An effective privacy protection mechanism in VANETs

Peng Yang
yangpeng@catr.cn

China Academy of Information and Communications Technology

Lingli Deng
dllcqupt@sina.com

Chongqing University of Posts and Telecommunications

Abstract. With the development of vehicle communication technologies, vehicular ad hoc networks (VANETs) achieve communication through short distance communication technology. However, the privacy of vehicles and messages are vulnerable attacked by adversary due to the dynamic network topology. To enhance the security of VANETs, a privacy protection mechanism is designed based on secrete sharing. The mechanism allows vehicles to use pseudonym to protect its privacy, and the exchange entropy is as a measure to evaluate the exchange conditions of the pseudonym to avoid the continuous tracking by the attackers; the message security can be protected by secret sharing. The security and performance analysis are carried out to demonstrate that our scheme can reduce the risk of message leakage and better protect the VANETs' privacy.

Keywords: VANETs, vehicle privacy, pseudonym exchange, message security.

1 Introduction

As an important part of intelligent transport system (ITS) [1], vehicular ad hoc networks (VANETs) can achieve emergency vehicle warnings, curve speed warnings, pedestrian crossing warnings to improve driving experience and road traffic safety. In many networks, security is an important issue that needs to be considered [2-4]. Similarly, the security of vehicles and messages also is an important factor for popularization of VANETs.

In order to prevent the information of messages from being lost or tampered during the process of transmission in VANETs, the asymmetric encryption technology is used in traditional privacy protection mechanism[5]. However, its shortcoming is that the key is also easily destroyed in the transmission process. Therefore, even if a vehicle holds a legal key, it still can not get messages through decryption. Besides, since the wireless media has open features in VANETs and the vehicle sub-netwoks are composed of many moving vehicles in self-organized manner, which causes some vehicles to be attacked. These attacks including attacker tracking the vehicles, stealing or tampering with the messages, transmitting fake messages in a forged identity, etc., make a serious threat to the privacy of vehicles.

To ensure the security of VANETs, and improve the utilization rate of message, an effective privacy protection mechanism is proposed in this paper, which uses the pseudonym exchange and secrete sharing. And the main contributions of this article are as follows:

(1) The method is proposed based on pseudonym and pseudonym exchange in this paper, and pseudonym exchange conditions are obtained according to the exchange entropy. So the vehicle privacy disclosure can be reduced.

(2) The leakage probability can be reduced. To prevent the related information is inferred by attackers from the messages and the participated vehicles information, the secret share scheme is adopted in our scheme. Therefore, although attackers obtain some message pieces, they still can not recover the origin message.

(3) The utilization rate of message can be improved in our scheme. Due to the message pieces will are recovered in application provider (AP), and then the complete message can be sent to vehicles by AP.

MOBIMEDIA 2018, June 21-22, Qingdao, People's Republic of China

DOI 10.4108/eai.21-6-2018.2276638

The remainder of this paper is structured as follows: Section II summarizes the related work. Section III presents the system and attack model, security goal. Section IV describes the privacy and security protection methods. The security and performance analysis are provided in Section V and VI, separately. Finally, this paper is summarized in Section VII.

2 Related works

Recently, the security protection of VANETs has been widely researched by both domestic and foreign researchers.

To prevent attackers from stealing vehicle privacy, the update of pseudonym is one of the effective methods to solve the problem that attackers keep tracking vehicles in VANETs. However, the privacy will not be protected if vehicles change pseudonym at inappropriate time or place, because that attackers can easily associate the new pseudonym with the previously used pseudonyms [6-7]. Beresford [8] first proposed the concept of Mix-zone in 2003, referring to the area of changing pseudonym. Buttyán et al. [9] first used the Mix-zone method into vehicle networks in 2007. They divided the road network model into observable and unobservable areas for attackers, and vehicles need to stop sending messages to refresh pseudonym in the unobservable areas. However, those approaches is at the expense of network performance to enhance the flexible of Mix-zone.

In order to protect the security of messages, a message protection method is devised in [10]. However, this scheme only randomly sends fragment messages to adjacent vehicles, and the vehicles reliability can not be ensured. Hence, the message may be discarded by malicious vehicles that will increase the probability of incomplete messages. To improve the decryption efficiency, the paper [11]adopts encryption technology, which part of the ciphertexts are handed over to the road side unites (RSUs) for decryption by the destination vehicle, but it will cause unnecessary communication overhead.

3 System model

The architecture of VANETs consists of trust authority (TA), RSUs, on board units (OBUs) and a AP. Specifically, the TA is responsible for the registration and key generation of network entities in VANETs. The RSUs as the communication relays are deployed on both sides of road or at road intersection. An OBU is a wireless communication device installed in vehicle, and AP can support safety related applications.

In this network, attackers may track the legitimate vehicles according to the information obtained, and send false messages by faking legal vehicles. Besides, As mentioned above, security and privacy protection play a key role in the acceptance and promotion of VANETs. The safety requirements of vehicle anonymity and message verification are designed in this paper. Anonymity is that the true identity of the vehicles should be anonymized by RSUs and other vehicles excepting the TA and themselves. Any third party should not reveal the true identity by the multiple messages from legal vehicles and the multiple messages from legal vehicles should not be revealed by any third party. Besides, the message authentication means that the AP can verify that certain messages are actually sent by legitimate vehicles without any modified or forged.

4 Our scheme

4.1 System key generation

The TA generates a set of public parameters $\{G, q, g\}$, the G is a finite element addition cycle group of order q and a generator g in G. And then, TA will chooses a random number $s \in Z_q^*$ as the private key of the system and the public key (PK) of the system is calculated by $PK = s \cdot g$. Besides, the hash function is an important tool for protecting messages from preventing replay attacks during message forwarding. The hash functions $H : \{0,1\}^* \to G$ and $h : \{0,1\}^* \to Z_q^*$ will be chosen by TA, where $\{0,1\}^*$ represents a string with arbitrary length.

Then, the $\Omega = \{G, q, g, PK, H(\cdot), h(\cdot)\}$ can be regarded as system public parameters, and it is published to each RSUs and vehicles. Based on Ω , TA executes the key generation and registration processes of entities in VANETs.

(1) Key Generation of RSUs and AP: For each RSU, a random number $s_{\mathrm{RSU}} \in Z_q^*$ is selected to be as the private key. Therefore, the corresponding public key is calculated as $PK_{\mathrm{RSU}} = s_{\mathrm{RSU}} \cdot g$, and the key pair $(s_{\mathrm{RSU}}, PK_{\mathrm{RSU}})$ is a key pair will be sent to the corresponding RSU via the secure channel. It is similarly that the TA generates a key pair $(s_{\mathrm{AP}}, PK_{\mathrm{AP}})$ for AP and broadcasts the PK_{AP} to the network.

(2) Key generation and registration of Vehicles: When vehicle v_i joins the VANETs, it will only can be considered as the legal vehicle after having been registered by TA. And then the TA will generates the key to it.

During the process of key generation of vehicle, TA chooses a random number $s_i \in Z_q^*$ as the private key of v_i , and then calculates the corresponding public key as $PK_i = s_i \cdot g$. Besides, v_i chooses a random number $d \in Z_q^*$, and the verify message can be generated by $a_i = h(d \cdot g \| RID_i)$ and $b_i = (d - s_i \cdot a_i)$. At the same time, v_i sends the $\{RID_i, PK_i, a_i, b_i\}$ to TA; after TA receives $\{RID_i, PK_i, a_i, b_i\}$ and checks whether the $a_i = h(b_i P + PK_i^{a_i} \| RID_i)$ holds or not to verify m_i. If holds, $\{RID_i, PK_i\}$ is stored in the tracing table of TA as the legal identity and public key of v_i ; otherwise, v_i will be refused to enter the VANETs by TA.

4.2 Dynamic updating of vehicle pseudonym

The proposed scheme uses the pseudonym to ensure that the identity of a legitimate vehicle can not be obtained by attackers.

Specifically, the TA can generate a pseudonym identity (PID) for v_i by utilizing the $PID_{i,1}$ after registration, and the $PID_{i,1}$ is consisted of $PID_{i,1} = w_i \cdot g$ and $PID_{i,2} = RID_i \oplus H(w_i \cdot PK_i)$, where w_i is a random number selected by TA and $w_i \in Z_q^*$. However, it is easy for the attackers to track and disclose the privacy of the trajectory if the pseudonym is used for a long time. Therefore, it needs to update the pseudonym. The exchange entropy is proposed in this paper as a control tool, and it is defined as the strength of location privacy protection for vehicle.

An anonymous set of vehicles in a pseudonym exchange area is denoted as $C = \{v_1, v_2, \cdots, v_m\}$, indicating that the m vehicles may exchange pseudonym with each other. Assuming that the probability of the vehicle v_i is tracked after pseudonym exchange is p_i , then the exchange entropy can be denoted by $E_i = -\log_2 p_i$. Therefore, the exchange entropy of the set C is $E_C = -\sum p_i \log_2 p_i$.

The probability that v_i happens to select an internal attacker for pseudonym exchange is presented by $A/(N-1)$, the N is the total number of vehicles in the current area, and A is the number of internal attacker. Then, the added exchange entropy of v_i is denoted by

$$\Delta E = \sum_{i=1}^{A} \frac{\binom{A}{i}\binom{N-1}{N-1-i}}{\binom{N-1}{m-1}} \log_2(m-i) \tag{1}$$

The exchange entropy is 0 if v_i exchanges pseudonym with an attacker; otherwise, the exchange entropy after times of pseudonym exchanging is derived by

$$E_i^m(v_j \notin C_{IA}) = E_i(m-1) + \Delta E \tag{2}$$

So, the condition for vehicle to participate in pseudonym exchange can be represented by

$$\Delta E > \frac{P_c(v_j \mid v_{IA}) E_i^{m-1}(v_j \notin C_{IA})}{1 - P_c(v_j \mid C_{IA})} \tag{3}$$

The vehicles that satisfied with the equation (3) can be called as intimate vehicles, and all vehicles are treated as alternative vehicles, it includes intimate vehicles.

When v_i evaluates alternative vehicles, it will observe the exchanging times of alternative vehicles, and identify the pseudonym exchange requests and confirmation or termination message. Meanwhile, v_i will periodically broadcast the pseudonym exchange requests and receive the requests from other vehicles. And then, v_i evaluates the benefit by the equation (3)

If the exchange condition equation (3) is satisfied, send out the pseudonym exchange confirmation message; otherwise, it will broadcast the pseudonym exchange confirmation message to indicate that it tends to abandon the chance.

4.3 Message fragmentation process

The Shamir's (k,n) secret sharing scheme is adopted in this paper. During the process of message fragmentation, v_i firstly calculates the $H(M_i)$ after the number of original messages M_i pieces is determined. The M_i and $H(M_i)$ are two independent secret data, and is divided into some fragments by constructing a polynomial with *k*-1 degrees $f(x_k) = M_i + a_1 x_1 + a_2 x_2^{\,2} + \ldots + a_{k-1} x_{k-1}^{\,k-1}$. Specifically, the $a_1, \ldots, a_{k-1}$ are the random numbers generated by v_i , and *k* represents the secret sharing threshold that is minimum number of fragments of messages for recovering the original message.

In order to ensure the success and safety of recovering, the number of vehicle involved in cooperative recovery is not less than *k* pieces and the number of attackers is not more than *t*. The best value of *k* when $(n-1)/2$. After M_i is fragmented, the content of message piece is $M_{i,j} = (j, f(j))$, and $j = 0, \ldots, k-1$. The AP can recover the message if the number of the received message pieces is satisfied with *k*. Otherwise, AP should wait for a period of time until to the message of time to life (TTL).

To ensure the safety and keep generality of message recovering, the Lagrange interpolation algorithm is used to recover M_i by AP. A polynomial is defined by

$$\Gamma_l(x) = \prod_{i \in I_l} \frac{x - x_i}{x_l - x_i} \tag{4}$$

where $l = 1, 2, \ldots, n$, $I_l = \{1, 2, \ldots, l, \ldots, k\}$. And it satisfies $\forall i \in I_l$, $\Gamma_l(x) = 0$ and $\Gamma_l(x_l) = 1$. so, the function $f(x)$ also can be denoted by

$$f(x) = \sum_{l=1}^{k} f(l) \Gamma_l(x) \tag{5}$$

According to the equation (5), the message will be recovered as $M' = f(0)$, and then the hash value $h(M'_i)$ of M' can be calculated. At the same time, the AP will receive the $h(M_i)$ that is sent together with fragment message. So, the recovery condition can be calculated as $h(M_i) = h(M'_i)$ .If holds, it indicates that the message is successfully recovered; otherwise, the message recovery is failure.

5 Security analysis

In this section, the security analysis of the proposed scheme is indicated as follows.

(1) Anonymity: The RID_i can be derived from the specific pseudonym by calculating $RID_i = PID_{i,2} \oplus H(s \cdot PID_{i,1})$ and $RID_i = PID_{i,2} \oplus H(w_i \cdot PK)$. However, an attacker can't easily get the real identity of vehicle in this paper. Owing to the facts that *s* is known only by TA and is not used in the communication process, the attacker can't get it. In addition,as a random number, w_i is selected by v_i in the process of pseudonym production.

(2) Message Verification: A mechanism is provided in this paper to verify the integrity of the recovered messages. After AP collects enough message pieces and recovers the original message M', it should have $H(M') = H(M)$; otherwise, $H(M') \neq H(M)$. Therefore, the fragment message whether be attacked and the integrity of the recover message both can be verified by the hash value.

In reality, the fragment of message may be dropped, tamped and forged by the trusted forwarding vehicles due to their own interests. To solve these problems, a method is proposed to verify the integrity of the recovered that the performance of routing protocol is better.

6 Performance analysis

In this section, it is mainly evaluate the validity of the proposed scheme based on NS-2 and SUMO, and the performance indicators include vehicle privacy and message exposure.

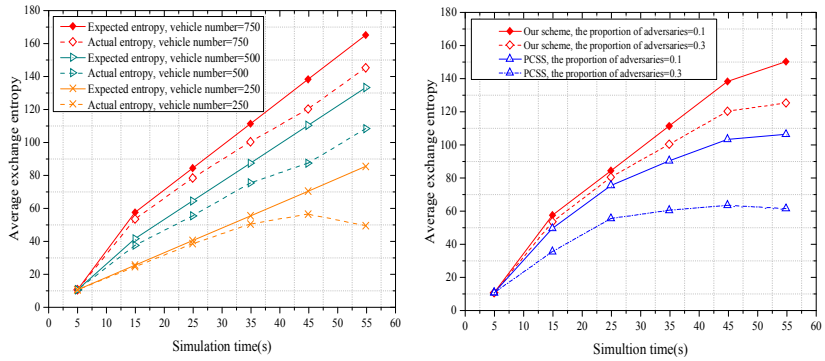
The parameters of specific simulation scenario are set as shown in Table 1.

Table 1. Simulation Parameters.

Parameter	Value
Network Area(m^2)	3000×3500
Simulation Time(s)	100
Mobility Model	SUMO
Vehicle Speed(m/s)	0~30
Number of Vehicles	100~900
TTL(min)	250
Vehicle communication protocol	802.11p

6.1 Utility verification of vehicle privacy protection

The relationship between the average exchange entropy and the simulation time is depicts as **Figure 1**. **[1(a)]** Figure shows that the expected and actual exchange entropy under different traffic conditions. We can see that the the average exchange entropy when the number of vehicles is 750 will be higher 59% than 200. The reason is that the vehicle will meet more other vehicles and so the more chances to exchange pseudonym. However, the actual average exchange entropy is lower than the expected value because that the attacker in the network will have an impact on the pseudonym exchange.



(a) Comparison of average exchange entropy between expected and actual

(b) Comparison of average exchange entropy between our scheme and PCSS

Fig. 1. Efficiency of vehicle privacy protection.

In **[1(b)]** Figure, we can obtain that the comparison of pseudonym exchange mechanism between the proposed scheme in this work and scheme proposed in PCSS [8]. And average exchange entropy decreases as the proportion of malicious vehicles increases. The reason is that the more malicious vehicle, the fewer exchange number, and even exchange pseudonym with attackers. But no matter under what circumstances, the average exchange entropy of the proposed scheme in this work is still surpass the PCSS.

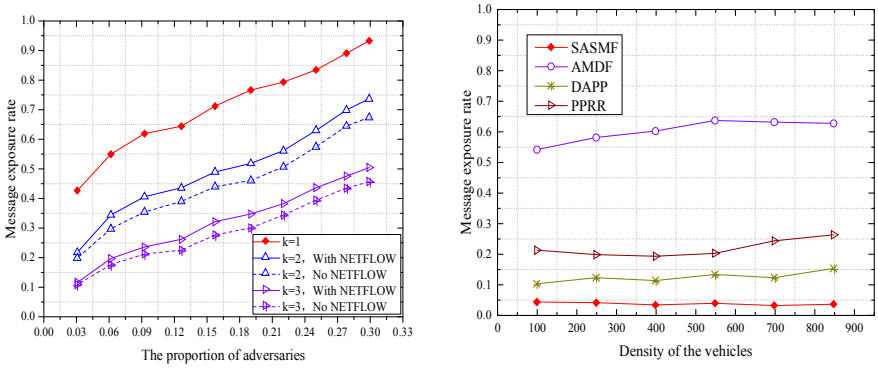
6.2 Utility verification of message privacy protection

The relationship between message expose rate and the proportion of malicious vehicles is shown as **Figure 2(a)**.

From the **[2(a)]** Figure, we can see that the message expose rate increases with the proportion of malicious vehicles increases. It is obvious that the message expose rate is utmost under without any protective measures, and we also can obtain that the message expose rate may be increased under attackers execute traffic analysis. The reason is that malicious vehicles can gain more information about origin messages by analyzing message pieces. Besides, the expose rate can be decreased about 18% with the message pieces increase.

With the increase of the density of vehicles, the exposure rate of the four mechanisms is relatively stable as shown in **Figure 2(b)**. Besides, although the secret sharing is utilized in the proposed scheme and DAPP [10], the message exposure rate of DAPP is still 10% higher than our scheme because there is lack of vehicle privacy protection in DAPP. In addition, we

also can see that the proposed mechanism has the lowest message exposure rate about 5%, while the paper [11] has the highest leakage rate around 56%, and the message exposure rate of [12] is 18% higher than our scheme.



(a)Efficiency of message fragmentation (b)Comparison of average message exposure rate

Fig. 2. Efficiency of message privacy protection.

7 Conclusions

To solve the problem of vehicle privacy and message leaks, we propose a privacy protection mechanism based on secret sharing. In the proposed scheme, it mainly consists of two parts that are the pseudonym exchanging and the message fragmentation. The pseudonym exchange scheme uses pseudonym to hide the real identity of the vehicle, and exchange entropy is used to evaluate the condition of pseudonym exchanging. The mechanism of message fragmentation utilizes the secret sharing scheme to divide the origin message into some fragments and then will be recovered. The security and performance analysis result show that the proposed mechanism can satisfy the safety requirements and vehicle privacy, message exposure rate are all improved.

References

[1] Osaba, E., Onieva, E.: Decentralised intelligent transport system with distributed intelligence based on classification techniques. IET Intelligent Transport Systems. Vol. 10, pp. 674-682 (2016)

[2] Junjie Yan., Dapeng Wu., Sunny Sanyal., Ruyan Wang.: Trust-Oriented Partner Selection in D2D Cooperative Communications. IEEE Access, pp. 3444-3453 (2017)

[3] Dapeng Wu., Shushan Si., Shaoen Wu., Ruyan Wang.: Dynamic Trust Relationships Aware Data Privacy Protection in Mobile Crowd-Sensing. IEEE Internet of Things Journal, pp. 1-1(2017)

[4] Jinbo, Xiong., Fenghua, Li.: A full lifecycle privacy protection scheme for sensitive data in cloud computing. Peer-to-Peer Networking and Applications, Vol. 8, no. 6, pp. 1025–1037 (2015)

[5] Luo T, Kanhere S, Das SK et al.: Incentive Mechanism Design for Heterogeneous Crowdsourcing Using All-Pay Contests. IEEE Trans Mob Comput Vol.15, no. 9, pp. 2234-2246 (2016)

[6] Rongxing, Lu., Xiaodong, Lin.: Pseudonym changing at social spots: An effective strategy for location privacy in vanets. IEEE Transactions on Vehicular Technology. Vol. 61, pp. 86-96 (2012)

[7] Bouksani W, Bensaber BA.: An efficient and dynamic pseudonyms change system for privacy in VANET. In: 2017 IEEE Symposium on Computers and Communications (ISCC). Heraklion, pp 59-63 (2017)

[8] Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing. Vol.2, no. 1, pp. 46-55 (2003)

[9] Levente, Buttyán., Tamás, Holczer.: On the effectiveness of changing pseudonyms to provide location privacy in VANET. Proceedings of ESAS, pp. 129-141 (2007)

[10] Di, Tang., Jian, Ren.: A Novel Delay-Aware and Privacy-Preserving Data-Forwarding Scheme for Urban Sensing Network. IEEE Transactions on Vehicular Technology. Vol. 65, no. 5, pp. 2578-2588 (2016)

[11] Yangjie, Xia., Wenzhi, Chen., Xuejiao, Liu.: Adaptive Multimedia Data Forwarding for Privacy Preservation in Vehicular Ad-Hoc Networks. IEEE Transactions on Intelligent Transportation Systems. Vol. 99, pp. 1-13 (2017)

[12] Khaled, Rabieh., Mohamed, M. E. A. Mahmoud., Mohamed, Younis.: Privacy-Preserving Route Reporting Schemes for Traffic Management Systems. IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2703-2713 (2017)