Location privacy protection scheme based on self-organizing cryptographic mix-zone in VANETs

Xin Xin*, Tianhan Gao, and Xinyang Deng
Software College, Northeastern University, Shenyang, China
xinxin@stumail.neu.edu.cn, gaoth@mail.neu.edu.cn, xinyang1121@sina.com

Abstract

How to ensure the location privacy of vehicles has become an important security issue of VANETS. One of the effective mechanisms to protect the vehicles' location privacy is replacing the pseudonym to achieve unlinkability with the help of road side unit (RSU). This paper takes the scenario into account where RSUs have not yet been deployed widely. When a vehicle wants to change pseudonym, it transmits group keys in a collaborative manner and creates encrypted areas with surrounding vehicles. At this point, the external attackers cannot crack any information in this area, the cryptographic mix-zone. During this period, some vehicles will be replaced with new pseudonyms. The external attackers are not able to associate the pseudonyms with the old ones to achieve the goal of location privacy protection of the vehicles.

Keywords: VANETs, Location privacy, cryptographic mix-zone, group key agreement

1 Introduction

In recent years, with the proliferation of vehicle users, the issue of road traffic safety has become a global public safety problem. How to improve the traffic safety situation has gradually become a research hotspot in both academic and industry community. Meanwhile, VANETs has brought revolutionary changes to the transportation system. It is an important part of the intelligent transportation system(ITS) and shoulders the responsibility of ensuring people's travel safety and improving the traffic efficiency of vehicles.

The basic idea of VANETs is that vehicles within a certain range of movement can exchange the obtained road condition information data with each other, and establish self-organizing networks according to the corresponding networking methods. Communication of VANETs is divided into two types: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). VANETs can not only achieve local communication between vehicles, but also be connected to other forms of networks, such as mobile communication networks, through roadside infrastructures to make the entire intelligent transportation more convenient and faster.

VANETs is able to help the driver to get the running status and road conditions of the surrounding vehicles, such as speed, direction, road accidents, etc, to obtain early response and processing time for accidents. At the same time, the VANETs system can help drivers obtain road traffic information in advance and arrange travel routes as rationally as possible, However,security issues have become a main obstacle for the wide deployment of VANETs. Privacy is one of the key problem in VANETs, where vehicles must periodically broadcast beacon messages to nearby vehicles for security applications such as co-drive or accident warnings[9].On one hand, identity privacy may be destroyed when drivers apply for such services, causing attackers to fake false information and causing traffic accidents, affecting the

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 4, Article No. 11 (September 15, 2018)
*Corresponding author: Software College, Northeastern University, Shenyang, CO 110169 CHN, Tel: +86-186-4034-9515

normal operation of the transportation system. On the other, the exposure of the vehicle node's location privacy means that the attacker can track certain vehicles, obtain their running trajectory, and even predict the direction of their subsequent travels.

In order to protect the privacy, the vehicle can adopt a method of periodically changing its anonymous certificate to mislead the attacker[2, 5, 3]. A better solution is to establish the Mix-Zone area[1, 6]. Our previous research proposes a location privacy protection scheme based on a random encryption period[7]. But this scheme needs RSU to obtain the group key. However, at the initial stage of the construction of VANETs, some specific area may have no RSUs. The main research of this paper is use to address this issue,which includes the following contributions.

1. According to the space-time factors in the network, the trust model is established.

2. A location privacy protection scheme based on group key agreement and random encryption period is proposed.

3. Performance analysis of the scheme is presented.

2 Preliminaries

2.1 Bilinear pairing

Given two groups $G1$ and $G2$ with same order p, where $p = q^n$, q is prime and $n \in Z^*$, $G1$ is an additive group, and $G2$ is a multiplicative group. Assume that the discrete logarithm problem on the above two groups is difficult. If the mapping $e : G1 \times G1 \to G2$ satisfies the following three properties, then e is a bilinear pairing:

(1) Bilinear: for any $P \in G1$,$Q \in G1$ and $a, b \in Z_q*$, there are $e(aP, bQ) = e(P, Q)ab$.

(2) Non-degeneracy: there must be certain $P \in G1$, $Q \in G1$ satisfy $e(P, Q) = 1$.

(3) Computability: there must be an efficient algorithm that can calculate $e(P, Q) \in G2$, where $P \in G1$, $Q \in G1$.

2.2 Location privacy protection approaches

Mix-Zone [1] was first proposed by Beresford in 2003 as a geographical area to protect user privacy. Mix-Zone is an area that cannot be monitored. Vehicles update the pseudonym in Mix-Zone, making it difficult to correlate information from the same node to protect the privacy of location.

Albert [7]etc. improved [4] and proposed a privacy protection scheme based on a random encryption period (REP). When a node changes a pseudonym, it requests a random encryption period to be triggered. Members in the group encrypt all the information with the group key to interfere with external eavesdroppers. The random encryption period prevents the global observer from listening for information in the area when the certificate update occurs, thus reducing the possibility of tracking the OBU. However, this scheme has a heavy burden on the TA. In addition, when the group key is updated, each OBU must perform a large number of calculations to update all the symmetric keys.

Our previous research used RSU to replace part functions of TA. Vehicle's pseudonym was generated by TA and RSU together. Group key was issued by RSU, which reduced the overhead of group key update. However, our previous research did not consider how the vehicles establish encrypted areas where RSUs are not deployed.

3 The Proposed Scheme

3.1 Trust model

As shown in Fig. 1, the trust model of the scheme is composed of three entities: Trusted Authority (TA), Roadside Units (RSUs), On-Board Units (OBUs).

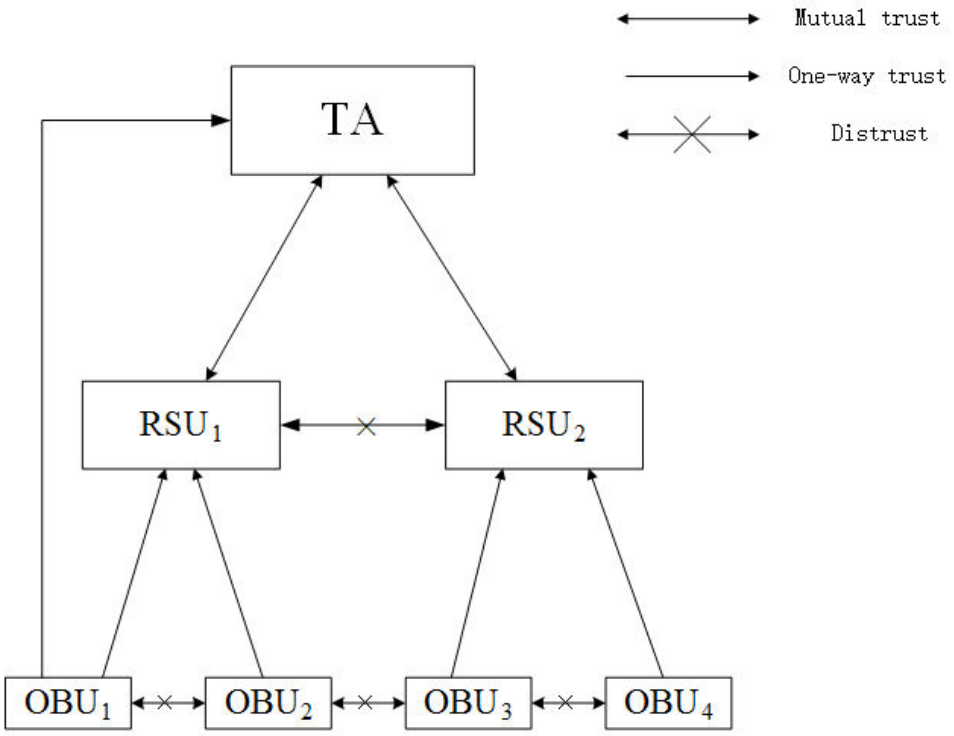

Figure 1: Trust model

- Trusted Authority (TA): TA is usually a trusted third party which is mainly responsible for the identity management of RSUs and OBUs.
- Roadside Units (RSUs): RSUs are managed and regularly monitored by TA. The RSUs and TA are connected through secure channel. RSU is credible and owns strong computing power.
- On-Board Units (OBUs): Each vehicle is equipped with an OBU, including tamper-proof device(TPD) that stores secret information, event data recorder (EDRs), and global positioning systems. Vehicles should regularly broadcast their safety information.

3.2 Description of the scheme

In our previous research, we have proposed a specific solution for vehicle location privacy protection in VANETs with the help of RSU. However, in the current situation where VANETs are not deployed on a large scale, the RSU cannot cover the entire area. The scheme proposed in this paper is mainly aimed at resolving how the vehicles negotiate the group key in the above-mentioned area and build the cryptographic Mix-zone to protect the privacy of location.

3.2.1 V2V Authentication

The pseudonym generation process for vehicles has been proposed in our previous research. After the vehicle generates the pseudonym, it uses the pseudonym to communicate with the rest of the vehicles. Certificate $Cert_{R_i}$ is part of a pseudonym and is used to test the validity of the pseudonym. When the vehicle v_a communicates with other vehicles, it is necessary to verify the legality of the v_a. Take v_a and v_b communication as an example. The verification process is as follows:

V_a sends its own pseudonym $PN^j_{(a,i)}$ when sending a message. When v_b receives the pseudonym of v_a, it first uses TA's public key P_{TA} to verify that $Cert_{R_i}$ is a legal certificate. If the certificate is valid, the signature $SIG(T_{(a,i)}, t_{(a,i)}; S_{R_i})$ is verified with the public key R_i in the certificate. If the signature is legal, v_a is regarded as a legal one. The specific process is shown as Fig. 2.

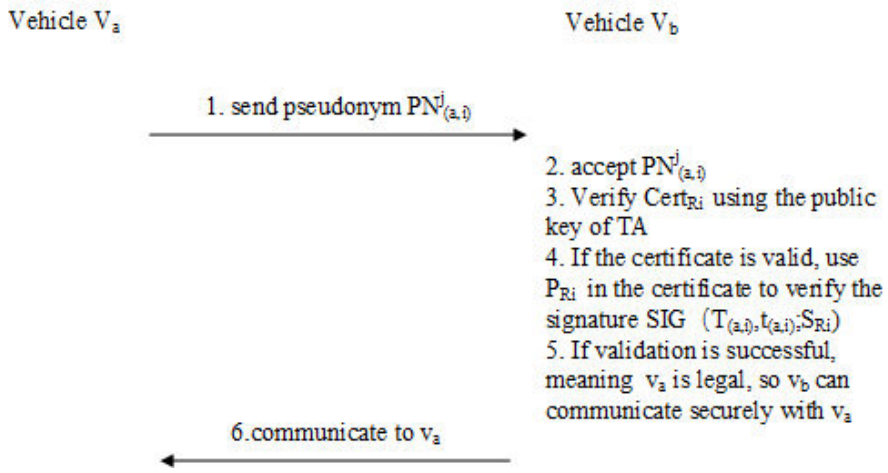

Figure 2: V2V Authentication

After V2V authentication, a session key can be negotiated build secure communications between vehicles. This not only ensures the security of the system, but also reduces the session overhead and improves the system performance.

3.2.2 Group Key Agreement

When the vehicle is driving in the area where the RSU is deployed, its group key is issued by the RSU. When the vehicle enters the RSU area, it needs to first authenticate with the RSU, and then the RSU issues a group key to the legally authorized vehicle. The vehicle uses the group key to create an encrypted zone, replacing the pseudonym to protect location privacy. This section proposes a scheme for how the vehicle negotiates a group key in an area without a RSU.

1. The vehicle v_a that needs to change the pseudonym broadcasts a message $msg = \{request_{CMIX}, PN^j_{(a,i)}, T_{CMIX}\}$, where $request_{CMIX}$ is a request to start a cryptographic Mix-zone, $PN^j_{(a,i)}$ is a pseudonym currently used by the vehicle, and T_{CMIX} is a duration of the cryptographic Mix-zone.

2. According to the DSRC protocol, vehicles can receive msg within 300 meters of v_a[8]. After receiving this message, the vehicles check the remaining validity of their current certificates. If the remaining period of validity is lower than T_{CMIX}, the vehicle needs to change its own pseudonym and a response is broadcast immediately.

3. If v_a receives the response, it generates the symmetric key k_g as the group key. Otherwise, v_a resends the request to turn on the random encryption period after a while.

4. v_a sends the group key to the vehicles that have established secure communication before, encrypts the group key using the session key, and sends it to the trusted vehicle.

5. The vehicle that received the group key judges whether it has received the request message *msg*. If the vehicle receives the *msg*, it repeats step 4 to encrypt the group key and sends it to the trusted vehicles that establish the secure communication. If the vehicle has not received *msg*, it only needs to save the group key.

6. If the vehicle v_c that received the *msg* has not received the group key, it judges whether $T_{current} - T_{CMIX_{start}} + T_{req_gk} < T_{CMIX}$, where $T_{current}$ represents the current time, and $T_{CMIX_{start}}$ represents the time when the random encryption period starts, T_{req_gk} represents the average duration when the vehicle broadcasts the request and obtains the group key. If condition satisfies, it means that v_c can obtain the current group key before the end of the random encryption period. At this time, v_c broadcasts a key request message and seeks the current group key to the nearby vehicles. When the nearest vehicle v_d who owns the group key returns a reply, v_c and v_d use the V2V authentication to establish secure communication. After establishing the secure communication, v_d sends the current group key to v_c.

3.2.3 Location Privacy Protection

1. After vehicle v_a generates a group key k_g and sends it to the trusted vehicles, v_a encrypts all secure messages using the group key. The vehicles that received the group key and *msg* also use the group key to encrypt the security information. We named the vehicles of the encrypted message as an encryption group.

2. After the encryption begins, v_a monitors all vehicles in the encryption group. In addition, v_a changes its own pseudonym and the speed or trajectory (lane/direction);

3. The vehicles whose remaining validity period is lower than T_{CMIX} also begin to change their pseudonyms and speed or trajectory;

4. The vehicles who changed pseudonyms together broadcast *response*2, indicating that they have completed changing the pseudonyms, speed or trajectory;

5. v_a checks if the condition(1) is satisfied within the cryptographic mix-zone period:

   The number of *response*2 received is ≥ 2 (1)

If (1) is satisfied at the end of T_{CMIX}, the cryptographic mix-zone period is terminated by broadcasting a message informing the encryption group to stop encrypting their message.

If (1) is not satisfied before T_{CMIX}, v_a will broadcast another request to open a new cryptographic mix-zone period to protect its own location privacy.

If v_a needs to continue V2V communication with other vehicles, The vehicle can encrypt the new pseudonym using the established session key and send it to the communicating vehicle, so as to ensure the normal communication.

In this process, the more vehicles with the replacement of the pseudonym, the higher the location privacy of the scheme. Since the legitimate members of the group have group keys, the cryptographic mix-zone does not affect the communication between them and the acquisition of security information.

On the contrary, the external adversary does not have the group key, which prevents them from eavesdropping messages during the certificate replacement period, thereby reducing the possibility of tracking vehicles.

4 Conclusion

This paper propose a scheme based on cryptographic mix-zone to protect the location privacy of vehicles in VANETs. this paper proposes that in the initial stage of VANETs deployment, if the RSU fails to cover all areas, the vehicle and its neighbors will negotiate a group key. For vehicles that need to change the pseudonyms, the surrounding vehicles will be triggered to build a cryptographic mix-Zone, which makes it impossible for external attackers to observe ,which achieve the purpose of confusing external attackers. Through the security analysis and performance analysis of the scheme, the reliability and efficiency of the scheme is proved.

References

[1] A. R. Beresford and F. Stajano. Stajano, f.: Location privacy in pervasive computing. ieee pervasive computing 2, 46-55. *IEEE Pervasive Computing*, 2(1):46–55, January 2003.

[2] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte. Slow: A practical pseudonym changing scheme for location privacy in vanets. In *Proc. of the 2009 IEEE Vehicular NETWORKING Conference (VNC'09), Tokyo, Japan*, pages 1–8. IEEE, October 2015.

[3] B. K. Chaurasia and S. Verma. Optimizing pseudonym updation for anonymity in vanets. In *Proc. of the 2008 IEEE Asia-Pacific Services Computing Conference (APSCC'08), Yilan, Taiwan*, pages 1633–1637. IEEE, October 2008.

[4] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J. P. Hubaux. Mix-zones for location privacy in vehicular networks. *Proc. of the 1st International Workshop on Wireless Networking for Intelligent Transportation Systems (WINITS'07), Vancouver, British Columbia, Canada*, January 2007.

[5] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Transactions on Vehicular Technology*, 61(1):86–96, July 2011.

[6] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su. Mix-zones optimal deployment for protecting location privacy in vanet. *Peer-to-Peer Networking and Applications*, 8(6):1108–1121, November 2014.

[7] A. Wasef and X. Shen. Rep: Location privacy for vanets using random encryption periods. *Mobile Networks and Applications*, 15(1):172–185, May 2009.

[8] S. H. Wu, C. M. Chen, and M. S. Chen. An asymmetric and asynchronous energy conservation protocol for vehicular networks. *IEEE Transactions on Mobile Computing*, 9(1):98–111, May 2009.

[9] B. Ying, D. Makrakis, and Z. Hou. Motivation for protecting selfish vehicles' location privacy in vehicular networks. *IEEE Transactions on Vehicular Technology*, 64(12):5631–5641, October 2015.

Author Biography

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained a promotion to a professor in June 2017. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He obtained the doctoral tutor qualification in 2016. He is the author or co-author of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, as well as virtual reality.

Xin Xin received the B.E. degree from the Software College, Northeastern University, in 2016. She is currently pursuing the master's degree with the Graduate School, Software College, Northeastern University. Her research interests include wireless mesh network security, vehicular networks security, and vehicular networks privacy.

Xinyang Deng received the BE in Software College from Dalian University of Foreign Languages in 2014, and now he studies in Software College of Northeastern University. His primary research interests are next generation network security, PMIPv6 security and Identity-based Cryptography