A Location Privacy-Preserving Scheme for VANETs Based on Virtual Mix Zone

Nan Guo, Linya Ma*, and Tianhan Gao
Northeastern University, Shenyang, Liaoning 110000 China
guonan@mail.neu.edu.cn, malinya199303@163.com, gaoth@mai.neu.edu.cn

Abstract

The location of vehicles, which may contain some sensitive information, is critical for VANETs security. The literature location privacy-preserving scheme suffers from either selfish vehicle node or vehicle density issues. In this paper, a novel location privacy-preserving scheme for VANETs is proposed based on virtual mix zone which is created dynamically when the pseudonyms of vehicle nodes are going to be expired. Moreover, a reputation model and mechanism is introduced to encourage the selfish node to join the mix zone. The evaluation and analysis show that the proposed scheme performs better than the typical ones in terms of privacy strength and energy cost.

Keywords: virtual mix zone, reputation model, location privacy, VANETs

1 Introduction

In recent years, with the rapid development of mobile ad hoc networks and wireless sensor technology, vehicle ad hoc networks (VANETs) emerge and become more and more popular [9]. VANETs are the specific applications of mobile ad hoc networks in the field of intelligent traffic system(ITS). VANETs consist of on-board units (OBUs) and road side units (RSUs), which allow the vehicle to communicate with other vehicles (vehicle-to-vehicle, V2V) or roadside infrastructures (vehicle-to-infrastructure, V2I) to build a multi-hop communication network. VANETs can provide location-based services (LBS) so as to achieve inter-vehicle collaborative safety driving, traffic decision support, traffic intelligent dispatching, real-time traffic information releasing, and other ITS services [4].

VANETs play an important role in traffic safety and traffic efficiency improvement. However, with the widespread of LBS in VANETs, privacy issues are becoming more and more prominent [6]. LBS employs location technologies (GPS, WiFi access positioning, etc.) to provide users with location-related personalized service. While the relevant services may lead to the disclosure of vehicle location privacy. Thus the preserving of location privacy in VANETs must be achieved.

Pseudonym changing is a feasible approach to protect the location privacy of vehicle nodes. In VANETs the most common solution for changing pseudonyms is establishing mix zone [14, 3, 11, 7, 8, 13]. Multiple vehicles simultaneously change pseudonyms in an area to confuse the association between old and new pseudonyms. However, in the conventional mix zone schemes [14, 11, 7, 8, 13], lower density of vehicle nodes and decentralization of cooperative vehicle nodes may cause the decrease of location privacy. As a result, establishing virtual mix zone is able to achieve higher location privacy.

Due to the rapid mobility of vehicle nodes in VANETs, the network topology changes rapidly and the density of vehicle nodes is unstable. In this paper, a virtual mix zone scheme (VMixzone) based on reputation model is proposed according to the characteristics of VANETs. VMixzone allows nodes

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 3, Article No. 10 (November 15, 2017)
*Corresponding author: Software College, Northeastern University, Shenyang, Liaoning, 110169, China, Tel: +86-186-0403-0441

to decide whether or not to cooperate with target nodes in changing pseudonyms. In order to stimulate selfish nodes to cooperate with each other, we combine the reputation mechanism with virtual mix zone. Through the evaluation and analysis, VMixzone has significant superiority in terms of location privacy strength and energy consumption compared with the typical VANETs location privacy-preserving schemes.

The remainder of this paper is organized as follows. In Section 2, the related technologies are discussed. The proposed VMixzone scheme is presented in detail in Section 3. The evaluation and analysis of VMixzone are given in Section 4. The conclusions are made in Section 5.

2 Preliminaries

2.1 VANETs

As shown in Figure 1, VANETs mainly include on-board units (OBUs), road side units (RSUs), trusted authority (TA), and service provider (SP). OBUs, embedded in the vehicles, are responsible for communication between vehicles and RSUs or other vehicle nodes. RSUs, deployed at regular intervals, are infrastructure nodes. RSUs are responsible for OBUs' network access and communication between OBUs and TA. TA is in charge of vehicle nodes authentication, certificate issuance, and certificate revocation, etc. SP is responsible for providing information services, including LBS. V2V and V2I communication is based on DSRC (special short-range communication technology) to achieve a small range of data transmission.

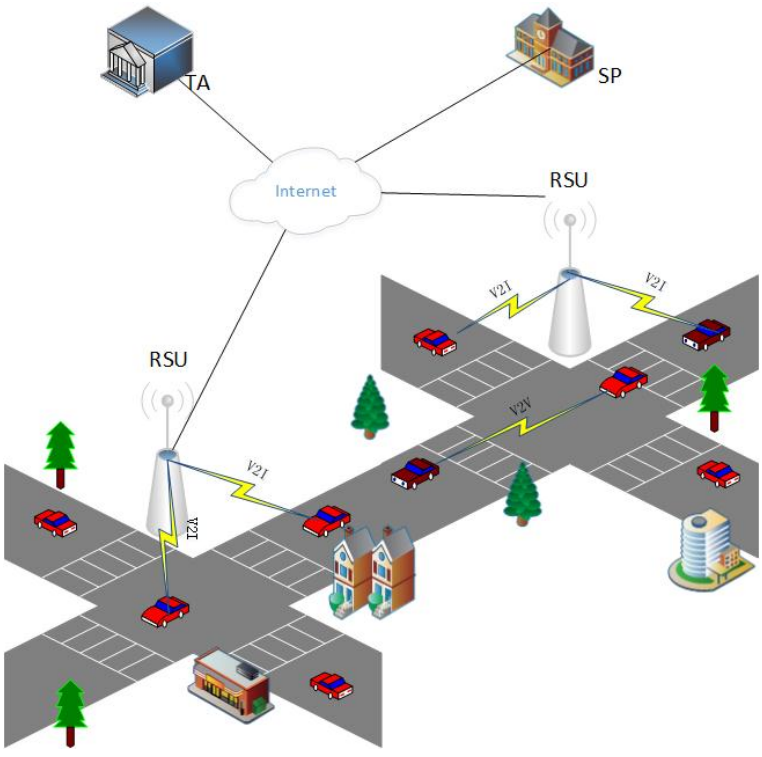


Figure 1: VANETs Framework

2.2 Mix Zone

Mix zone was firstly proposed by Beresford[1] in 2003. It is an area for vehicle nodes to change pseudonyms so that messages from the same node are difficult to associate. Several kinds of mix zone have been proposed. The mix zone based on special location[11] allows vehicle nodes change pseudonyms in a pre-defined area, such as the intersection, and vehicle nodes choose different paths to leave after pseudonyms changed. The mix zone based on silent period[7] allows vehicles randomly select a period of time not to send beacon message that is silent to change pseudonyms. But for some of the demanding real-time applications such as collision avoidance, this kind of mix zone is not applicable. The encryption mix zone[5, 2] is to construct an encrypted communication area at the selected intersection. And RSU at the intersection is responsible for issuing the session key to vehicles entering the area. This kind of mix zone has high security, high communication overhead and latency. The dynamic mix zone[14, 3, 8, 13] allows vehicle nodes loosely change pseudonyms when their strength of location privacy is low or their pseudonyms are about to expire.

3 The Proposed VMixzone Scheme

3.1 Network Architecture and Trust Model

As shown in Figure 2, the network architecture in this scheme includes four types of entities: Trusted Authority (TA), Control Servers (CSs), Roadside Units (RSUs), and Onboard Units (OBUs). TA and CSs are trusted in default, and have certain storage and computing power. TA is mainly responsible for certificate issuing and identity authentication for RSUs and OBUs. CSs are responsible for controlling and adjusting the pseudonym changing process and setting or updating reputation for nodes. OBUs can directly communicate with each other within 300m distance.

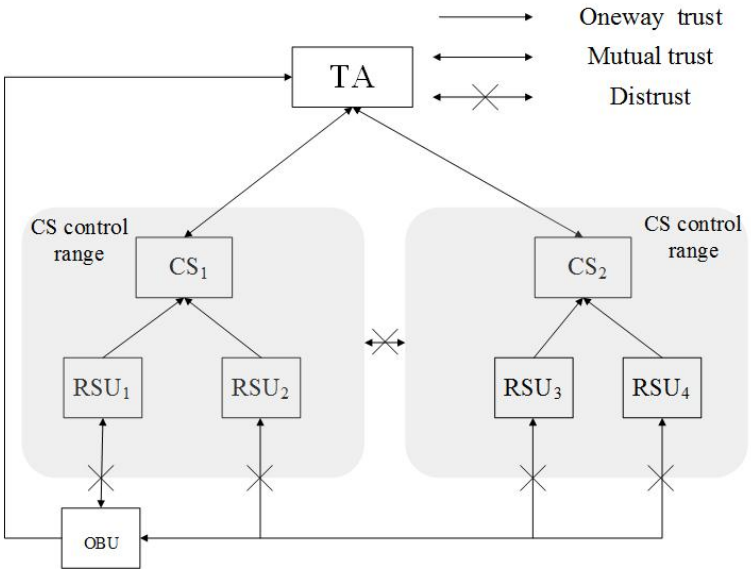


Figure 2: Network Architecture and Trust Model

In addition, for the convenience of the scheme description, Table 1 gives the relevant identifications and descriptions.

Table 1: Identifications and Descriptions

Identification	Description
N_s	Target vehicle node
S	The region that N_s requests for virtual mix zone
N_i	Other nodes within S
M	The virtual mix zone
PS_{N_i}/PS'_{N_i}	The old/new pseudonym of N_i
T_i/T'_i	The validity period of old/new pseudonym
SoLP	Strength of location privacy
$P_{d\|b}$	The probability of establishing associations between old pseudonym and new pseudonym
δ	Threshold of reputation
R_i/R'_i	Reputation /new reputation of N_i
t_R	The last response time to N_s
t_{GM}	The time to generate virtual mix zone
k	The number of collaborative nodes that N_s needs
Sig_s	Footprint signature generated by N_s
Sig	Footprint signature set
PK_{N_i}/Prv_{N_i}	Public key/Private key of N_i

3.2 Reputation Model

Assume that attacker has monitored that all vehicle nodes (number of nodes is N) in S have experienced pseudonym changing. The attacker compares the old pseudonyms sequence B with the new pseudonyms sequence D by (1) according to [14]:

$$P_{d|b} = P(Pseudonymd \in D \leftarrow b \in B) \tag{1}$$

For the target vehicle node, the highest strength of location privacy is (2) from [12]:

$$H - SoLP = -\sum_{i=1}^{N} P_{d|b} log_2 P_{d|b} \tag{2}$$

In this paper, CS is able to detect vehicle nodes who change pseudonyms. Assume that CS detects that r vehicle nodes have changed pseudonyms in S. The strength of target and cooperative nodes' location privacy can be obtained by the equation 3:

$$SoLP = -\sum_{i=1}^{r} P_{d|b} log_2 P_{d|b} \tag{3}$$

It can be seen that the strength of location privacy depends on the number of vehicles that collaborate (r) and $P_{d|b}$. If only the target node changes pseudonym in S, the adversary can establish a correlation between its old and new pseudonym causing the location privacy strength of target vehicle is zero, SoLP = 0. When $P_{d|b}$ for cooperative nodes is the same, that is, $P_{d|b} = 1/r$, the value of SoLP is maximal $SoLP = log_2 r$.

Due to the limited pseudonyms and the high cost of updating pseudonyms, there may be some selfish vehicle nodes not cooperating in S. We introduce a reputation model to motivate selfish nodes to cooperate. The reputation value of cooperative node N_i will increase. And the value of increase depends on the

number of cooperative vehicles. The new reputation strength of N_i is calculated as follows:

$$R_i^{'} = R_i + \frac{SoLP}{H - SoLP} = R_i + \frac{-\sum_{i=1}^{r} P_{d|b} log_2 P_{d|b}}{-\sum_{i=1}^{N} P_{d|b} log_2 P_{d|b}} \quad (4)$$

When N_i register to VANETs, its reputation is set with zero. The reputation of N_i will increase if it cooperate with other vehicles. We assume that after N_i establishes its own virtual mix zone, N_i runs out its reputation and has to accumulate it by cooperation. The CS sets a reputation threshold δ to judge whether a node is selfish or not. A node is regarded as selfish node, if its reputation is lower than δ. Otherwise it can avoid frequently change pseudonyms to achieve higher reputation.

3.3 VMixzone Scheme

When the system is initialized, the TA is responsible for issuing certificates for nodes. Each node should first register with TA after entering VANETs. TA issues a series of public and private keys pairs Pub/Prv and pseudonyms to vehicle nodes. Legal vehicle node has a reputation value of zero.

VMixzone is divided into four phases: virtual mix zone request, virtual mix zone response, virtual mix zone preparation, virtual mix zone establishment.

(1) Virtual mix zone request

When the pseudonym of N_s is about to expire and no other nodes request to establish a virtual mix zone, N_s will broadcast its pseudonym changing collaboration request to the peers. First, N_s generates request $Req =< S, t_R, t_{GM}, k, R_s >$, containing virtual mix zone region S, the response deadline t_R, virtual mix zone generation time t_{GM}, number of requested collaborators k, and N_s's reputation value R_s.

(2) Virtual mix zone response

After receiving request message from N_s, N_i will decide whether to cooperate with N_s according to its own reputation R_i, reputation of N_s, R_s, and validity of its pseudonym.Three cases should be considered:

- If $R_i \leqslant \delta$, N_i decides to cooperate with N_s to increase its own reputation value.
- If $R_s \geqslant \delta$, N_i cooperates with N_s.
- If the pseudonym of N_i is about to expire, N_i decides to cooperate with N_s.

If any of the above cases is satisfied, N_i will choose to cooperate with N_s. Meanwhile N_i will generate the footprint signature $Sig_i = \{PS_{N_i}^{'} \parallel M \parallel T_i^{'}\}_{Prv_{N_i}}$, including its new pseudonym $PS_{N_i}^{'}$, virtual mix zone region M, and the validity of new pseudonym $T_i^{'}$. Then N_i encrypts its current pseudonym PS_{N_i}, M, the validity of current pseudonym T_i, the current reputation R_i, and footprint signature with its public key. Finally, N_i sends response message $\{PS_{N_i} \parallel M \parallel T_i \parallel R_i \parallel Sig_i\}_{PK_{N_s}}$ to N_s by epidemic routing protocol[10] within t_R.

(3) Virtual mix zone preparation

After receiving response message from N_i, N_s checks whether the number of nodes replying is larger than k. If the number is less than k, N_s will enlarge the size of S and resend the request. If the number is equal or larger than k, N_s will choose k collaborators with the highest reputation. Then N_s will generate its footprint signature $Sig_s = \{PS_{N_s}^{'} \parallel M \parallel T_s^{'}\}_{Prv_{N_s}}$ through $PS_{N_s}^{'}$, M, and $T_s^{'}$. N_s will collect all cooperators' footprint signatures to form footprint signature set $Sig = \{Sig_i \mid i = 1, \ldots, i = k+1\}$. Finally, for each participant N_i, N_s encrypts Sig with N_i's public key : $\{Sig\}_{PK_{N_i}}$and sends it to N_i.

(4) Virtual mix zone establishment

At t_{GM}, all collaborators start to broadcast footprint signatures of other vehicles to establish virtual mix zone. Each virtual mix zone has at least k+1 vehicles (virtual / real) to update their footprint signatures. Every footprint signature represents one vehicle node. The pseudonym of vehicle node is hidden in the footprint signature.

After the virtual mix zone is established, CS will monitor how many vehicles change their pseudonyms. CS is responsible for calculating the new reputation value for nodes who change the pseudonym:

$$R_i^{'} = R_i + \frac{SoLP}{H - SoLP} = R_i + \frac{-\sum_{i=1}^{k+1} P_{d|b} log_2 P_{d|b} - \sum_{i=1}^{n} P_{d|b}^{'} log_2 P_{d|b}^{'}}{-\sum_{i=1}^{N} P_{d|b} log_2 P_{d|b} - \sum_{i=1}^{n} P_{d|b}^{'} log_2 P_{d|b}^{'}} \tag{5}$$

Where n is the number of virtual vehicle nodes in virtual mix zone, and $P_{d|b}^{'}$ is the probability of establishing correlation between the virtual vehicle pseudonym and its corresponding true vehicle old pseudonym.

After the virtual mix zone is established, the reputation of target vehicle node returns zero, that is, $R_s^{'} = 0$.

4 Evaluation and Analysis

In this section, we will analyze VMixzone, MPSVLP [14], and AVATAR [3] in terms of strength of location privacy and cost of energy. MPSVLP [14] combines reputation model and mix zone scheme to motivate selfish vehicles to cooperate by using reputation. AVATAR [3] requires cooperative vehicles to generate signature sets and target vehicle to choose cooperators through multiunit discriminatory auction game.

Strength of location privacy is the degree of confusion for vehicles who change pseudonyms. The privacy strength of VMixzone and AVATAR is higher than that of MPSVLP with different k, since cooperative vehicles use the footprint signature to establish virtual mix zone in VMixzone and AVATAR. Every cooperative vehicle has k neighbor nodes who change pseudonyms. Moreover, several virtual mix zones will be established in S in VMixzone and AVATAR against to achieve higher location privacy strength, only one mix zone in MPAVLP.

In the related schemes, target vehicles consume some energy when they send request, generate footprint signatures, and change pseudonyms. Energy consumption is larger in AVATAR and VMixzone when the location privacy strength is the same. The mix zone is bigger in MPSVLP. Cooperative vehicles in MPSVLP do not need to generate footprint signatures and reply them to target vehicles. Meanwhile, target vehicles do not need to send footprint signature sets to cooperative vehicles. Therefore the energy cost is lower. In AVATAR, every cooperative vehicle needs to generate a footprint signature set containing several signatures. Thus the energy consumption in AVATAR is the highest.

5 Conclusion

In this paper, we propose VMixzone—a location privacy-preserving scheme where the reputation model is combined with the virtual mix zone. VMixzone allows vehicles to determine whether or not to cooperate with each other in order to cut down unnecessary pseudonyms expenses. The cooperative vehicles generate footprint signatures, so that there are a number of virtual vehicle nodes around cooperative vehicles to improve the location privacy. The concrete performance analysis and simulations are presented to demonstrate the efficiency and adaptability of VMixzone.

Acknowledgments

This work was supported by National Natural Science Foundation of China under [Grant Number 61402095].

References

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

[2] M. Dahl, S. Delaune, and G. Steel. Formal analysis of privacy for vehicular mix-zones. In *Proc. of the 15th European Symposium on Research in Computer Security, Athens, Greece (ESORICS'10), LNCS*, volume 6345, pages 55–70. Springer, Berlin, Heidelberg, September 2010.

[3] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong. Mixzone in motion: Achieving dynamically cooperative location privacy protection in delay-tolerant networks. *IEEE Transactions on Vehicular Technology*, 62(9):4565–4575, June 2013.

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero. Vanet security surveys. *Computer Communications*, 44(5):1–13, May 2014.

[5] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. P. Hubaux. Mix-zones for location privacy in vehicular networks. In *Proc. of the 2007 ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS'07), Vancouver, Canada*. ACM, August 2007.

[6] B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18, November 2007.

[7] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing wireless location privacy using silent period. In *Proc. of the 2005 IEEE Wireless Communications and Networking Conference, New Orleans, Louisiana, USA*, volume 2, pages 1187–1192. IEEE, March 2005.

[8] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran. Swing & swap: user-centric approaches towards maximizing location privacy. In *Proc. of the ACM Workshop on Privacy in Electronic Society (WPES'06), Alexandria, Virginia, USA*, pages 19–28. ACM, October 2006.

[9] H. E. Ming-Xing, W. Zhu, L. I. Xiao, D. W. Luo, and J. X. Zhao. Privacy-preserving authentication protocols in vehicular ad hoc networks. *Journal of Xihua University*, pages V1:437–V1:442, April 2012.

[10] P. Mundur, M. Seligman, and G. Lee. Epidemic routing with immunity in delay tolerant networks. In *Proc. of the 2008 Military Communications Conference (Milcom'08), San Diego, California, USA*, pages 1–7. IEEE, November 2008.

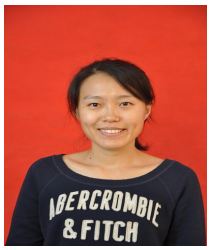
[11] B. Palanisamy and L. Liu. Mobimix: Protecting location privacy with mix-zones over road networks. In *Proc. of the 27th International Conference on Data Engineering (ICDE'11), Hannover, Germany*, pages 494–505. IEEE, April 2011.

[12] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In *Proc. of the 2nd International Workshop on Privacy Enhancing Technologies (PET'02), San Francisco, California, USA, LNCS*, volume 2482, pages 41–53. Springer, Berlin, Heidelberg, April 2002.

[13] J. H. Song, V. W. S. Wong, and V. C. M. Leung. Wireless location privacy protection in vehicular ad-hoc networks. *Mobile Networks and Applications*, 15(1):160–171, February 2009.

[14] 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, December 2015.

Author Biography



Nan Guo received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2005, respectively. She joined Northeastern University in September 2005. She has been an associate professor since 2008. She has been a visiting scholar at department of Computer Science, Purdue, from August 2010 to August 2011. Her research interests are security and privacy in social network and digital identity management.

Linya Ma received the BE degree in Software College from Northeastern University in 2016. Currently she is taking a master's course at Graduate School of Software College, Northeastern University. Her research interests include wireless mesh network security, VANETs security and VANETs privacy.

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 an early promotion to an associate professor in January 2010. 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.