Efficient Privacy Protection Authentication Scheme in Vehicle Ad Hoc Networks

Lv ShanGuo(✉)

Software School, East China Jiaotong University, Nanchang, China
42883824@qq.com

Abstract. In this paper, a group signature-based vehicle information sharing scheme for vehicular ad hoc networks with effective privacy protection is proposed. The design goals are achieved by technologies such as distributed management, HMAC, batch signature verification and cooperative authentication. First, divide the entire network into different domains for local management. Second, HMAC is used instead of time-consuming revocation list checking, and the integrity of messages prior to bulk authentication is ensured to avoid the number of invalid messages in bulk verification. Finally, we also use the cooperative certification method to further improve the efficiency of the program. By adopting the above technology, our proposed solution can meet the verification requirements. Security and performance analysis shows that our proposed solution enables efficient group signature-based authentication while maintaining conditional privacy.

Keywords: Group signature · Ad Hoc networks · Privacy protection authentication

1 Introduction

With the rapid development of wireless communication, ad hoc networks and Internet of things technology, in recent years, vehicular ad hoc networks have been widely concerned by academia, industry and government departments. In order to improve the traffic situation, vehicles need to periodically perceive the relevant information of their own driving process, such as the position, speed and direction of the vehicle, and broadcast these information to the surrounding vehicles by wireless communication, so as to realize the sharing of traffic-related information between them, so that drivers and traffic managers can obtain the vehicles of other vehicles beyond the visual range. Real-time and comprehensive road condition information can effectively improve traffic safety and efficiency, and fundamentally solve the existing road traffic accidents and congestion problems [1]. In the vehicular ad hoc network, between the vehicle and the vehicle, the vehicle and the roadside unit communicate wirelessly. Once the user's hidden information, such as identity, trajectory and references are not well protected [2], the attacker can easily get this information.

In order to achieve efficient anonymous authentication in vehicular ad hoc networks, group signature technology is widely used in vehicular ad hoc networks [3]. Because it allows group members to sign messages in the name of the group, while not

J. Vaidya et al. (Eds.): CSS 2019, LNCS 11982, pp. 279–288, 2019.
https://doi.org/10.1007/978-3-030-37337-5_23

revealing the true identity of the signer. In order to verify a group signature, it takes 11 ms [8], which means that only 91 messages can be authenticated per second. However, when there is 180 vehicles in the communication range of a roadside unit [1], it needs to authenticate 600 safety-related messages per second. Additional authentication and decryption time will be consumed if the value service is considered again [4]. In addition, before group signature verification, vehicles need to check the revocation list to avoid communication with revoked vehicles. According to the literature [1], it takes 9 ms to check an identity in the revocation list. If there are n vehicles that are revoked in the revocation list, each message takes 9n + 11 ms. In this way, the number of messages that can be authenticated per second is 1000/(9n + 11), which is far from the target 600 messages. Therefore, it is necessary to reduce the delay due to the authentication of the revocation list check and the group signature to achieve fast authentication.

In order to solve the problem of revocation list checking, Wasef et al. [5] and Jiang et al. [6] used the hash message digest code HMAC instead of the revocation list, which greatly reduced the inspection time. In the scheme of Wasef et al., the key for calculating the HMAC is global. Once an illegal vehicle is discovered, a global key update process will be performed, which is another form of revocation list and is difficult to implement. Jiang et al. adopted a distributed approach to further improve the efficiency of HMAC inspection. However, both schemes are based on pseudonym authentication schemes and may not be directly applicable to group signature-based schemes. In order to reduce the time of signature verification, Wasef et al. [7] and Zhang et al. [3] adopted the method of batch verification of group signatures, which made a large number of messages can be authenticated in time. However, the problem is that they do not check the integrity of messages before batch authentication. Once there is an invalid message caused by packet loss or malicious injection in the wireless channel, it will lead to additional authentication delay and loss of efficiency. Even if we do not consider the problem of re-authentication, the computational overhead of group signature batch authentication in document [3] is $2T_{pai} + 13nT_{mul}$, while that in document [7] is $3T_{pai} + (6n + 7)T_{mul}$. T_{pai} is the time to perform pairing operation, T_{mul} is the time to perform point multiplication [7]. According to literature [1], it runs on Intel Pentium IV3.0GHZ main frequency computer. T_{pai} is 4.5 ms, T_{mul} is 0.6 ms. Therefore, without considering invalid messages, literature [3] can only authenticate 127 and 274 messages per second, which still fails to meet the requirements of the number of authenticated messages.

The solutions mentioned above focus only on how to achieve fast certification in a single vehicle. However, based on the fact that nearby vehicles require authentication to be almost identical, Zhang et al. [8] and Hao et al. [9] proposed a scheme based on inter-vehicle cooperative certification. By allowing neighboring vehicles to collaborate for certification, their solution allows a vehicle to know the legitimacy of all received messages without having to verify all received messages. Zhang et al.'s scheme uses a Pseudonym-based authentication scheme, while Hao et al.'s scheme is based on group signature. However, although Hao et al.'s scheme can meet the authentication requirement per second, their scheme does not consider revocation list checking. Therefore, the efficiency of their schemes will be reduced in practical application.

In order to achieve efficient and anonymous authentication in vehicular ad hoc networks, Zhu et al. [10] proposed an efficient conditional privacy protection authentication scheme. In this scheme, RSUs are assumed to be credible. However, in practical applications, RSUs may want to obtain user's privacy information. Some existing schemes, such as document [11], consider the security of semi-trusted RSUs in vehicular ad hoc networks.

Under the model of semi-trusted RSUs, by combining distributed management technology, HMAC, batch verification group signature and cooperative authentication, this paper proposes an efficient conditional privacy authentication scheme to realize real-time information sharing during vehicle driving. First, the jurisdictional area is divided into several domains to implement regional management; then, the HMAC is calculated using the key generated by the self-healing group key generation algorithm [12], thereby replacing the time-consuming revocation list checksum. Ensure the integrity of the message before batch verification of the group signature; finally, an example of the Hao et al. cooperative authentication scheme [9] is given to improve its authentication efficiency. Security and performance analysis show that the proposed scheme can achieve higher group signature-based authentication efficiency while achieving conditional concealment.

2 System Model

As shown in Fig. 1, the system model involved in this paper consists of TMC, RSUs fixed to the roadside unit, and OBUs loaded on the moving vehicle:

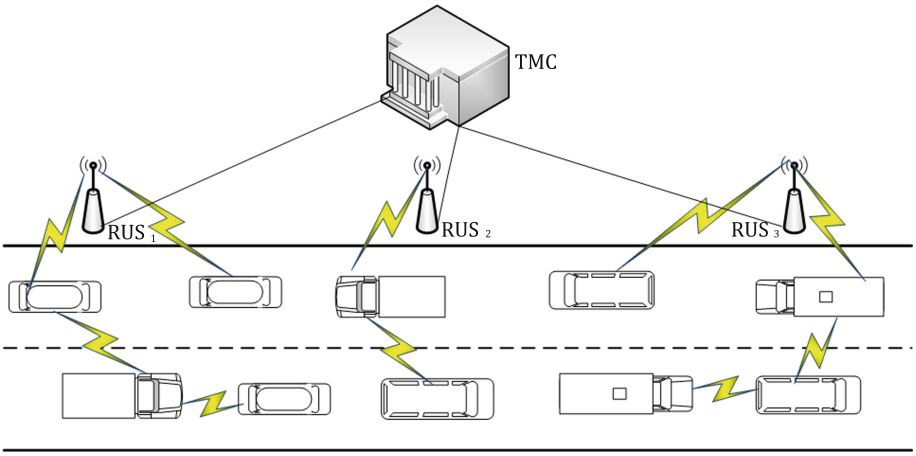

Fig. 1. System model of vehicular ad hoc network.

(1) TMC is a trusted management center for the entire network. When joining the network, RSUs and OBUs need to register at the TMC and obtain a certificate. The TMC also divides its entire jurisdiction into several different domains,

and generates a corresponding group key and group signature material for each domain, and then the TMC sends these security materials to all RSUs in the domain. In general, assume that the TMC has unlimited communication capabilities, computing power, and storage space, and assumes that the attacker is unable to capture the TMC.

(2) RSUs manage vehicles within their communication range. The RSUs connect to the TMC through a wired channel and connect to the OBUs through a wireless channel. They are the bridge between the connecting TMC and the user. In this article, assume that RSUs are semi-trusted [11], for example, they will run as predefined by the system, but they may reveal some secret information to the attacker. The RSUs also have the function of distributing the group key material and the group signing key to the legal OBUs entering the domain.

(3) The OBUs periodically broadcast traffic-related status information including location, speed, and direction of travel to improve the road environment and traffic safety of drivers and pedestrians. We also assume that each vehicle has a Tamper-Proof Device to store safety-related materials.

Without loss of generality, this paper does not consider sharing secrets between vehicles and other users, because almost all security systems cannot prevent this type of active attack.

3 Solution

3.1 System Initialization

In this paper, SCHNONRR signature algorithm [13] is used as the basic signature algorithms of TMC, RSUs and OBUs. TMC selection:

(1) Prime numbers P and g satisfy $q|p-1, q \geq 2^{140}, p \geq 2^{512}$;
(2) $\alpha \in \mathbb{Z}_p$, and the order is g, for example $\alpha^q = 1(\mathrm{mod}\, p), \alpha \neq 1$;
(3) A one-way hash function $h(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^l$;
(4) A random number $s \in \mathbb{Z}_q^*$ as its private key, then $SK_{TMC} = s$.

Then calculate its public key $PK_{TMC} = p^s$ and expose the system parameter tuple $(p, q, \alpha, h(\cdot), PK_{TMC})$.

3.2 Certificate Distribution for RSUs

TMC divides the jurisdiction into several domains, each containing several RSUs. For the roadside unit R_x in the domain, the TMC verifies its identity and distributes the certificate $Cert_{TMC,R_x}$ as follows:

(1) TMC selects a random number $Sk_{R_x} \in \mathbb{Z}_q^*$ as the private key of R_x, and calculates the public key $PK_{R_x} = p^{SK_{R_x}}$;
(2) TMC calculates the signature $\sigma_{TA,R_x} = Sig_{SK_{TA}}(PK_{R_x}||D_A)$;
(3) TMC transmits SK_{R_x} and $Cert_{TMC,R_x}$ to R_x through the secure channel, where $Cert_{TA,R_x} = (PK_{R_x}||D_A, \sigma_{TA,R_x})$.

3.3 Certificate Distribution of Vehicles

For the vehicle V_i, after the TMC has verified its identity, the certificate $Cert_{TMC,R_x}$ is distributed as follows:

(1) TMC selects a random number $Sk_{V_i} \in \mathbb{Z}_q^*$ as the private key of V_i, and calculate its corresponding public key $PK_{V_i} = p^{SK_i}$;
(2) TMC calculates the certificate $Cert_{TA,V_i} = Sig_{SK_{TA}}(PK_{V_i})$ of V_i;
(3) TMC securely transmits Sk_{V_i} and $Cert_{TMC,V_i}$ to the vehicle V_i.

3.4 Secure Group Key Distribution and Batch Authentication

For the domain D_A, the TMC generates the group signature key, the public material and the group public key GPK_{D_A}. This paper uses the Wasef scheme [7] to implement the batch verification group signature.

Given the linear pair parameters $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, the TMC generates the group public key as follows:

(1) TMC selects a random generator $g_2 \in \mathbb{G}_2$ and calculates $g_1 \in \psi(g_2)$, where g_1 is the generator of $\mathbb{G}_1$, and the isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, such as $g_1 \in \psi(g_2)$;
(2) TMC selects the random numbers $h, u, v \in \mathbb{G}_1$ and $s_1, s_2 \in Z_p$, makes $u^{s_1} = v^{s_2} = h$;
(3) TMC selects the random numbers $\gamma \in \mathbb{Z}_p$ and $\lambda \in \mathbb{Z}_p^*$, makes $\omega = g_2^{\gamma}$.

Where s_1 and s_2 are the master private keys of the domain D_A that are managed by the TMC. The public system parameters of the domain D_A are $(g_1, g_2, u, v, h, \lambda)$, the group public key is $GPK_{D_A} = \omega$, the TMC sends the system public parameters and the group public key to all RSUs of the domain. Vehicles and roadside units can use these pre-stored information to achieve mutual authentication. When a vehicle V_i joins a new domain D_A, it needs the first RSUs registry in the domain D_A, which prevents illegal vehicles from joining the domain D_A.

Registration: When V_i joins a new domain, a mutual authentication protocol will be executed between V_i and the first roadside unit it encounter. It should be noted that if a roadside unit is captured, the TMC will revoke the roadside unit by broadcasting its domain and its identity, so that all vehicles will also know the revocation information.

(1) Each roadside unit periodically broadcasts its certificate, its domain and group public key. For the way unit R_x in the domain D_A, it broadcasts the message message 1: $\left(PK_{R_x}, D_A, Cert_{TMC,R_x}, GPK_{D_A}, Sig_{SK_{R_x}}(GPK_{D_A})\right)$. When V_i receives the message, it first verifies whether D_A is a new domain. If D_A is a new domain, V_i will begin the registration process. V_i first authenticates the legitimacy of R_x by running $Verify(PK_{TMC}, PK_{R_x}||D_A, \sigma_{TMC,R_x})$, if $Cert_{TMC,R_x}$ is Legally, V_i will verify $Sig_{SK_{R_x}}(GPK_{D_A})$ by PK_{R_x}.
(2) After authenticating R_x and D_A is a new domain, V_i will reply to the message message 2: $\left\{PK_{V_i}, Cert_{TMC,V_i}, x_i, Sig_{SK_{V_i}}(x_i)\right\}_{PK_{R_x}}$ to R_x, where x_i is the random number used to calculate the group private key GSK_{D_A,V_i}. It is worth noting the

public key and certificate $Cert_{TA,V_i}$ of V_i is unique throughout the system. Therefore, it is also an identity of V_i. In the proposed scheme, the public key and certificate of V_i are encrypted by PK_{R_x} of R_x, which allows only R_x to obtain the corresponding plaintext, thus protecting the identity privacy of R_x.

(3) After obtaining GSK_{D_A,V_i}, R_x will reply V_i message 3: $\{H(GSK_{D_AV_i}), Sig_{SK_{R_x}}(H(GSK_{D_AV_i}), x_i)\}_{PK_{V_i}}$. When V_i receives the message 3, it first decrypts the message with its private key SK_{V_i} and then verifies the signature.

(4) If the signature is valid, V_i will reply message 4: $\{T, H(V_i||x_i), Sig_{SK_{V_i}}(H(V_i||x_i), T)\}$ to R_x, where T is a timestamp. When R_x receives message 4 at T^*, Algorithm will be executed. Where, $f(TID_i, y)$ is such as $s_{0,0} + s_{1,0} \cdot x + s_{0,1} \cdot y + s_{1,1} \cdot xy + \cdots + s_{t,t} \cdot x^t y^t$ A binary polynomial, where x and y are two variables and $s_{i,j}$ is a constant coefficient. K^B_{m-j-l} and K^F_j are seeds for calculating the group key, l is the length of the backward hash chain, and LC is the life cycle of the group key.

(5) Then, R_x sends a message 5 $\{GSK_{D_AV_i}, LC, l, K^B_{m-j-l}, K^F_j, TID_i, f(TID_i, y), \mathrm{Sig}_1\}_{PK_{V_i}}$ to V_i. After receiving the message 5 sent from R_x, V_i will execute Algorithm to obtain the group key required to calculate the HMAC. We use the formula (1) to calculate the current group key GK_j, where K^F_j and K^B_{m-j+1} are the forward keychain and backward key chain respectively.

$$GK_j = H\left(K^F_j + K^B_{m-j+1}\right) \tag{1}$$

Finally, R_x stores the information shown in Fig. 2, V_i also stores the information shown in Fig. 3.

χ_i	GPR_{D_y,V_i}	$H(V_i \mid\mid \chi_i)$	PK_{V_i}	T

Fig. 2. Records stored at R_x

χ_i	GPR_{D_y,V_i}	$Sig_{SK_{R_X}}(H(GPR_{D_y,V_i}), \chi_i)$

Fig. 3. Records stored at V_i

Batch Verification: According to DSRC [2], vehicles need periodic broadcast security-related messages every 300 ms. In order to ensure the legitimacy of the message source and the integrity of the message, the receiver of the message should verify the received message. Cancellation list checking is a commonly used method to exclude illegal vehicles before authentication. However, according to document [1],

group signatures take about 9 ms to check whether an identity is in the revocation list. Therefore, if a vehicle receives n messages and the number of vehicles revoked is m, it takes 9 ms for the vehicle to verify the identity legitimacy of the sender. Obviously, revocation list checking results in a lot of computational overhead, which seriously reduces the performance of the system.

3.5 Periodic Update of Group Key

When V_i is authenticated by an RSUs in the domain D_A, it periodically receives a message of the group key update broadcast by the RSUs in the domain D_A. The message B_{j+1} of the $(j+1)$th update period is as shown in the formula (2):

$$\begin{cases} B_{j+1} = \{r_{j+1}(x)\} \cup \{p_{j+1}(x)\} \\ r_{j+1}(x) = (x - TID_{r_1})(x - TID_{r_2}) \cdots (x - TID_{r_w}) \\ p_{j+1}(x) = r_{j+1}(x)K^B_{m-j} + f\left(x, K^F_{j+1}\right) \end{cases} \tag{2}$$

Where $TID_{r_1}, TID_{r_2}, \ldots, TID_{r_w}$ is the temporary identity of the vehicle being revoked, It has obtained the group key material $f(TID_i, y), K^B_{m-j+1}$ and K^F_j in the domain D_A before the $(j+1)$th period, and Vehicles that were revoked during the $(j+1)$ period. $r_{j+1}(x)$ is the undoing polynomial of the $(j+1)$th cycle, $p_{j+1}(x)$ is a hidden polynomial of the $(j+1)$th cycle.

It is worth noting that only the vehicle that is legally certified by domain D_A can obtain the group key material, and the RSUs only need to manage the vehicles in the domain. Therefore, the vehicles that are revoked are very few, and each vehicle has only one temporary identity to calculate $f(TID_i, y)$, so $p_{j+1}(x)$ is very small.

After V_i receives the broadcast revocation B_{j+1}, it uses K^F_j to calculate $K^F_{j+1} = H\left(K^F_j\right)$ and $f\left(TID_i, K^F_{j+1}\right)$. Then, V_i calculates $p_{j+1}(TID_i)$, and obtains K^B_{m-j} by formula (3):

$$K^B_{m-j} = \frac{p_{j+1}(TID_i) - f\left(TID_i, K^F_{j+1}\right)}{r_{j+1}(TID_i)} \tag{3}$$

After obtaining K^B_{m-j}, V_i calculates whether $H^l\left(K^B_{m-j-l}\right) = K^B_{m-j}$ is formed. If it is established, V_i will calculate a new group key according to formula (1).

4 Cooperative Certification

In the basic solution, even if only legal vehicles are added to the domain, and there is no invalid signature at the time of batch verification, the scheme can only verify at most 274 messages per second, and still cannot meet the certification speed requirement. Because of this, we must design new solutions to solve this problem. According to the work of Zhang et al. [8] and Hao et al. [9], the efficiency of certification can be

improved by using cooperative authentication. By cooperating with neighboring vehicles, their solution can ensure that the vehicle knows the reliability of the received message without having to verify each message signature. Selecting a co-certifier requires the following requirements:

(1) The physical location of a cooperating verifier must precede V_i while the other must be after V_i. This means that the selected cooperating verifiers are preferably paired and can broadcast the authentication results to other users;
(2) Co-verifiers need to be far enough apart from each other;
(3) The number of co-verifiers should be moderate.

Assume that each security-related message contains the sender's location information. When the vehicle V_i receives a message sent from a different message sender at the same time, it first extracts the location information of the message sender, and then executes a selection procedure of the cooperation certifier that satisfies the above requirements to determine who will be selected as the cooperative certifier.

V_i checks the received message every 300 ms and calculates the distance between the sender of the message and itself based on the location information. Then, create a table as shown in Table 3.2, where the message ID is a random sequential index, the direction is whether the sender of the message before or after the recipient, and the distance is the distance between the receiver and the sender.

Assuming that the vehicles are evenly distributed, as shown in Fig. 3.6, the communication range is divided every 60 m according to the basic needs selected by the collaborators and the number of authenticated messages. We define vehicles from the sender (50 ± 5) m, (110 ± 5) m, (170 ± 5) m, (230 ± 5) m and (290 ± 5) m away. As shown in Fig. 3.6, V_i simultaneously receives 10 messages sent from senders 1 through 10, and then calculates its distance from each sender to obtain Table 3.2. Thus V_i should add messages 1, 2, 3 to the bulk verification. Because the cooperation program can reduce the number of messages verified, thus increasing the speed of authentication. Performance analysis indicates that the cooperative certification can meet the demand for the number of messages authenticated per second in the on-board ad hoc network.

5 Safety Analysis

Considering the problem that the roadside unit is captured, in the process of mutual authentication and group key generation, V_i can obtain the service without revealing its identity to the roadside unit. Therefore, even in the presence of some roadside units being captured, the proposed protocol can still protect the identity of the vehicle. Resist the obituary: If a vehicle is investigated, the TMC will begin an audit process and ask some roadside units for information about the vehicle being surveyed. However, RSUs may be captured to protect the vehicle being investigated by the information of the TA-some other vehicles, and this behavior is called obituary. In the delivery we will show that the proposed solution can resist such attacks.

In the designed protocol, each message sent by the vehicle V_i is signed by its private key SK_{V_i}, and the group private key and V_i are bound together. Since R_x does not have SK_{V_i}, it cannot forge the signature of the legal V_i. More importantly, the group

private key and the private key are bound together, which adds to the falsification difficulty of R_x. We also store mutual authentication information in Figs. 2 and 3. When the dispute occurs, the TA can ask the vehicle and the roadside unit to present the information.

The non-repudiation of the vehicle's group private key: once R_x has distributed the group private key to V_i, it cannot be denied. In the message messages, the roadside unitization sends a hash value $GSK_{D_A V_i}$, and the signature of the group private key. After V_i receives the message message 5 and obtains $GSK_{D_A V_i}$, it can verify the validity of $GPR_{D_A V_i}$ by hash value. In order to ensure that the group private key is generated by x_i, V_i stores the signature status sent by R_x $Sig_{SK_{R_x}}(H(GSK_{D_A V_i}), x_i, x_i$ At the same time, R_x also stores x_i and $H(V_i||x_i)$. When an argument occurs, R_x can present this information to the TA. Since the public parameters of the group signature are generated by the TA, it can calculate the group of V_i. The private key. The TA can obtain the identity of V_i according to PK_{V_i}, so that $H(V_i||x_i)$ can be verified. If $H(V_i||x_i)$ passes the legality verification, the group private key is $GSK_{D_A V_i}$ is valid, otherwise, $GSK_{D_A V_i}$ is invalid. For V_i, V_i sends x_i to TMC, then TMC can calculate the group private key $GSK_{D_A V_i}$ of V_i. If $GSK_{D_A V_i}$ is correct, the TMC verifies the signature to ensure that it is generated.

Preventing the collusion of the vehicles: A captured roadside unit may collude with a malicious vehicle and send the group private key of the other vehicle to its colluder. The malicious vehicle can then broadcast a message to represent the behavior of the other vehicle. In order to prevent such attacks, in the designed protocol, the signature of the message contains the identity information. At the same time, R_x and V_i also store this information after completing mutual authentication with each other. In the event of an argument, V_i can send its stored information to the TMC. By calculating the group key $GSK_{D_A V_i}$ and verifying the signature $Sig_{SK_{R_x}}(H(GSK_{D_A V_i}), x_i$, TMC can confirm The owner of $GSK_{D_A V_i}$.

6 Conclusion

In this paper, a group signature-based vehicle information sharing scheme for vehicular ad hoc networks with effective privacy protection is proposed. The design goals are achieved by technologies such as distributed management, HMAC, batch signature verification and cooperative authentication. First, divide the entire network into different domains for local management. Second, HMAC is used instead of time-consuming revocation list checking, and the integrity of messages prior to bulk authentication is ensured to avoid the number of invalid messages in bulk verification. Finally, we also use the cooperative certification method to further improve the efficiency of the program. By adopting the above technology, our proposed solution can meet the verification requirements. Security and performance analysis shows that our proposed solution enables efficient group signature-based authentication while maintaining conditional privacy.

Acknowledgment. The work of this paper were supported in part by East China Jiaotong university research fund under Grant No. 14RJ02 and Jiangxi provincial department of science and technology research found under Grant No. 20122BAB201040.

References

1. Author, F.: Article title. Journal **2**(5), 99–110 (2016). Zhang, C., Lu, R., Lin, X., et al: An efficient identity-based batch verification scheme for vehicular sensor networks. In: Proceedings of the 27th IEEE Conference on Computer Communications, INFOCOM 2008, pp. 246–250 (2008)
2. Sun, Y., Lu, R., Lin, X., et al.: An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans. Veh. Technol. **59**(7), 3589–3603 (2010)
3. Zhang, L., Wu, Q., Solanas, A., et al.: A scalable robust authentication protocol for secure vehicular communications. IEEE Trans. Veh. Technol. **59**(4), 1606–1617 (2010)
4. Mershad, K., Artail, H.: A framework for secure and efficient data acquisition in vehicular Ad Hoc networks. IEEE Trans. Veh. Technol. **62**(2), 535–551 (2013)
5. Wasef, A., Shen, X.: Expedite message authentication protocol for vehicular Ad Hoc networks. IEEE Trans. Mob. Comput. **12**(1), 78–89 (2013)
6. Jiang, S., Zhu, X., Wang, L.: A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks. In: Proceedings of 2013 IEEE International Conference on Wireless Communications and Networking, WCNC 2013, pp. 2375–2380 (2013)
7. Wasef, A., Shen, X.: Efficient group signature scheme supporting batch verification for securing vehicular networks. In: 2010 IEEE International Conference on Communications, ICC 2010, pp. 1–5 (2010)
8. Zhang, C., Sun, X.R., Lu, P.-H.H., et al.: An efficient message authentication scheme for vehicular communications. IEEE Trans. Veh. Technol. **57**(6), 3357–3368 (2008)
9. Hao, Y., Chen, Y., Zhou, C., et al.: A distributed key management framework with cooperative message authentication in VANETs. IEEE J. Sel. Areas Commun. **29**(3), 616–629 (2011)
10. Zhu, X., Jiang, S., Wang, L., et al.: Privacy-preserving authentication based on group signature for VANETs. In: Proceedings of the 2013 IEEE Global Communications Conference, GLOBE-COM 2013, pp. 4609–4614 (2013)
11. Hao, Y., Cheng, Y., Ren, K.: Distributed key management with protection against RSU compromise in group signature based VANETs. In: Proceedings of IEEE GLOBECOM 2008, pp. 1–5 (2008)
12. Dutta, R., Mukhopadhyay, S., Collie, R.M.: Computationally secure self-healing key distribution with revocation in wireless ad hoc networks. Ad Hoc Netw. **8**(6), 597–613 (2010)
13. Schnorr, C.: Efficient signature generation by smart cards. J. Cryptol. **4**(3), 161–174 (1991)