Journal of

Software Engineering

ISSN 1819-4311

Academic
Journals Inc.

www.academicjournals.com

OPEN ACCESS Journal of Software Engineering

ISSN 1819-4311
DOI: 10.3923/jse.2017.134.142

Review Article
An Anonymity Authentication Scheme Based on Forward Security in VANETs

[1,2]Wang Xiaoliang, [1]Zhao Shujing and [1]Li Shuifan

[1]School of Computer Science and Engineering, Hunan University of Science and Technology, 411201 Xiangtan, China
[2]Department of Computer Science, University of Alabama, 35487 Tuscaloosa, United State of America

Abstract
Vehicular *ad hoc* networks (VANETs) are created for data exchange of intelligent transportation systems (ITS), which have recently attracted great attentions. In an open environment the privacy of the vehicle faces serious threats, so some vehicles do not like to publish their identities. But due to security consideration, a vehicle only wants to exchange information with verifiable partners, which needs identities authentication. There is a contradiction in VANETs. Aiming at this dilemma, an effective solution of the anonymity authentication scheme is proposed in this study. It uses ring signature technology to ensure anonymous authentication and forward security technology to reduce key compromise hazard. Performance evaluation shows this scheme can provide secure information exchange among vehicles and enhance the application of VANETs.

Key words: VANETs, privacy, anonymity, authentication, track, forward security

Received: July 20, 2016 Accepted: October 05, 2016 Published: March 15, 2017

Citation: Wang Xiaoliang, Zhao Shujing and Li Shuifan, 2017. An anonymity authentication scheme based on forward security in VANETs. J. Software Eng., 11: 134-142.

Corresponding Author: Wang Xiaoliang, School of Computer Science and Engineering, Hunan University of Science and Technology, 411201 Xiangtan, China

Copyright: © 2017 Wang Xiaoliang *et al.* This is an open access article distributed under the terms of the creative commons attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

With the rapid development of information technology, the vehicular *ad hoc* networks (VANETs) become popular. However, VANETs also face a large amount of challenges. One of the most challenge in this field is the contradiction between security and privacy[1]. That is to say, at the most situation, VANETs must have security schemes that ensure that the identities of vehicles can be verified. In addition, the driver's privacy is also important in the VANETs. So in VANETs, system need not only ensure the information authentication, but also prevent the attackers from affecting the driver's privacy.

Current researches like to use the pseudonym or group signature to solve these problems. However, creating a pseudonym needs a large amount of computation and storage overhead in the pseudonym generation stage. Although a group signature can lighten the burden and increase the difficulty of counterfeiting, the group managers is easy to be compromised, which leads to all the group keys leaked quickly. At the same time, the cost of group signature is relatively large, because any member joining and leaving will lead to the group keys redistribution[2]. In contrast, the ring signature can guarantee the anonymity and reduce the overhead. Although the ring signature applied in VANET can guarantee the anonymity of the information communication, it cannot guarantee conditional anonymity. Conditional anonymity means that legal vehicles can use anonymity to protect privacy but the misuse vehicles will be tracked. So far, using ring signature in VANET is common, but there is no scheme considering the conditional tracking ability. Another issue is that the key leakage will make all the previous ring signatures invalid, which destroys all the previous work and is not suitable for real applications.

In this study, an authentication scheme based on forward security in VANETs is proposed. The use of the VANET traceable ring signature provides authentication for preventing the information from forging and guarantees the effective transmission of the anonymous information, but also can track the user who misused anonymity. In addition, this scheme can guarantee previous signatures valid and neighboring vehicles can still determine normal route according to the previous precaution information even if the key of signature is compromised.

AUTHENTICATED SCHEMES IN LITERATURE

In recent years, some authentication schemes are proposed in the literatures. Common techniques used in studies include group signature scheme[3-5], ring signature scheme[6], ID-based signature scheme[7-11], blind signature[12], pseudonym[13-15] or mess-up technology[16-19].

Sun *et al.*[3] and Guo *et al.*[4] early use Boneh group signature technology for in-vehicle communications. Calandriello *et al.*[5] point out that the computational overhead and length of the group signature in the signature generation and verification process are much larger than the general PKI digital signature schemes (such as ECDSA), so schemes using the kind of signature for in-vehicle safety are inefficient. Following researchers want to improve the high overhead and security risks of the group signature. Among them, some researchers resort to use ring signature scheme to achieve the desired objectives. Ring signature is similar to a simplified group signature scheme and it uses rules to form a ring, which has anonymity feature. For example, Zhang *et al.*[6] proposed a privacy-preserving authentication protocol based on ring signature without bilinear pairings in VANETs. It achieves effective privacy protection and authentication mechanisms and also reduces the computational overhead of signature generation process because of discarding the complex operation of bilinear pairings. There are some researchers who focus on using the Identity Based Signature (IBS) to implement identity-based anonymous authentication such as Sun *et al.*[7], ACPN[8], Jinila and Komathy[9], PPAS[10] and He *et al.*[11]. Among these international researchers, Sun *et al.*[7] are relatively early researchers who pay attention to this problem. They use zero-knowledge proof and threshold secret sharing algorithm to design an anonymous identity authentication scheme based on signatures. The PPAS[10] uses identity based signature based on bilinear pairings to solve anonymous authentication issues not only between OBUs but also between the RSUs and OBUs. In addition, in order to achieve conditional privacy and authentication purposes. He *et al.*[11] designed a similar identity-based signature. But because it is based on elliptic curve algorithm without bilinear pairings operation, it has less computational overhead and more safe. PBSS[12] proposed a signature scheme based on blind signature and proxy multi-signature certification technology, which solves authentication problems between the nodes. The use of two signature technologies realizes the on-board authentication interactivity and improved communication safety. Experimental result shows PBSS can better meet the on-board node mobility and complexity and the authentication efficiency has good performance.

Typical pseudonym schemes are studied[13-15]. In literature[13], a certain department of motor vehicles (DMV) node distributes several pseudonyms for each vehicle, which

can be used to hide real identity. But all pseudonyms are in the charge of the DMV node, which needs a large amount of storage space. In literature[14], researchers propose a scheme based on public key infrastructure PKI. Pseudonym is produced at vehicle terminals. Each car has two identities, named as temporary ID and permanent ID. When system deals with CRL (Revocation list certificate), RSU and OBU will work together to make this process more rapid. Although, the processing speed is accelerated, but also payment is large because this proposal heavily relies on of a serious dependence tamper-resistant device (TRD). Literature[15] presents the design of a pseudonym-supporting framework that considers the following issues: Multi-layer pseudonym addressing, adapting routing to work with changing pseudonyms to avoid packet loss, anonymity abuse, reusing pseudonyms without creating addressing conflicts or jeopardizing privacy, non-repudiation and accountability against collusion attacks involving RSUs and vehicles.

Other VANET anonymous authentication schemes use different kinds of obfuscation techniques. The VSPN[16] uses bilinear mappings and proxy re-encryption mechanism to design a credential authentication for automotive networks. Van den Berg *et al.*[17] proposed a vehicle-based certificate-selection method for enhancing the privacy in VANETs, in which vehicles share numbers of certificates. Each vehicle is able to detect and identify the certificates used by neighbors, then it can choose a used certificate for its own safety communication. This method makes the certificate not unique to achieve anonymous authentication enhancing privacy. In addition, k-anonymity is also used in this field. The k-anonymity means unless there are k-1 data that are released at the same time the k-user can be disclosed. Chen *et al.*[18] proposed a query-aware location privacy scheme based on p-sensitive and k-anonymity for road networks, which puts all the k users as an anonymous entity in a certain area and authority uses the optimized queries to determine a specific entity.

However, all the schemes do not regard the issue of key leakage and are not able to restrain the damage after the signature key is compromised.

OVERVIEW OF FORWARD SECURITY

In encryption system, regardless of what time key leakage happens, it will make the total system collapse. This is incompatible with many practical applications, which need preventing the compromise of a long-term secret key from affecting the confidentiality of past conversations[20,21]. Therefore, the forward security of the digital signature was proposed by Anderson[22]. It means all the signatures are correct and effective if signing time is priority to the time of the digit key being destroyed. That is to say, the availability of signature will not be affected because the signature of a certain moment is destroyed.

In this scheme, a special forward secure signature scheme is proposed for VANET. This scheme adds key update algorithm to common ring signature, which ensures system can use unique public key and private key in each period to sign so as to avoid the problems caused by key exposure. Of course, due to the unique nature of this algorithm, system will check the time stamp correctness when signature is verified. Figure 1 shows the evolution process of the signature key. With the help of evolution function h, the period key is keeping evolving. The SK_i is the private key for signature in a certain period.

MODEL FRAME

The model is given in Fig. 2. The scheme sends time information by GPS system. When the GPS has sent time information to OBU time via the RSU, the scheme uses this time as a landmark for signature and ensures real-time and communication anonymity.

The following Table 1 describes the meaning of the symbol in the communication process.

FORWARD SECURITY AUTHENTICATION SCHEME

In this scheme, system put the vehicle travel time into the T time periods and every time period is also the valid period of a public key. This can ensue different key is used during

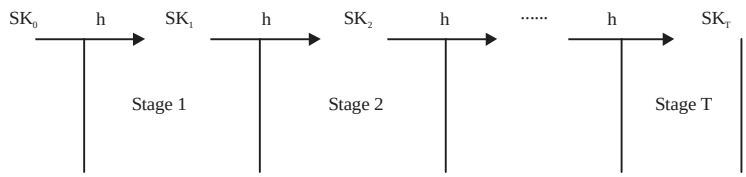

Fig. 1: Key evolution process

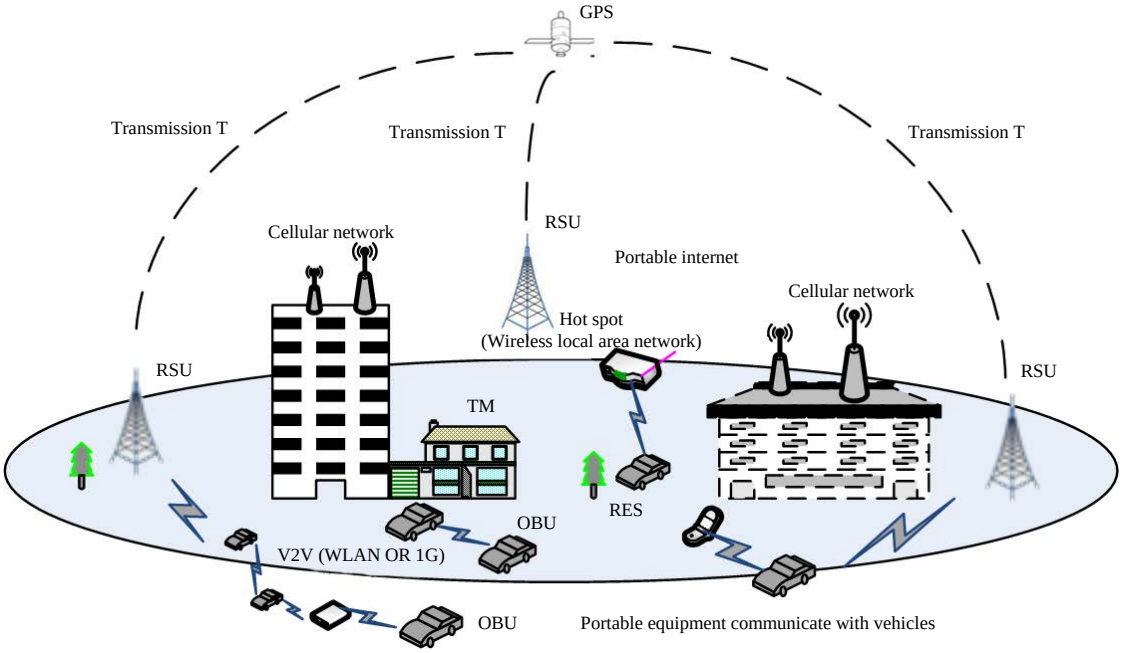

Fig. 2: VANET system structure diagram

Table 1: Symbolic variable list

Notations	Descriptions
*G	*A finite field of order n, where n is a prime number
*g	*The generator of G
*H()	*A hash function of $\{0, 1\}^* \rightarrow \{0, 1\}^\beta$
*H′()	*A hash function of $\{0, 1\}^* \rightarrow \{0, 1\}^\beta$
*H″()	*A hash function of $\{0, 1\}^* \rightarrow \{0, 1\}^\rho$
*V_i	*A vehicle (ring member)
*TM	*The traffic management department
*(Sk_i, 0, PK_i)	*The pairs of keys of V_i: Public key PK_i and private key SK_i
*ID	*License plate
*Flag = (ID, PK_N)	*Signature tag
*T	*Valid time of driving
*$S_{i,j}$	*The private key of V_i during time j

different period, which strengthens the security of the communication. At the same time, the addition of time can ensure the data that vehicles collect are real-time, which can effectively prevent key compromise. This also ensures that the transmitted information is valid, so the near vehicles can predict the next route based on above information. In this process, the public key remains constant, the private key is formed by a one-way evolution of the previous one in order to ensure the signature can not be forged. The advantage of this scheme is as follows. Firstly, the evolution information is added in the process of key generation ensuring the absolute anonymous and user information unforged; secondly, at the low cost, scheme not only ensures the anonymity but also realizes the vehicle tracking functionality. In addition, if it is removed out the entire network environment is not affected and there is also no additional overhead.

We denote all the vehicles in a region as a set N, (1,2,...,n), $n \in N$. All the vehicles are managed by TM. In order to save the storage and computation overhead, each terminal vehicle generates its key rather than uniformly allocated by TM. Public key set is defined as $PK_N = (PK_1,...,PK_n)$, which is composed of the public key each vehicle. Before a vehicle runs on the road, TM will issue a license, called ID, which is unique. Scheme will store the vehicle identification information for the later tracking once illegal behavior happens. In the scheme, system updates the private key by time parameter to ensure the real-time information and communication is effective before key compromise. This key update process can guarantee the forward security of system. Assume the effective travel time of the vehicle is denoted as T, the initial time is set as 0.

System initialization phase: Traffic management department (TM) calculates parameters (n, G, g) representing the region unique information through a probabilistic algorithm for each region (i.e., a vehicle management domain). All these parameters and H(), H′(), H″() are embedded in OBU sensors of vehicles. Each vehicle is described as Vi, $i \in (1,...,n)$. The TM generates two security parameters k_i, l_i for each vehicle and then distributed them to each vehicle. Each vehicle randomly chooses two distinct large prime numbers p_i, q_i through the algorithm to produce their own key pair to meet $p_i \equiv q_i \equiv 3 \bmod 4$, $2^{ki-1} \leq (p_i-1)(q_i-1)$ and $p_i q_i \leq 2^{ki}$. At the same time, TM randomly chooses $S_{i,0} \in G^*_{Ni}$ as the initial value of private key. By the initial value scheme can

calculate $u_i = 1/S_{i,0}^{2^{l_i}(T+1)}$ mod N_i and get the segment of the public key of vehicles u_i. The public key of vehicle can be described as PK_i (N_i, u_i, T) and the private key can be described as SK_i (N_i, T, 0, $S_{i,0}$), so the (SK_i, 0, PK_i) denote public/private key pairs of vehicle.

TM backups vehicle information: The vehicles will register at TM before running. If it is used vehicle, it needs a transfer procedure supervised by TM. Before register, scheme will firstly check the database to ensure the vehicle is valid. Once the vehicle is confirmed legitimate, the traffic management department uses corresponding public key $N_i = p_iq_i$ stored at TM and the unique parameter g of this region to get the private key d by RSA encryption algorithm gd = 1(mod $(p_i-1)(q_i-1)$) and then use the d to sign this information. After TM received the signature, it verifies again to ensure whether transfer is lawful. if lawful, the vehicle information, corresponding license number of and public key will be stored in a database. This means that when the vehicle is illegal it is easy to find the corresponding identity.

Key update: In order to ensure the validity of the signature will not be affected even if the key is compromised, according to the principle of forward security, the scheme uses time factor to control dynamic change of the key. If the private key of the vehicle V_i in j-1 time interval is $SK_{i,j-1}$ (N_i, T, j-1, $S_{i,j-1}$), $j \leq T$, then for each vehicle in the time interval j its private key is determined by its previous time period j-1, namely $S_{i,j} = S_{i,j-1}^{2^{l_i}}$ mod N_i, so the private key of the vehicle V_i in j time interval is $SK_{i,j}$ (N_i, T, j, $S_{i,j}$) (Fig. 3, 4).

Signature: Suppose the signer vehicle in the region is V_i. The V_i asks TM and get all the security parameters (k_1, l_1,...,k_n, l_n) as inputs. It records the time of signature as j, signed message as m including vehicle speed, direction and other related information. Public key set of signature ring is $PK_N = (PK_1,...,PK_n)$. Signature label is Flag = (ID, PK_N) (the Flag is abbreviated as F) and the signer's private key $SK_{i,j}$. Assume ρ is twice as long as the maximum bit length among N_i, β is the smallest bit length among N_i, hash function is H: $\{0,1\}^* \rightarrow \{0,1\}^\beta$, H': $\{0,1\}^* \rightarrow \{0,1\}^\beta$, H'': $\{0,1\}^* \rightarrow \{0,1\}^\rho$, so the signature process is as follows:

- Calculate h = H(F)(mod|N|), $\sigma_{i,j} = S^{-h}_{i,j}$ mod N_i
- Let $A_{i,0} = H'(F||m||i)$, $A_i = \sigma_{i,j}^{A_{i,0}^{-1}}$
- For each k = I, calculate $A_{k,0} = H'(F||m||k)$, $\sigma_{k,j} = A_1^{Ak,0}$ mod N_k

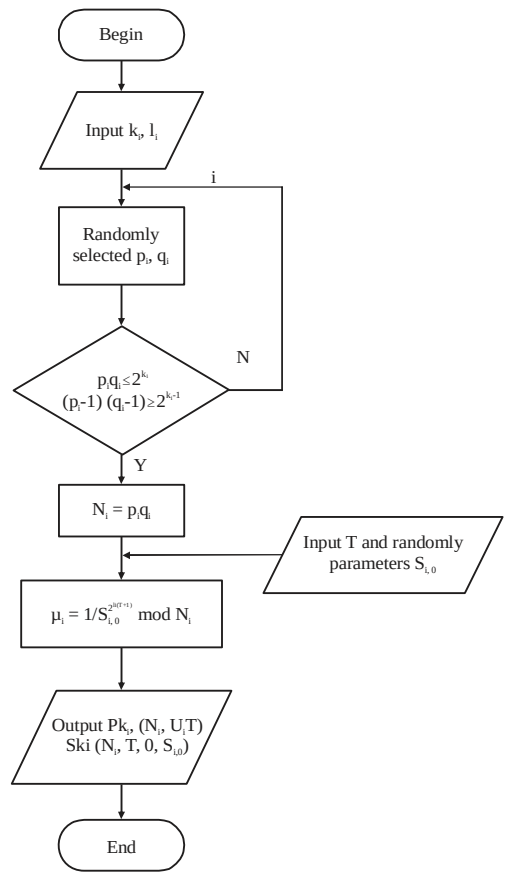

Fig. 3: Key generation

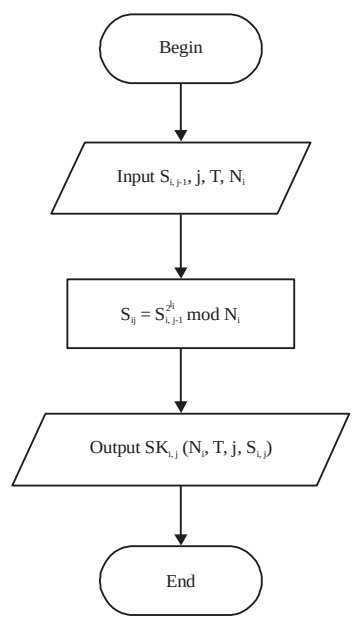

Fig. 4: Key update

- Except real signed vehicle V_i, the other vehicles V_K, $k \neq i$, selects $Z_k \in Z_{N_k}$, $c_k \in \{0, 1\}^{l_i}$ as random parameters,

calculates $y_k = z_k^{2^{li}(T+1-j)}$ u_k^{ck} mod N_k, $\lambda_i \equiv z_k^h \sigma^{ck}_{k,j}$ mod N_k, for real signed vehicle V_i, randomly selects $r_i \in Z_{N_i}$ and calculates $y_i \equiv r_i^{2^{li}(T+1-j)}$ mod N_i, $\lambda_i \equiv z_i^h$ mod N_i, Let $A_N = (A_{1,0},...,A_{n,0})$, $y_N = (y_1,...,y_n)$, $\lambda_N = (\lambda_1,...,\lambda_n)$, calculate $c = H''(F||m||A_N||y_N||\lambda_N)$

- Calculate:

$$c_i = c - \sum_{k \neq i} c_k, z_i = r_i S_{i,j}^{c_i} \bmod N_i$$

- Let $c_N = (c_1,...,c_n)$, $z_N = (z_1,...,z_n)$ the ring signature of output is $\sigma = (F,m,A_N,c_N,z_N,j)$

Authentication between vehicles: Verify whether the vehicle belongs to the region and whether the information transmitted by the vehicle is tampered with:

- Calculate h = H(F)(mod|N|)
- For each vehicle V_i, calculate $A_{i,0} = H'(F||m||I)$, $\sigma_{i,j} = A_1^{A_{i,0}}$ mod N_i
- Verify whether $H''(F, m, A_N, y_N, \lambda_N) = \sum_{i \in N} c_i$ if successful, output 1 to indicate that the signature is valid, otherwise output 0

TM track and revoke vehicles: Check the relationships between the two message/signature pairs (m,σ), (m′,σ′) of label F to find the misbehaved vehicle. Firstly, scheme needs to assume an empty list TL and set a time period j, then verifies the following steps:

- Set $\sigma = (F, m, A_N, C_N, z_N, J)$, $\sigma' = (F, m', A_N', C_N', Z_N', j)$, calculate $A_{i,0} = H'(F||m||I)$, $\sigma_{i,j} = A_1^{A_{i,0}}$ mod N_i and $\sigma_{i,j}' = A_1'^{A'_{i,0}}$ mod N_i
- For each vehicle V_i, if $\sigma_{i,j} = \sigma'_{i,j}$, record PK_i into TL
- If one item in TL, output PK of this item. If all the public display in TL is in ring, output "Linked", otherwise output "Independent".

$$\text{Trace}(F, m, \sigma, m', \sigma') = \begin{cases} \text{independent; if signers are different} \\ \text{linked; if } m = m', \text{signers are same} \\ PK_i\text{; if } m \neq m', \text{ signers are same} \end{cases}$$

If these signers are different, output "Independent",
If m = m′ and the same signer, output "Linked",
If m ≠ m′ and the same signer, output corresponding public key PK of signer.

For "Linked" output, according to signature and related records TM lookups information in its own database to find the true identity of the vehicle of the signature (Fig. 5).

PROOFS AND SECURITY ANALYSIS

Theorem 1: The feasibility of the forward security of this scheme.

Proof: Assume an imitator A wants to emulate a signature of the vehicle V_i at the time j under the label Flag = (ID, PK_N). In this imitation stage, the imitator visit H″ q_H times, visit RSU in the region q_s times and totally visit H, H′′ q_H times. A polynomial algorithm T of N is needed to generate, which is created in initialization phase of a time decomposition system.

The algorithm T wants to get the square root ε of ω by random selection $x \in Z_N^*$ and calculating $\omega = x^2$ mod N as well as the result of multiple access of imitator. Because the random selection of the square root of x has four values, so the probability of $x \neq \pm\varepsilon$ is only 1/2. So T splits N by computing (x-ε, N).

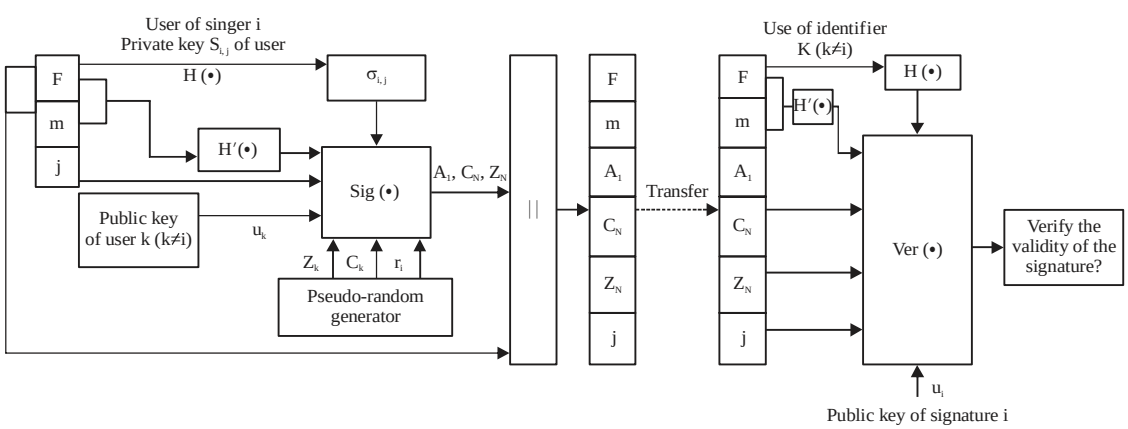

Fig. 5: Forward security tracking scheme

We assume the starting traveling time of imitator is τ and the signature can be got from RSU stored in the region.

Imitator A randomly selects τ<T. Algorithm T guesses the time point when imitator starts to enter the region. By random selection of $1 \le t \le T$, the traveling time is assumed to be $\tau \ge t$, which means before this time forgery has been successful. The algorithm T randomly chooses a terminal $\delta \in_R \{1,2,...,n\}$ and calculates influence factor of its public key $u_\delta = 1/\omega^{2^{l\delta(T+1-t)}}$ and uses $N_\delta = N$ to ensure that the public key (N_δ, u_δ, T) belongs to a certain terminal vehicle in the region. Such the T can provide all public keys to the imitator.

If $\tau \ge t$ is successful, imitators can successfully emulate ring signature $\sigma = (F, m, A_N, c_N, z_N, j)$ in the period of j<t. with the help of the algorithm T, imitator can emulate a ring signature $\sigma' = (F, m', A_N', c_N', z_N', j)$ with a certain probability. According to $y_\delta \equiv z_\delta^{2l\delta(T+1-j)}$ and $y_\delta \equiv y'_\delta$ it can get:

$$z_\delta^{2l\delta(T+1-j)} u_\delta^{C_\delta} \equiv z'^{2l\delta(T+1-j)}_\delta u_\delta^{C'_\delta} \pmod{N_\delta} \Rightarrow$$
$$(\omega^{-2^{l\delta(T+1-j)}})^{C_\delta - C'_\delta} \equiv (\frac{z'_\delta}{z_\delta})^{2^{l\delta(T+1-j)}} \pmod{N_\delta} \Rightarrow$$
$$\omega^{C_\delta - C'_\delta} \equiv (\frac{z'_\delta}{z_\delta})^{2^{l\delta(t-j)}} \pmod{N_\delta}$$

According to the lemma A.1 of literary[23], $\alpha = c_\delta - c'_\delta$, $X = z'_\delta / z_\delta$, $\gamma = l_\delta (t-j)$ and the square root of ω can be calculated with the assistance of the algorithm T.

Theorem 2: Beside from having the anonymity and traceability, this program also has non-forge ability.

Proof for anonymity: A terminal vehicle i in period j randomly chooses c_k, z_k ($k \neq l$) and generate a valid signature $\sigma = (F, m, A_N, c_N, z_N, j)$ for message m. For the message m of label Flag = (ID, PK_N), the possible values of $z_N = (z_1, ..., z_N)$ are $\prod_{i=1}^{n} N_i$ options. Since, these values are independently even distributed, only the signer can know who is this signer. That is to say, others can not know who is the true signer. So this scheme is anonymous.

Proof for traceability: Let |TL| denotes the number of elements of TL, according to the tracking algorithm, $A_{i,0} = H'(F||m||i)$ and $\sigma_{i,j}' = A_1'^{A'_{i,0}}$ mod N_i can be found. Because H' is random, so to a certain label, the maximum number of messages is $2^{-\beta}$. For any imitator, even after q_H times queries, the most probability of |TL|>1 is $q_{H'}/2^{-\beta}$. So this scheme satisfies the traceability.

Proof for non-forge ability: According to theorem 1, proof by contradiction is adopt and the scheme is assumed to be forged, that is to say imitator can arbitrarily fakes signature, then the square root of ω will be calculated, which is contrary to reality. So the scheme can also satisfy the un-forgery.

PERFORMANCE EVALUATION

To verify the effectiveness of the proposed scheme, simulation experiment is carried out. Experiment uses C++ language and is based on visual studio 2012 platform of Windows 7 system with 2.6 GHZ i5 processor and 4G memory. The experimental data set is generated using Thomas Brinkhoff road network[24] widely recognized by the mobile data management industry. Oldenburg traffic network (5×5 km) is taken as the input to generate mobile data set and communication node objects (Fig. 6).

According to the definition of data packet format of security standard IEEE[25] 1609.2 for VANET, the definition of pseudonym message format is as given in Table 2.

Performance analysis: Table 3 compares the algorithm, called PBSS[26] in anonymity, authentication and traceability fields. PBSS adopts the distributed proxy blind signature, which can avoid forgery attacks and meet authentication security, but never consider tracking of the abuse of anonymous and the impact of key leakage.

Communication and storage overhead: The scheme PBSS[12] needs three phases: the signature authorization, proxy signature and signature verification phase. Each message in the signature process need carry pseudonym certificate. Compared with PBSS, the number of interactive of the

Table 2: Message format for vehicle

Parameters	Default value
MID	2B
MData	100B
TS	4B
Sign	136B
CertPV	698B
TTL	1B

Table 3: Schemes features comparison

Attributes	PBSS	Our scheme
Integrity	Yes	Yes
Authentication	Yes	Yes
Anonymity	Yes	Yes
Privacy protection	No	Yes
Conditional tracking	No	Yes
Resist key leakage	No	Yes

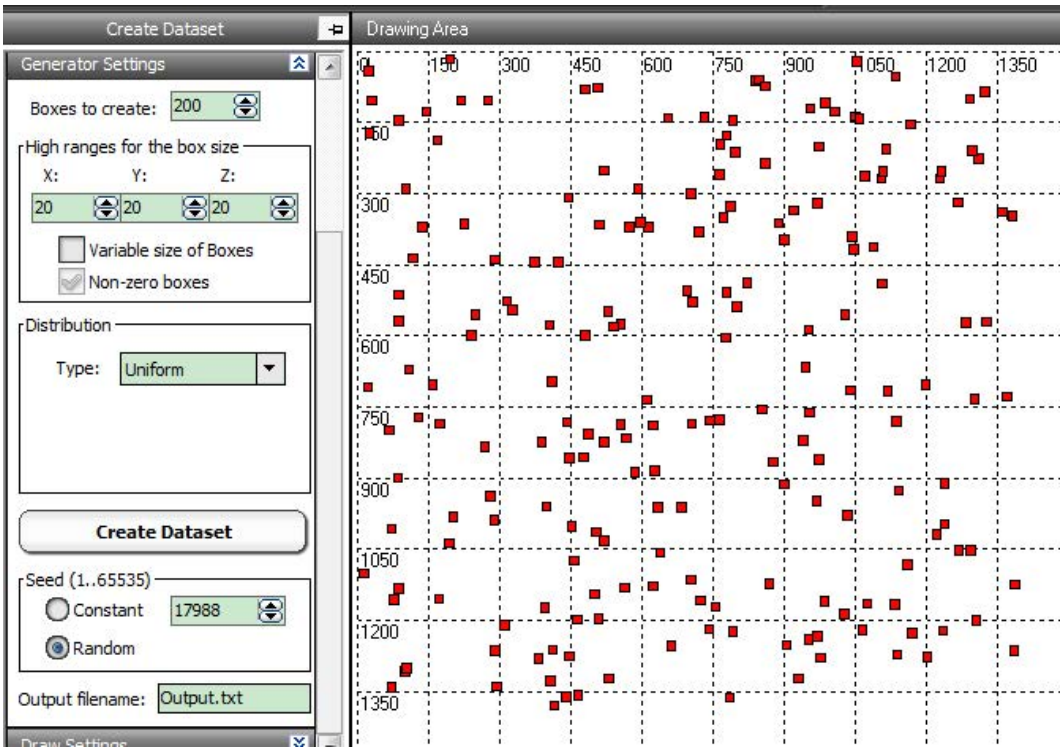

Fig. 6: Communication nodes

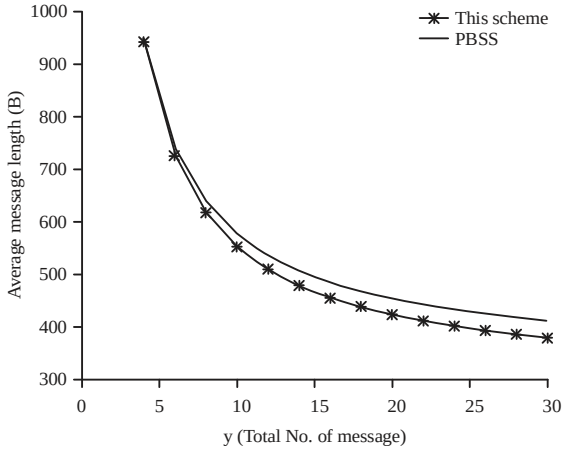

Fig. 7: Average length of the message with number changed

pseudonym issue phase is reduced to two-cycle. At the same time, it is unnecessary that all the information carry pseudonym certificate in the signature process. In this experiment, we set the number of message in a communication cycle is 400. Define the average length of the message is:

$$\text{Len} = \frac{z\times 941+(y-z)}{y}$$

when z = 4, guaranteeing the success rate $P_{auth} \geq 90\%$, the relationship between the average message size and the total number of messages in a cycle is as given in Fig. 7.

CONCLUSION

In this study, a novel anonymity authentication framework with forward security for VANETs has been proposed, which utilizes the addition of time parameter to restrain the leakage of key. The ability of forward secrecy makes the key leakage at a certain time do not harm the security of communication, which considerably improves the practicability of VANETs. In addition, the key update module is added to system to enhance the anonymity of communication. Finally, the feasibility of the scheme is verified by security analysis and experimental results.

ACKNOWLEDGMENTS

The Internet innovation and open platform base of Ministry of education of China [KJRP1401]. The US-China Computer Science Research Centre of Nanjing University of Information Science and Technology [KJR16059], Hunan University of Science and Technology [E51372, G31410] and the China Scholarship Council [201409480003].

REFERENCES

1. Babar, S., P. Mahalle, A. Stango, N. Prasad and R. Prasad, 2010. Proposed security model and threat taxonomy for the Internet of Things (IoT). Proceedings of the 3rd International Conference on Network Security and Applications, July 23-25, 2010, Chennai, India, pp: 420-429.
2. Libert, B., T. Peters and M. Yung, 2012. Scalable group signatures with revocation. Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, April 15-19, 2012, Cambridge, UK., pp: 609-627.
3. Sun, X., X. Lin and P.H. Ho, 2007. Secure vehicular communications based on group signature and ID-based signature scheme. Proceedings of the IEEE International Conference on Communications, June 24-28, 2007, Glasgow, Scotland, pp: 1539-1545.
4. Guo, J., J.P. Baugh and S. Wang, 2007. A group signature based secure and privacy-preserving vehicular communication framework. Proceedings of the Mobile Networking for Vehicular Environments (MOVE) Workshop in Conjunction with IEEE INFOCOM, May 2007, Anchorage, Alaska, pp: 103-108.
5. Calandriello, G., P. Papadimitratos, J.P. Hubaux and A. Lioy, 2007. Efficient and robust pseudonymous authentication in VANET. Proceedings of the 4th ACM International Workshop on Vehicular ad Hoc Networks, September 9-14, 2007, Canada, pp: 19-28.
6. Zhang, J., Y. Cui and M. Xu, 2012. A novel and efficient privacy-preserving authentication protocol in VANETs. Int. J. Digital Content Technol. Applic., 6: 157-164.
7. Sun, J., C. Zhang, Y. Zhang and Y. Fang, 2010. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans. Parallel Distributed Syst., 21: 1227-1239.
8. Li, J., H. Lu and M. Guizani, 2015. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans. Parallel Distributed Syst., 26: 938-948.
9. Jinila, Y.B. and K. Komathy, 2014. An efficient authentication scheme for vanet using cha Cheon's ID based signatures. Indian J. Applied Res., 4: 106-109.
10. Zhu, H., T. Liu, G. Wei and H. Li, 2013. PPAS: Privacy protection authentication scheme for VANET. Cluster Comput., 16: 873-886.
11. He, D., S. Zeadally, B. Xu and X. Huang, 2015. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inform. Forensics Secur., 10: 2681-2691.
12. Tian, X. and S. Qiang, 2012. Research of an authentication scheme based on the proxy blind signature scheme for the vehicular Ad-hoc networks. Bull. Sci. Technol., 28: 170-173, (Chinese).
13. Raya, M. and J.P. Hubaux, 2007. Securing vehicular ad hoc networks. J. Comput. Secur., 15: 39-68.
14. Wasef, A. and X. Shen, 2009. MAAC: Message authentication acceleration protocol for vehicular ad hoc networks. Proceedings of the Global Telecommunications Conference, November 30-December 4, 2009, Honolulu, HI.
15. Artail, H. and N. Abbani, 2016. A pseudonym management system to achieve anonymity in vehicular Ad hoc networks. IEEE Trans. Dependable Secure Comput., 13: 106-119.
16. Chim, T.W., S.M. Yiu, L.C.K. Hui and V.O.K. Li, 2014. VSPN: VANET-based secure and privacy-preserving navigation. IEEE Trans. Comput., 63: 510-524.
17. Van den Berg, E., T. Zhang and S. Pietrowicz, 2009. Blend-in: A privacy-enhancing certificate-selection method for vehicular communication. IEEE Trans. Veh. Technol., 58: 5190-5199.
18. Chen, J., H. Xu and L. Zhu, 2012. Query-Aware Location Privacy Model Based on P-Sensitive and K-Anonymity for Road Networks. In: Internet of Things, Wang, Y. and X. Zhang (Eds.). Springer, New York, ISBN: 9783642324277, pp: 157-165.
19. Caballero-Gil, C., J. Molina-Gil, J. Hernandez-Serrano, O. Leon and M. Soriano-Ibanez, 2016. Providing k-anonymity and revocation in ubiquitous VANETs. Ad Hoc Networks, 36: 482-494.
20. Gunther, C.G., 1989. An identity-based key-exchange protocol. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, April 10-13, 1989, Belgium, pp: 29-37.
21. Menezes, A.J., P.C. van Oorschot and S.A. Vanstone, 1997. Handbook of Applied Cryptography. CRC Press, USA.
22. Anderson, R., 1997. The forward security of the digital signature (Invited lecture). Proceedings of the 4th Annual Conference on Computer and Communications Security, April 1997, Zurich, Switzerland pp: 1-4.
23. Michel Abdalla, L.R., 2000. A New Forward-Secure Digital Signature Scheme. In: Advances in Cryptology-ASIACRYPT 2000, Okamoto, T. (Ed.). Springer, Kyoto, Japan, ISBN: 9783540414049, pp: 116-129.
24. Brinkhoff, T., 2002. A framework for generating network-based moving objects. GeoInformatica, 6: 153-180.
25. Intelligent Transportation Systems Committee, 2006. IEEE trial-use standard for wireless access in vehicular environments-security services for applications and management messages. IEEE Vehicular Technology Society Standard 1609, July 2006.
26. Tian, S.Q.X., 2012. Research of a authentication scheme based on the proxy blind signature scheme for the vehicular Ad-hoc networks. Bulletin of Science and Technology No. 10. http://www.kjtb.net/index.php