot \gamma_y^{\lambda}}$ and $c^{'} = H\left(DID_{u_i} \| A_1 \| B_1 \| E_I \| \gamma_U \| \gamma_V \| Y_k \| \lambda_1^{'} \| \lambda_2^{'}\right)$, and then the receiver verifies whether the following three equations hold:

$$N_i = A_1 \tag{1}$$

$$c^{'} = c \tag{2}$$

$$e\left(sig, Y_k \cdot g_2^{H(M)}\right) = e\left(g_1, g_2\right) \tag{3}$$

If(1)-(3)hold, the legitimacy of the message sender and the integrity of message M will pass verification. Otherwise, the receiver drops the message msg .

3.2.5 Conditional Tracking. Given a particular anonymous certificate $Cert_k = \{Y_k \| E_i \| DID_{u_i} \| \gamma_U \| \gamma_V \| c \| \lambda \| \delta_1 \| \delta_2\}$, the TA computes

$$\frac{\gamma_V^b}{\gamma_U^a} = \frac{(T_i \cdot A_1^{\mu})^b}{(B_1^{\mu})^a} = \frac{T_i^b \cdot A_1^{\mu b}}{g_1^{\mu ab}} = T_i^b \tag{4}$$

From this, the TA can reveal the real identity of the producer of the $Cert_k$ by looking up the value T_i^b in its tracking list.

4 ATTACK ON THE CPPA SCHEME OF AZEES *et al.*

4.1 Bogus Message Attack

The authors of [22] claim that their scheme can resist bogus message attacks because the attacker cannot generate two parameters E and DID such that $E \times DID = A_1$. Here, we prove that an attacker (an external adversary who is an unregistered vehicle user) can produce these two parameters efficiently in two different methods.

4.1.1 First Method. From the public system parameters, an attacker can obtain parameter A_1 . Then, the attacker randomly selects $x \in Z_q^{*}$, and computes $DID = g_1^x \cdot A_1$ and $E = g_1^{-x}$. It is obvious that $E \times DID = g_1^{-x} \cdot g_1^x \cdot A_1 = A_1$.

4.1.2 Second Method. Suppose the attacker received a valid message $msg = (M \| sig \| Y_k \| Cert_k)$ broadcasted by a legal user u_i . The attacker can extract $E_i \| DID_{u_i}$ from $Cert_k$, and then select $x \in Z_q^{*}$ randomly and compute $E = g_1^{-x} \cdot E_i$ and $DID = g_1^x \cdot DID_{u_i}$. Thus, the attacker obtains a new valid E and DID because of $E \times DID = g_1^{-x} \cdot E_i \cdot g_1^x \cdot DID_{u_i} = E_i \cdot DID_{u_i} = A_1$.

The above two methods clearly show that theorem 2 of [22] is completely incorrect, which means that their scheme cannot resist bogus message attacks.

4.2 Impersonation Attack

The authors of [22] claim their scheme can resist impersonation attack because it is infeasible for an attacker to obtain the secret values of μ and T_i from a given anonymous certificate. Here, we prove that the attacker can successfully execute an impersonation attack even he cannot reveal these two values.

Anonymous certificate and signature generation: Given a valid message $msg = (M \| sig \| Y_k \| Cert_k)$, the attacker prepares an anonymous certificate using the following steps.

Step 1: Extract $E_i \| DID_{u_i} \| \gamma_U \| \gamma_V$ from $Cert_k = \{Y_k \| E_i \| DID_{u_i} \| \gamma_U \| \gamma_V \| c \| \lambda \| \delta_1 \| \delta_2\}$.

Step 2: Randomly select $r^{'},\lambda^{'},\delta_1^{'},\delta_2^{'} \in Z_q^{*}$, and compute $\lambda_1 = \frac{\gamma_U^{\lambda^{'}}}{\gamma_U^{\delta_1^{'}}}$, $\lambda_2 = \frac{\gamma_U^{\lambda^{'}} \cdot \gamma_V^{\delta_2^{'}}}{\gamma_U^{\delta_1^{'}} \cdot \gamma_V^{\lambda^{'}}}$, and $Y = g_2^{r^{'}}$.

Step 3: Compute challenger $c^{'} = H(DID_{u_i} \| A_1 \| B_1 \| |E_i \| \gamma_U \| \gamma_V \| Y \| \lambda_1 \| \lambda_2)$.

Step 4: Generate anonymous certificate $Cert = \{Y \| E_i \| DID_{u_i} \| \gamma_U \| \gamma_V \| c^{'} \| \lambda^{'} \| \delta_1^{'} \| \delta_2^{'}\}$.

Step 5: Compute signature $sig = g_1^{\frac{1}{r^{'}+H(M)}}$ for arbitrary message M and broadcast $msg^{'} = (M \| sig \| Y \| Cert)$.

Verification process: Given the $msg^{'}$, the receiver will verify its validity as follows.

Step 1: Compute $N_i = E_i \times DID_{u_i}$, $\lambda_1^{'} = \frac{\gamma_U^{\lambda^{'}}}{\gamma_U^{\delta_1^{'}}}$, and $\lambda_2^{'} = \frac{\gamma_U^{\lambda^{'}} \cdot \gamma_V^{\delta_2^{'}}}{\gamma_U^{\delta_1^{'}} \cdot \gamma_V^{\lambda^{'}}}$.

Obviously, the values of $\lambda_1^{'},\lambda_2^{'}$ are equal to λ_1,λ_2 respectively.

Step 2: Compute $c^{''} = H(DID_{u_i} \| N_i \| B_1 \| |E_i \| \gamma_U \| \gamma_V \| Y \| \lambda_1^{'} \| \lambda_2^{'})$.

It is clear that

$$c^{'} = c^{''} \tag{5}$$

Because

$$N_i = E_i \times DID_{u_i} = g_1^{-n_i} \times g_1^{n_i+a} = g_1^a = A_1 \tag{6}$$

Step 3: Compute and check whether $e(sig, Y \cdot g_2^{H(M)}) = e(g_1,g_2)$. This equation must hold because

$$e\left(sig, Y \cdot g_2^{H(M)}\right) = e\left(g_1^{\frac{1}{r^{'}+H(M)}}, g_2^{r^{'}} \cdot g_2^{H(M)}\right) = e(g_1,g_2) \tag{7}$$

From (6)–(7), the receiver authenticates the sender and verifies the integrity of message M . This means that the attacker can generate a valid anonymous certificate and sign arbitrary messages successfully. Furthermore, the attacker can generate many valid certificates by choosing different parameters $r^{'},\lambda^{'},\delta_1^{'},\delta_2^{'}$.

When the TA needs to reveal the real identity from the certificate $Cert$, the TA computes $\frac{\gamma_V^b}{\gamma_U^a} = \frac{\left(T_i \cdot A_1^{\mu}\right)^B}{\left(B_1^{\mu}\right)^a} = \frac{T_i^b \cdot A_1^{\mu b}}{B_1^{\mu a}} = \frac{T_i^b \cdot g_1^{a\mu b}}{g_1^{b\mu a}} = T_i^b$. Then, the TA will accept that u_i is the real sender of the message $msg^{'}$.

This shows that the attacker has successfully impersonated u_i .

4.3 Forgery Attack

In this type of attack, the attacker can forge a valid certificate and successfully sign a message. This differs from an impersonation attack because in a forgery attack there is no need to know an anonymous certificate generated by a legal user. In order to execute this attack, the attacker generates two parameters E and DID by using the first method described above in an impersonation attack. The attacker then randomly selects $\gamma_U,\gamma_V,r,\lambda,\delta_1,\delta_2 \in Z_q^{*}$ and generates $c = H(DID \| A_1 \| B_1 \| |E \| \gamma_U \| \gamma_V \| Y \| \lambda_1 \| \lambda_2)$ and $Cert = \{Y \| E \| DID \| \gamma_U \| \gamma_V \| c \| \lambda \| \delta_1 \| \delta_2\}$, where $Y = g_2^r$, $\lambda_1 = \frac{\gamma_U^{\lambda}}{\gamma_U^{\delta_1}}$, and $\lambda_2 = \frac{\gamma_U^{\lambda} \cdot \gamma_V^{\delta_2}}{\gamma_U^{\delta_1} \cdot \gamma_V^{\lambda}}$. The attacker also computes the signature $sig = g_1^{\frac{1}{r+H(M)}}$ for any message M and broadcasts message $msg = (M \| sig \| Y \| Cert)$. The validity of message msg can be verified in the same way as Steps 1–3 described in verification process.

This shows that the CPPA scheme presented in [22] cannot resist forgery attacks.

Since the attacker is an unregistered user, the TA stores nothing about the attacker in its tracking list. Therefore, it is clear that the TA cannot trace the real identity of this *Cert* by computing (4). This means that theorem 4 of [22] is also incorrect.

5 CONCLUSION

We have executed several methods of attacking the CPPA scheme presented in [22] and have shown that it is vulnerable to impersonation attack, bogus message attack, forgery attack. Through these attacks, an attacker can not only generate valid anonymous messages but also cannot be traced by a TA. More importantly and problematic, an attacker can broadcast harmful messages by impersonating a legal vehicle user and frame this innocent user as the malicious user revealed by the TA. Similarly, the attacker can enter the VANET as a forged RSU or an impersonated RSU. These conclusions collectively demonstrate that the CPPA scheme presented in [22] is insecure. Therefore, further research is still required to implement a secure and efficient CPPA scheme .

6 ACKNOWLEDGEMENTS

This work was supported by the Funds for Key Research and Development Plan Project of Shaanxi Province, China (Grant No. 2018GY-022, 2018GY-032, 2018GY-136).

References

[1] Azimi, R., Bhatia, G., Rajkumar, R. *et al*.: 'Vehicular networks for collision avoidance at intersections',. Proc. SAE World Congr.., Detroit, USA, Apr. 2011, pp. 406–416

[2] Tangade, S.S, Manvi, S.S.: 'A survey on attacks, security and trust management solutions in VANETs' , Proc. ICCCNT13, Tiruchengode, July India, 2013, pp. 1-6

[3] AI-Sultan, S., AI-Doori, M.M., AI-Bayatti, A.H., *et al*.: 'A comprehensive survey on vehicular ad hoc network', Journal of Network and Computer Applications, 2014, 37, (2014), pp. 380-392

[4] Fengzhong, Q., Zhihui, W., Fei-Yue, W., *et al*.: 'A security and privacy review of VANETs', IEEE Trans. Intell. Transp. Syst., 2015, 16, (6), pp. 2958–2996

[5] Xiaodong, L., Xiaoting, S., Ping-Han, H., *et al*.: 'GSIS: A secure and privacy preserving protocol for vehicular communications'. IEEE Trans. Veh. Technol., 2007, 56, (6), pp. 3442–3456

[6] Chenxi, Z., Xiaodong, L., Rongxing, L., *et al*.: 'An efficient message authentication scheme for vehicular communications', IEEE Trans. Veh. Technol., 2008, 57, (6), pp. 3357–3368

[7] Lei, Z., Qianhong ,W., Agusti, S., *et al*.: 'A scalable robust authentication protocol for secure vehicular communications'. IEEE Trans. Veh. Technol., 2010, 59, (4), pp. 1606–1617

[8] Wasef, A., Shen, X.: 'Efficient group signature scheme supporting batch verification for securing vehicular networks'. Proc. IEEE ICC, Cape Town, South Africa, May 2010, pp. 1–5

[9] Yuan, H., Shengke, Z., Xingwei, L.: 'Privacy-preserving Communication for VANETs with Conditionally Anonymous Ring Signature'. International Journal of Network Security, 2015, 17, (2), pp.135-141

[10] 'An Anonymous Communication Scheme based on Ring Signature in VANETs', article available on website. Available at https://arxiv.org/pdf/1410.1639.pdf, accessed 10 December 2017

[11] Rongxing, L., Xiaodong, L., Haojin, Z., *et al*.: 'ECPP: Efficient conditional privacy-preservation protocol for secure vehicular communications'. Proc. IEEE Conf. Comput. Commun., Phoenix, USA, Apr. 2008, pp. 1229-1237

[12] Maxim, R., Jean-Pierre, H.: 'Securing vehicular ad hoc networks', J. Comput. Security-Special Issue Security Ad Hoc Sensor Netw., 2007, 15, (1), pp. 39–68

[13] Ahren, S., Elaine, S., Fan, B.: 'Tacking together Efficient Authentication, Revocation, and Privacy in VANET'. Proc SECON , Rome, Italy, Jun 2009, pp. 1-9

[14] Dan, B., Matthew, F. :'Identity-Based Encryption from the Weil Pairing'. Proc. CRYPTO 2001, California, USA, August 2001, pp. 213-229

[15] Debiao, He., Sherali, Z., Baowen, X., *et al*.: 'An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks'. IEEE Trans. Inform. Forensics Secure, 2015, 10, (12), pp. 2681-2691

[16] Lei, Z., . Wu, B. Qin.: 'APPA: Aggregate privacy-preserving authentication in vehicular ad hoc networks'. Proc. ISC, 2011, Xi'an, China, October 2011, pp. 293-308

[17] Lei, Z., Qianhong, W., Domingo-Ferrer, J., *et al*.: 'Distributed Aggregate Privacy-Preserving Authentication in VANETs', IEEE Trans. Intell. Transp. Syst., 2017, 18, (3), pp. 516-526

[18] Kiltz, E. Pietrzak, K.: 'Leakage resilient ElGamal encryption'. Proc. Advances in Cryptology - ASIACRYPT 2010, Singapore, Dec 2010, pp. 595-612

[19] Nai-Wei, L., Jia-Lun T.:' An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings', IEEE Trans. Intell. Tansp. Syst., 2016, 17, (5), pp. 1319-1328

[20] Xiaoyan, Z., Shunrong, J., Liangmin, W., *et al*.: 'Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks', IEEE Trans. Veh. Technol., 2014, 63, (2), pp. 907-918

[21] Shunrong, J., Xiaoyan, Z., Liangmin W.: 'An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs', IEEE Trans. Intell. Transp. Syst., 2016, 17, (8), pp. 2193-2204

[22] Azees, M., Vijayakumar, P., Jegatha Deboarh, L.: 'EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks', IEEE Trans. Intell. Transp. Syst., 2017, 18, (9), pp. 2467-2476