A Group Signature-Based Anonymous Authentication Scheme with Controllable Linkability for VANTEs

Yousheng Zhou[1,2(✉)] and Xiaofeng Zhao[2]

[1] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
zhouys@cqupt.edu.cn

[2] School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract. Vehicle sensor networks (VSN) play an increasingly important part in smart city, due to the interconnectivity of the infrastructure. However similar to other wireless communications, vehicle sensor networks are susceptible to a broad range of attacks. In addition to ensuring security for both data-at-rest and data-in-transit, it is essential to preserve the privacy of data and users in vehicle sensor networks. Many existing authentication schemes for vehicle sensor networks are generally not designed to also preserve the privacy between the user and service provider (e.g., mining user data to provide personalized services without infringing on user privacy). Controllable linkability can be used to facilitate an involved entity with the right linking key to determine whether two messages were generated by the same sender, while preserving the anonymity of the signer. Such a functionality is very useful to provide personalized services. Thus, in this paper, a threshold authentication scheme with anonymity and controllable linkability for vehicle sensor networks is constructed, and its security is analyzed under the random oracle model.

Keywords: Threshold authentication · Controllable linkabilty · Group signature · Vehicle sensor networks

1 Introduction

While vehicle sensor networks research is fairly mature [1], there is plenty of research opportunities in this space due to continuing and rapid advances in

Our work was jointly supported by the National Natural Science Foundation of China (No. 61872051, No. 61702067), the Chongqing Natural Science Foundation of China (No. cstc2020jcyj-msxmX0343) and the Venture & Innovation Support Program for Chongqing Overseas Returnees (No. CX2018122).

W. Li and D. Tang (Eds.): MOBILWARE 2020, LNICST 331, pp. 211–221, 2020.
https://doi.org/10.1007/978-3-030-62205-3_21

vehicular communication technology and other underpinning technologies (e.g., smart/driverless vehicles and other Internet-connected technologies in a smart city). In vehicle sensor networks, there are two key types of entities – see Fig. 1, namely: wireless on-board units (OBUs) on vehicles to supply wireless communication ability, and roadside unit (RSU) located on the road or buildings within a certain coverage. Normally, a remote central authority (CA) is also deployed to assist OBUs or RSU to perform a given task, such as authentication. These parties can support two types of communications, namely: vehicle-to-infrastructure (V2I) communication and vehicle-to-vehicle (V2V) communication [2]. Such communications can be used to support activities such as reporting of traffic congestion and accidents/incidents. However, due to characteristics such as self-organizing, rapid-changing and open channel, vehicle sensor networks are susceptible to a broad range of attacks. Achieving secure and efficient authentication services is a basic and critical component [3,4], but increasingly there are other properties/features that should be considered. Examples include privacy preservation [6,7,9], and the related notions such as anonymity and unlinkability [5,10].

In general, striking a balance between preserving user privacy and maximizing the utility of user data (e.g., to offer better and customized services, based on mining and analysis of user data) is tricky [8]. For example, a key characteristic required to provide personalized services is linkability, which contradicts the privacy requirement. Controllable linkability, first proposed by Hwang et al. [18], is one potential solution. In such a concept, an entity who owns a linking key can dervie whether two authentication messages were generated by the same user (or not). Doing so does not infringe the user's anonymity since the identity of the message signer cannot be obtained. Since the seminal work of Hwang et al. [18], a great many group signature schemes with controllable linkability have been investigated in the literature [18–20]. However, the verifier can only check the valid signature message generated by a group member but cannot decide whether the message has been fabricated. Threshold authentication can, however, mitigate such a limitation. Specifically, the receiver accepts a message only after it has been confirmed by the specified threshold number of user.

In this work, we present a group signature-based anonymous authentication scheme for vehicle sensor networks, which is designed to achieve threshold authentication, anonymity, non-repudiation, and controllable linkability. In addition, we will demonstrate that it is more efficient than similar existing schemes in regard to both communicational and computational costs, based on the findings from our evaluations using the widely accepted OpenSSL library. We also demonstrate the security of the scheme under the random oracle model, as well as explaining how it achieves the other desirable security properties.

2 Related Work

In recent years, authentication schemes with different properties have been investigated in the literature. For instance, Raya and Hubaux [14] introduced an anonymous authentication scheme for vehicle sensor networks by employing anonymous certificates. In such a scheme, a vehicle is preloaded with large anonymous certificates such that the vehicle can employ different public/private key pairs during each authentication process to avoid being traced. However, the public/private key pairs must have a short lifetime so as to achieve privacy preservation; otherwise, there will be significant storage and management costs. Lu et al. [15] presented a new method to deal with the challenge of preloading a mass of anonymous certificates, by leveraging RSUs. To update the anonymous certificate in order to keep linkability of the message, each vehicle would request the RSU to issue a short-time anonymous certificate when the vehicle passes by the RSU. Consequently, frequent interaction between vehicle and RSU may influence the performance of the entire vehicle sensor networks. Huang et al. [16] proposed two certificateless signatures scheme; however, anonymity is not achieved because the public key of the user is needed during verification.

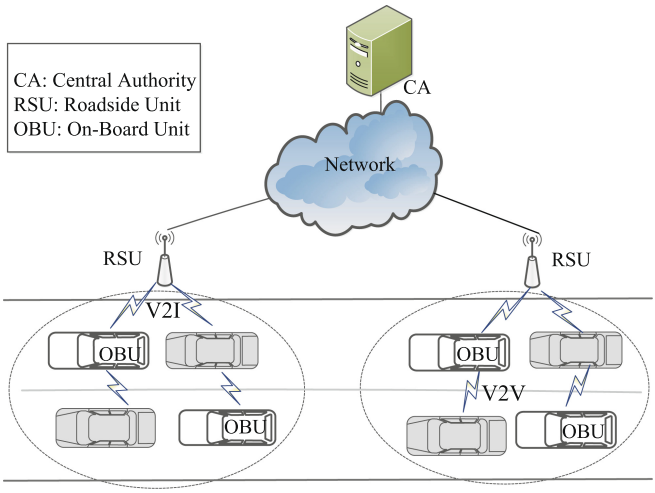

Fig. 1. Simulation results for the network.

Group signature schemes can also be used to achieve privacy preservation [12,13,17]. For example, Hwang et al. [18–20] introduced three group signature schemes with controllability linkability, for purpose of preserving the privacy between the users and service providers. However, these schemes do not support threshold authentication and require significant computing cost due to the number of exponentiation operations and bilinear pairings operations.

Threshold authentication is a common approach to assure the authenticity of the received (traffic) information [21–23]. For example, Shao et al. [24,25] introduced two threshold anonymous authentication schemes for vehicle sensor networks, designed to resist an attack on a single malicious message. However, the cost of computation of these schemes is significantly high on account of the employment of exponentiation and bilinear pairing.

Therefore, in this work, we construct a group signature-based anonymous authentication scheme with controllable linkability, based on Shao et al.'s [24,25] scheme. However, our proposed scheme is more efficient because we utilize the point multiplication operation instead of the exponentiation operations.

3 Preliminaries

Before the construction of our scheme, preliminaries including the system and security models and the Bilinear groups are introduced in this section.

3.1 System and Security Models

Our proposed protocol comprises four entities, namely: central authority (CA), service providers (SP), RSUs and OBUs (see also Fig. 2). CA is mainly tasked with issuing of the corresponding public key certificates for both RSUs and OBUs after their respective public keys have been successfully authenticated. Moreover, CA can uncover the original identity of the sender who is found to send a fabricated message in VANET. SP is responsible for providing personalized services, first by examining whether given two messages are produced by the same sender with the linking key. RSUs are densely deployed along the road, and each of them is assumed as the manager of a group consisting of OBUs within its communication area. Besides, RSUs are also responsible for issuing group certificates for vehicles equipped with OBUs when they enter into its communication range, which can be used to communicate with other OBUs by signing the message with its private key. Note that if an OBU is in the revocation list obtained from the CA, it would not be assigned with a group certificate by its RSU.

CA is assumed to be fully honest, whereas SPs and RSUs are presumed to be semi-honest (i.e., honest but curious), in the sense that they would honestly follow the proposed protocol and would not conspire with other RSUs. However, they are curious about the user's identity information and trace information, and hence may passively seek to collect group signatures and gather other information. Honest OBUs can accept a message only when they have received the number of valid signatures whose number is greater than the threshold value on the same message. However, OBUs could also be malicious, in the sense of attempting to obtain the user's identity information and trace information by launching either passive or active attack. For instance, they may attempt to broadcast many fabricated message signatures without being perceived or conspire with each other.

3.2 Bilinear Groups

Let G_1, G_2 and G_3 denote three different additive groups over elliptic curve with the same order q, where q is a prime number, and they all satisfy non-degenerated properties and are used to construct a bilinear map $e : G_1 \times G_2 \rightarrow G_3$, such that $e(aP_1, b\tilde{P}_1) = e(P_1, \tilde{P}_1)^{ab}$ for all $a, b \in Z_q^*$, any $P_1 \in G_1$ and $\tilde{P}_1 \in G_2$. For convenience, the symbol "$\sim$" is used to label the elements in G_2.

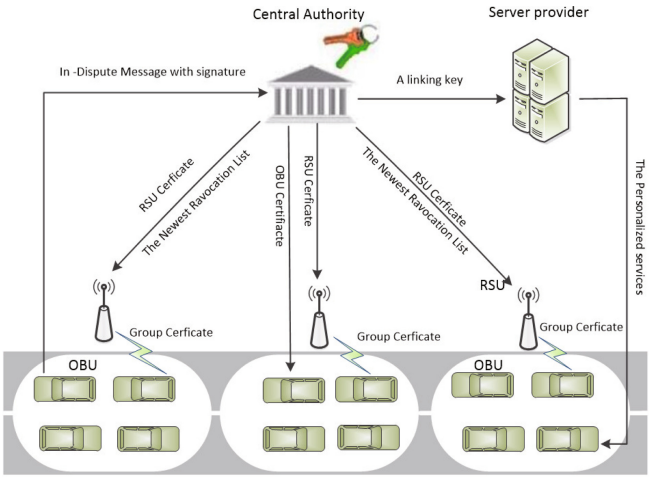

Fig. 2. System model.

We analyze the security of the proposed threshold anonymous authentication scheme based on the eCDH assumption and the eDDH assumption, which are defined as follows [25],

Definition 1 (eCDH Assumption): Given $P, aP, bP \in G_1$ and $\tilde{P}, a\tilde{P} \in G_2$, where $a, b \in Z_q^*$, to output abP. The (t, ε) eCDH assumption states that there is no t-time algorithm that can break the eCDH assumption with a non-negligible advantage of at least ε.

Definition 2 (eDDH Assumption): Given $P, aP, bP, cP \in G_1$ and $\tilde{P}, a\tilde{P}, b\tilde{P} \in G_2$, where $a, b, c \in Z_q^*$, to decide whether $abP = cP$ holds or not. The (t, ε) eDDH assumption states that there is no t-time algorithm can break the eDDH assumption with non-negligible advantage of at least ε.

4 Proposed Authentication Protocol

The construction of our proposed group signature-based anonymous authentication scheme with controllable linkability is illustrated here, and the scheme includes initialization, registration, joining, signing, verifying, linking, and tracing stage.

First, the CA follows the initialization process to produce public/private key pairs for itself and the public parameters for the entire system. Before each RSU and OBU join the network, they need to follow the registration process to produce the pairs of the public key and private key for itself and obtain corresponding public certificates from the CA. RSUs are deployed on critical points along the road (e.g., roadsides or building and other installations). When a vehicle employed with an OBU enters into a new range covered by a certain RSU, it has to follow the joining process to obtain the corresponding group certificate from the RSU. Then, the vehicle can sign and broadcast messages. After that, the receiver can perform the threshold authentication process to verify any received messages and signatures. In order to identify the malicious signer, the CA can perform identity tracing process to uncover the identity of the singer corresponding to the suspicious signature. To provide personalized service, one can perform linking process to check whether two given pairs of signatures and messages are from the same sender.

The definition of used notations is shown as Table 1, and details of our proposed authentication scheme is illustrated in the remaining of this section.

Table 1. Summary of notations

Notation	Definitions
q	A secure large prime
G_1, G_2, G_3	Three groups with the same order q
P_1, P_2	The primitive generator of G_1
$\tilde{P}_1$	The primitive generator of G_2
x_{ca}	The private key of CA to issue certificates
x_{tm}	The private key of CA to trace
x_{rsu}	The private key of RSU
x_{obu}	The private key of OBU
P_{link}	The linking key of SPs
$(P_{ca}, \tilde{P}_{ca}, \tilde{P}_{tm})$	The public key of CA
$\tilde{P}_{rsu}$	The public key of RSU
$\tilde{P}_{obu}$	The public key of OBU
Z_q^*	The collection including all primes in $\{0, 1, ..., q-1\}$
H_1	A hash function mapping to G_1
H_2	A hash function mapping to Z_q^*
τ	A signature of message

4.1 Initialization

In this stage, CA produces the key pairs for itself and the public parameters for the entire system. The detailed description is as follows.

- First, CA produces the public parameter $q, P_1, P_2 \in G_1, \tilde{P}_1 \in G_2, e : G_1 \times G_2 \to G_3, H_1(\cdot) : \{0,1\}^* \to G_1, H_2(\cdot) : \{0,1\}^* \to Z_q^*$.
- Then, CA randomly chooses $x_{ca}, x_{tm} \in Z_q^*$, and computes $P_{ca} = x_{ca}P_1, \tilde{P}_{ca} = x_{ca}\tilde{P}_1$ and $\tilde{P}_{tm} = x_{tm}\tilde{P}_1, P_{link} = -x_{tm}P_1$. Finally, CA sets P_{link} as the linking key, $(P_{ca}, \tilde{P}_{ca}, \tilde{P}_{tm})$ as its public key and keeps (x_{ca}, x_{tm}) as its private key.

4.2 Registration

The registration stage consists of two parts, namely: RSU registration and OBU registration. CA assign RSUs and OBUs with the corresponding public certificates by performing this process.

RSU Registration. Each RSU registers itself as follows,

- RSU selects $x_{rsu} \in Z_q^*$ randomly as its private key, and evaluates $\tilde{P}_{rsu} = x_{rsu}\tilde{P}_1$ as its public key.
- RSU sends $\tilde{P}_{rsu}$ to CA through a secure channel. After receiving the message, CA produces a public certificate $cert_{rsu}$ on $\tilde{P}_{rsu}$, and sends $cert_{rsu}$ and the current revocation list CRL to RSU, where CRL is defined as

$$\begin{aligned} CRL =&((cert_{obu\_1}, \tilde{P}'_{obu\_1}), (cert_{obu\_2}, \tilde{P}'_{obu\_2}), \cdots, \\ &(cert_{obu\_n}, \tilde{P}'_{obu\_n})) \end{aligned}$$

Vehicle OBU Registration

- Each OBU selects $x_{obu} \in Z_q^*$ randomly as its private key and evaluates $P_{obu} = x_{obu}P_1$ as its public key.
- Then, OBU sends P_{obu} and $\tilde{P}_{obu} = x_{obu}\tilde{P}_1$ to CA through a secure channel. After receiving the message, if $e(P_{obu}, \tilde{P}_1) = e(P_1, \tilde{P}_{obu})$ holds, then CA produces corresponding public certificate $cert_{obu}$ on P_{obu}, and sends $cert_{obu}$ to the OBU. Finally, CA records $(cert_{obu}, \tilde{P}_{obu})$ in the user list.

4.3 Joining

In this stage, RSUs will issue corresponding group certificate for the OBUs within their radio coverage. When OBU_i gets into the communication area covered by a new RSU, the joining stage is activated between OBU_i and the particular RSU. The detailed steps are as follows.

- To begin with, OBU_i sends a request message to RSU for obtaining its public key,
- Upon receiving the request from OBU_i, RSU returns its certificate and public key $(cert_{rsu}, \tilde{P}_{rsu})$ to OBU_i.

- Upon receiving $(cert_{rsu}, \tilde{P}_{rsu})$, OBU_i checks $(cert_{rsu}, \tilde{P}_{rsu})$. If it is not valid, OBU_i would be required to send another request message again; otherwise, OBU_i selects $k, n \in Z_q^*$ randomly and computes $P'_{obu} = x_{obu}P_{ca}$. Then, it uses the public key of RSU $\tilde{P}_{rsu}$ to encrypt P'_{obu}, where the encrypting process is found by computing $k\tilde{P}_{rsu} = (x_1, y_1)$ and $C_{obu} = (k\tilde{P}_1, P'_{obu} + x_1P_1)$. Finally, OBU_i sends $(cert_{obu}, P_{obu}, C_{obu}, n)$ to RSU, where n is a random number chosen from Z_q^*.
- Upon receiving $(cert_{obu}, P_{obu}, C_{obu}, n)$, RSU uses its private key x_{rsu} to decrypt C_{obu} and obtains P'_{obu}, and checks whether $cert_{obu}$ exists in the revocation list CRL. Then it checks whether $e(P_{obu}, \tilde{P}_{ca}) = e(P'_{obu}, \tilde{P}_1)$. If it does not holds, then it terminates at this stage; otherwise, RSU chooses two random numbers $r, t \in Z_q^*$ and computes group certificate $cert_g = (c_1, c_2)$, where $c_1 = x_{rsu}P_2 - r(P'_{obu}), c_2 = rP_1$. Finally, RSU adds OBU_i's certificate $cert_{obu}$ to member list(ML) and uses OBU_i's public key P_{obu} to encrypt $cert_g$, where the encrypting process is found by computing $tP_{obu} = (x_2, y_2)$ and $C_{rsu} = (tP_1, c_2 + x_2P_1, c_1 + x_2P_1)$. It then broadcasts (C_{rsu}, n, CRL_{rsu}) within its communication range, where CRL_{rsu} is the latest and is obtained from CRL and $cert_{obu}$ exists in ML of this RSU.
- When OBU_i receives (C_{rsu}, n, CRL_{rsu}), OBU_i first determines whether this message is sent to itself by using the value n. If it holds, then OBU_i uses its private key x_{obu} to decrypt C_{rsu} and obtains $cert_g$, prior to checking whether $e(c_1, \tilde{P}_1) \cdot e(x_{obu}c_2, \tilde{P}_{ca}) = e(P_2, \tilde{P}_{rsu})$. If it holds, then OBU_i accepts this group certificate $cert_g = (c_1, c_2)$; otherwise, OBU_i sends the request message to RSU again.

4.4 Signing

When an OBU intends to broadcast a message m, it performs the following steps to sign the message.

- OBU_i chooses $r', \alpha, s \in Z_q^*$ randomly.
- Randomizes the group certificate as $\tau_1 = c_1 - r'(x_{obu}P_{ca})$ and $\tau_2 = c_2 + r'P_1$.
- Encrypts $\tilde{P}_{obu}$ for tracing as $\tilde{\tau}_3 = \alpha \cdot \tilde{P}_1$, $\tilde{\tau}_4 = x_{obu} \cdot \tilde{P}_1 + \alpha \cdot \tilde{P}_{tm}$.
- Binds (τ_1, τ_2) and $\tilde{\tau}_3, \tilde{\tau}_4$ together by $\tau_5 = x_{obu} \cdot \tau_2$ and $\tau_6 = \alpha \cdot \tau_2$.
- Computes $\tau_7 = x_{obu}H_1(m)$, which would be employed to determine whether two given signatures for a certain message are produced by a same OBU or not. However, the characteristic of threshold authentication is enabled by τ_7.
- A bundle of the above evaluated values is made by $S_1 = s \cdot \tau_2$, $S_2 = s \cdot H_1(m)$, $\sigma_8 = H_2(m||\tau_1|| \cdots ||\tau_7||S_1||S_2)$, $\tau_9 = s - \tau_8 x_{obu}$.
- Set $\tau = \{\tau_1, \tau_2, \tilde{\tau}_3, \tilde{\tau}_4, \tau_5, \tau_6, \tau_7, \tau_8, \tau_9\}$ and broadcast (m, τ).

4.5 Verifying

Upon receiving a message m and its signature τ, OBU_j uses CA's public key $(\tilde{P}_{ca}, \tilde{P}_{tm})$, RSU's public key $\tilde{P}_{rsu}$, and the revocation list CRL_{rsu} to verify this signature as follows:

- Signature verification: Initially check if the signature $\{\tau_1, \tau_2, \tilde{\tau}_3, \tilde{\tau}_4, \tau_5, \tau_6, \tau_7, \tau_8, \tau_9\}$ is valid by checking the following equations.
  - $e(\tau_1, \tilde{P}_1) \cdot e(\tau_5, \tilde{P}_{ca}) = e(P_2, \tilde{P}_{rsu})$
  - $e(\tau_2, \tilde{\tau}_3 + \tilde{\tau}_4) = e(\tau_5, \tilde{P}_1) \cdot e(\tau_6, \tilde{P}_{tm} + \tilde{P}_1)$
  - $S_1 = \tau_9\tau_2 + \tau_8\tau_5$
  - $S_2 = \tau_9 H_1(m) + \tau_8 \cdot \tau_7$
  - check $\tau_8 = H_2(m||\tau_1|| \cdots ||\tau_7||S_1||S_2)$
- Revocation check: Check whether the signer within this RSU range is not revoked, by checking the equation $e(\tau_1, \tilde{P}_1) \cdot e(\tau_2, \tilde{P}'_{obu\_i}) \neq e(P_2, \tilde{P}_{rsu})$, for all $\tilde{P}'_{obu\_i} \in CRL_{rsu}$.

If all equations hold, then OBU_j believes the validity of the signature, i.e., the sender of the signature has not been revoked. Once OBU_j had received exceeding threshold number of valid signatures about the same message from distinctive OBUs, it would accept and believe the message.

In addition, the OBU can also use batch verification to speed up the verification on $\{m_1, \tau^1\}$, $\{m_2, \tau^2\}$, $\cdots$, $\{m_n, \tau^n\}$, as follows,

- $e(\sum_{i=1}^{n} \tau_1^i, \tilde{P}_1) \cdot e(\sum_{i=1}^{n} \tau_5^i, \tilde{P}_{ca}) = e(P_2, \tilde{P}_{rsu})$
- $\prod_{i=1}^{n} e(\tau_2^i, \tilde{\tau}_3^i + \tilde{\tau}_4^i) = e(\sum_{i=1}^{n} \tau_5^i, \tilde{P}_1) \cdot e(\sum_{i=1}^{n} \tau_6^i, \tilde{P}_{tm} + \tilde{P}_1)$

4.6 Linking

With the linking key P_{link}, SP can check whether two given pairs (m', τ') and (m, τ) are generated by a same user, as follows:

- First, it performs the verification process to check the validity of two given signatures.
- If the pairs are not valid, $\perp$ would be returned; otherwise, it examines whether the equation $e(P_{link}, \tilde{\tau}'_3) \cdot e(P_1, \tilde{\tau}'_4) = e(P_{link}, \tilde{\tau}''_3) \cdot e(P_1, \tilde{\tau}''_4)$ holds or not. If yes, 1 would be returned, i.e., the pairs are linked; otherwise, 0 would be returned, i.e., the pairs are unlinked.

4.7 Tracing

In this stage, CA can recover the real identity of the sender corresponding to a valid pair (m, τ), then it updates the CRL and sends CRL to each RSU. The detailed process is as follows.

- First, CA reveals the identity of signer corresponding to the signature message (m, τ) by computing $\tilde{P}_{obu} = \tilde{\tau}_4 - x_{tm}\tilde{\tau}_3$.
- Then, CA finds signer's certificate $cert_{obu}$ in user list and computes $\tilde{P}'_{obu} = x_{ca}\tilde{P}_{obu}$.
- Finally, CA records $(cert_{obu}, \tilde{P}'_{obu})$ in CRL and sends CRL to each RSU.

5 Conclusion

In this paper, a group signature-based anonymous authentication scheme with controllable linkabilty was proposed. The scheme is designed to enable providers who have an linking key to determine whether two messages were produced by the same signer, while preserving the user's anonymity. Threshold authentication enables the receiver to figure out whether the received signature is produced by the same sender to prevent the replay attack. In addition, the function of verifier-local revocation is supported (i.e., a verifier is able to check whether a received signature is generated by a revoked user). Security and performance evaluations demonstrated the utility of our presented scheme.

References

1. Hubaux, J.P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Secur. Priv. **3**(2), 49–55 (2004)
2. Chuang, M.C., Lee, J.F.: TEAM: trust-extended authentication mechanism for vehicular ad hoc networks. IEEE Syst. J. **8**(3), 749–758 (2014)
3. Zhou, Y., Zhao, X., Jiang, Y., Shang, F., Deng, S., Wang, X.: An enhanced privacy-preserving authentication scheme for vehicle sensor networks. Sensors **17**(12), 2854 (2017)
4. Huang, X., Xiang, Y., Chonka, A., Deng, R.H.: A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Trans. Parall. Distr. **22**(8), 1390–1397 (2011)
5. Bohli, J.M., Pashalidis, A.: Relations among privacy notions. ACM **14**(1), 362–380 (2011)
6. Li, J., Lu, H., Guizani, M.: ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans. Parall. Distr. **26**(4), 938–948 (2015)
7. Hao, H., Lu, R., Cheng, H.: TripSense: a trust-based vehicular platoon crowdsensing scheme with privacy preservation in VANETs. Sensors **16**(6), 803 (2016)
8. Fayyad, U.M., PiatetskyShapiro, G., Smyth, P.: From data mining to knowledge discovery: an overview. Adv. Knowl. Disc. Data Min. **17**(3), 1–34 (1996)
9. Wang, H., Qin, B., Wu, Q., Domingo-Ferrer, J.: TPP: traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids. IEEE Trans. Inf. Forensics Secur. **10**(11), 2340–2351 (2017)
10. Zhao, D., Peng, H., Li, L., Yang, Y.: A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wirel. Pers. Commun. **78**(1), 247–269 (2014). https://doi.org/10.1007/s11277-014-1750-y
11. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_22
12. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_3
13. Chaurasia, B.K., Verma, S., Bhasker, S.M.: Message broadcast in VANETs using group signature. In: IEEE Fourth International Conference on Wireless Communication Sensor Networks (WCSN 2009), pp. 131–136, December 2008

14. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
15. Lu, R., Lin, X., Zhu, H., Ho, P.H., Shen, X.: ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of IEEE Infocom, pp. 1229–1237, 14–18 April 2008
16. Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W.: Certificateless signatures. Comput. J. **55**(4), 457–474 (2012)
17. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
18. Hwang, J.Y., Lee, S., Chung, B.H., Cho, H.S., Nyang, D.H.: Short group signatures with controllable linkability. In: Proceedings of LightSec, pp. 44–52, March 2011
19. Hwang, J.Y., Lee, S., Chuang, B.H., Cho, H.S., Nyang, D.H.: Group signatures with controllable linkability for dynamic membership. Inform. Sci. **222**(3), 761–778 (2013)
20. Hwang, J.Y., Chen, L., Cho, H.S., Nyang, D.H.: Short dynamic group signature scheme supporting controllable linkability. IEEE Trans. Iin. Foren. Sec. **10**(6), 1109–1124 (2015)
21. Harn, L.: Group authentication. IEEE Trans. Comput. **62**(9), 1893–1898 (2013)
22. Zhang, L., Wu, Q., Solanas, A., Domingo-Ferrer, J.: A scalable robust authentication protocol for secure vehicular communications. IEEE Trans. Veh. Technol. **59**(4), 1606–1617 (2010)
23. Morshed, M.M., Atkins, A., Yu, H.: Efficient mutual authentication protocol for radiofrequency identification systems. IET Commun. **6**(16), 2715–2724 (2012)
24. Shao, J., Lu, R., Lin X., Zou, C.: New threshold anonymous authentication for VANETs. In: IEEE ICC, pp. 1–6, November 2015
25. Shao, J., Lin, X., Lu, R., Zou, C.: A threshold anonymous authentication protocol for VANETs. EEE Trans. Veh. Technol. **65**(3), 1711–1720 (2016)