2019 International Conference on Computer Communication and Informatics (ICCCI -2019), Jan. 23 – 25, 2019, Coimbatore, INDIA

Location Privacy Preservation in VANET using Mix Zones – A survey

C. Kalaiarasy
Department of Computer Science
and Engineering
Pondicherry Engineering College
Puducherry, India
kalaidivi043@gmail.com

N. Sreenath
Department of Computer Science
and Engineering
Pondicherry Engineering College
Puducherry, India
nsreenath@pec.edu

A. Amuthan
Department of Computer Science
and Engineering
Pondicherry Engineering College
Puducherry, India
amuthan@pec.edu

Abstract—A Vehicular Networks are intelligent transportation system which provides data dissemination, and traffic management services. In VANETs, privacy is the major issue in safety-related application. It becomes a challenging problem to maintain the privacy of the vehicle and the user. To avoid linking of messages which is sent between the vehicles in the network, many privacy schemes utilizes pseudonym changing mechanism. But the beacons containing spatiotemporal information makes the vehicle vulnerable to attacks and privacy is breached. Hence, preserving the context of privacy is a major challenge in the vehicular network. In order to enhance the privacy, mix zone is considered as the optimal method among pseudonym changing mechanism. The mix zones are created by multiple numbers of vehicles that concurrently change their pseudonym to admit uncertainty to the malevolent competitors such that it turns into inaccessible for them to extract the cooperation between the current and former pseudonyms employed by the vehicles. This paper reviews various pseudonym strategies and mix zone schemes for privacy preservation.

Keywords—ITS, Security, Location privacy, Pseudonym, VANETs

I. INTRODUCTION

The vehicles are connected as nodes which form a network called Vehicular networks (VANETs). The vehicle in the network communicates each other through on-board-unit (OBU) and with infrastructures through road-side-unit (RSU) as shown in Fig 1. Broadcasting communication in the vehicle is of two distinct types (i.e.) naïve broadcasting and intelligent broadcasting. VANETs provides safety and non-safety related applications. The major components in VANETs are on-board-unit (OBU) which is mounted in the vehicles, roadside unit (RSU) which is in the roadsides and Trusted Third Party (TTP) which enables an effective communication between driver and the roadside infrastructure, as depicted in Fig 2. Each vehicle is provided with On-Board unit, collects the data from the various sensors fitted inside the vehicle and sends the collected information such as the location of the vehicle, vehicle acceleration, deceleration, and speed to the other vehicles [1].

978-1-5386-8260-9/19/$31.00 ©2019 IEEE

RSU has installed at the roadsides and infrastructure acts as an access point for OBUs which transmits road-safety application messages, traffic warnings. A Trusted Third Party (TTP) consists of a trusted management with acceptable computational memory and cache systems. To receive a certificate from TTP, all the vehicles in the network should register by using its id for vehicular management. There are separate TTP for each signature is used in geographical location. Before performing the communication between vehicles, all the interacting vehicle and roadside units should complete the registration process with a trusted third -party.

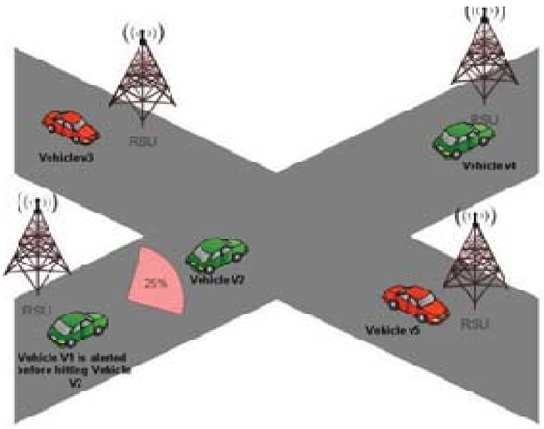

Fig 1: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication

The trusted third-party controls roadside units and its infrastructures are fixed on the roadside location. Roadside units are not fully trusted since it is easily vulnerable to attacks.

II. PRIVACY

A. Privacy:
   Privacy is the ability of preserving a confidential information from an illegitimate individual.

In VANETs, preserving the original id of the interacting vehicle from other vehicles and roadside units. [3].

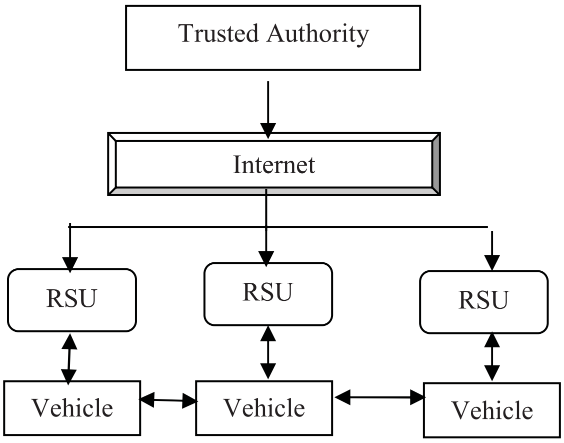

Fig 2: System Architecture in VANET

B. Location Privacy

Location privacy is the capability of preventing from an unauthorized person knowing the present and past location of the interacting vehicle in the network [4]. The present and past location of the interacting vehicle in the network can be identified through tracking of the vehicle.

The Mechanisms to solve the location privacy issues are,

- Pseudonyms
- K-anonymity
- Group signature
- Silent period
- Mix-zone

The Pseudonyms: Pseudonymity terminology was first proposed in [3], where the attacker intercepts the communication between sender and receiver to know what they are communicating. The pseudonym is the unique id which authenticates the sender messages.

k-anonymity: The level of the location privacy is measured by using the following metrics such as k-anonymity, I-diversity, and road segment s-diversity [26]. The k-anonymity protects the location privacy of the user by providing an obfuscation area which includes his spot and the location of k-1 other users [27]. Since k-anonymity does not handle homogeneity and background knowledge attack, l-diversity was introduced by A. Machanavajjhala [28]. The idea of this approach is that it uses Bayes-optimal privacy which is susceptible to homogeneity and background knowledge attack even the attacker knows the background knowledge of the user.

Group signature: For securing and preserving privacy, group signature scheme is proposed by Chaum et.al [28]. In this method, the members in each group can sign and verify a message using their public and private keys. GSIS and TACKing protocols provide handover to permit OBU for modifying the private and public keys periodically. Compared to GSIS protocol, TACKing offers fast handover.

Silent periods: Privacy enhancing mechanism in location based-services is silent period presented in [29].In this approach, the user will not change pseudonyms for certain amount of time in order to provide unlinkability between old and new pseudonyms. Since, the user does not use location-based services, the quality of service gets degraded.

Mix-zone model: To provide unlinkability between old and new pseudonyms a technique called mix-zone was proposed by R. Beresford [10]. A mix-zone is a region where k number of users enter the region in some order modify their pseudonyms and exit the region in different to provide unlinkability. To guarantee privacy the following assumptions are ensured in mix-zone model,

- A mix-zone region should consist of k no of participants must arrive the region before any participant leave the region.
- Each participant inside the region spends arbitrary interval of time since they arrive and leave the region in different entry and exit point.
- The uniform distribution is followed in probability of transition

Mix-zone construction techniques: Considering the protection of location privacy for mix-zones, time window-based approaches are presented in [30]. For constructing effective mix-zones, three construction strategies developed based on the mix-zone model. First, in the time window bounded approach, the rectangle is defined in some default size at the centre of the road junction. In this approach, an anonymity set is formed based on the assumption that within the time interval the number of users entering the mix-zone. The chosen time interval should be small value. The factors such as size of the zone, anonymity level and speed of the users are considered for defining the size of the window. Second, in the TWB shifted Rectangular Mix-zones, the rectangle is defined in shifted way. Third, in the TWB Non-Rectangular mix-zones, the size is defined in non-rectangular way. This approach is free from timing attack since it uses non-rectangular way.

Attacks in mix-zone: In recent years, two major types of attacks in location privacy for mix zones is presented in [31]. The combined timing and transition attack occur when the attacker have the knowledge of timing information and transition probabilities about the users inside the mix-zone region. The attackers find the mapping between entry and exit point of user by using the timing knowledge of the user. The continuous query correlation attack occurs when the participant of the mix-zone region receives continuous query services through mobiles. Whenever the participant performs continuous query, the repeated snaps of the query are utilized for finding the mapping between the old and new pseudonyms.

III. LOCATION PRIVACY PRESERVATION USING MIX ZONE

The Privacy preserving mechanism changes the state of the information before being addressed by the attacker to protect location privacy. Location privacy preservation mechanism primitives are hiding events, adding dummy events, obfuscation and anonymization. In hiding events, the information about the path of the users are hided and the event are mapped with different timings. In adding dummy events, additional events or the events of a normal user are added. In obfuscation, the noise is added with the location information. E.g. Spatial cloaking and Temporal cloaking. In anonymization, the exposure of the user identity is protected by unlinkability between the location and the user identity. Anonymization can be achieved by means of Pseudo identifiers or pseudonyms, Mix zones, Group signatures, Silent periods [9].

Users register their interest in application zone to receive updates regarding the updates of the registered events. This help the user to know the updated information about products. But when user communicates directly with the application, the location can be easily traced. Middle ware communication between vehicle and application does not allow the vehicle to directly connect the network with the vehicle. R. Beresford et al proposed the method called Mix zone [10]. Mix zone is a region where the vehicle mixes with the unregistered vehicle which does not have any application call back. A Mix network is a store and forward network which facilitates anonymous communication. The messages are reordered by some metrics before transmitting them. So, the relation between the sent and received messages are unlinkable. Mix zone techniques are of different types which are used to preserve the location privacy of users. Effectiveness of the mix zone depends on factors such as mix zone geometry, population of users, spatial and temporal resolution and spatial constraints in road networks. In mix zone, the mapping of the location with the vehicle identities should not be done since the vehicles are not connected with the location-based services and they do not have any application call back. When a people communicate directly with the application that identity can be easily identified. To protect the identity of the user, a middleware is used as an intermediary one for communication within the vehicle and the application. The usage of middleware makes the information confidential and the identity of the user are not revealed. When a user changes pseudonym in normal traffic environment, his old and the new pseudonyms are easily linked. Whenever a user changes pseudonym in mix zone, the user identity cannot be linked with the location i.e. unlinkability can be achieved.

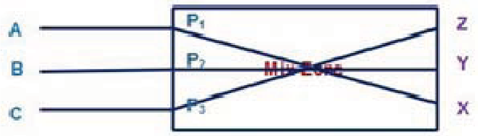

Fig. 3. Mix zone model

Fig 3 discusses on pseudonym changes in mix zone. Three vehicles A, B and C enter mix zone with pseudonym p1, p2 and p3. When the vehicles leave the mix zone it changes its pseudonyms to X, Y and Z. When the entry and exiting time of all the vehicles are same then attacker can able to map the pseudonym and find the identity of the vehicle. Mix zone will be effective when the vehicle spends random time inside the mix zone.

In [11], a Beresford et al refined the mix zone model with quantifiable metric from the attacker point of view. When a user directly accesses the application, the user's location can be easily tracked. Instead of directly accessing the application, the user can use the middleware system to access the application. This can prevent the user from finding their location. Beresford discussed a boundary line which is the border between the mix zone and the application. Considering the entry points and exit points of vehicle, attacker can able to trace the vehicle. By changing pseudonyms, long-term user movements are protected from the attacker.

Mix zones can be created by different techniques such as anonymization, cryptography and changing pseudonyms. Even the attacker uses the middle ware for communication, the attacker can able to trace the identity of the vehicle since the messages transmitted are open. For this, J. Freudiger et al proposed [12] Cryptographic Mix zones (CMIX Protocol). The legitimate users inside the mix zone get the symmetric key from the RSU of the mix zone and encrypt all the messages using this key. Key forwarding mechanism is used for obtaining the key and key update mechanism update the old keys if it is expired. To achieve unlinkability mix networks and mix zones are combined. Mix networks can be obtained by combining all the mix zones. By encrypting the messages can be transferred between the vehicles the location information is prevented from tracing. The CMIX are vulnerable to internal attackers because the messages are encrypted using a group secret key.

To overcome this issue,[13] A. M. Carianha et al improved the location privacy of mix zones by extension to the CMIX protocol. Whenever the user encrypts the message using group secret key, authenticated internal attacker can have access to status information of all nodes in the network. Whenever user wants to know about the status of a vehicle it requests the RSU. RSU gets the status of the vehicle requested and decrypts the status information. Privacy can be breached by means of status information. So, all the information except status of the system are encrypted using secret key. Finally, it forwards to the requested vehicle by encrypting the information using private key. Thus, status information of a vehicle is preserved by extension of CMIX. Based on the traffic density, the mixing effectiveness of vehicle can be improved. J.-H. Song et al proposed Density-based Location Privacy (DLP). Using DLP [14], location privacy can be achieved by considering the neighboring vehicle density as a threshold to change pseudonyms. With the delay information, the attacker can able to track the vehicle using selection rule. Each vehicle listens to other vehicles beacon messages for vehicle count. When there is no link between neighboring vehicle or the vehicle is lost then count of neighboring vehicle decreases by 1. If it is present, then the count increases by 1. Pseudonyms are changed only when there are at least k-1 neighboring vehicles. This scheme is more efficient than AMOEBA with random silent period. Mix zones are formed static in DLP. B.

Ying et al proposed Dynamic Mix zone Location Privacy (DMLP) [15], which form Mix zones dynamically at the required time.

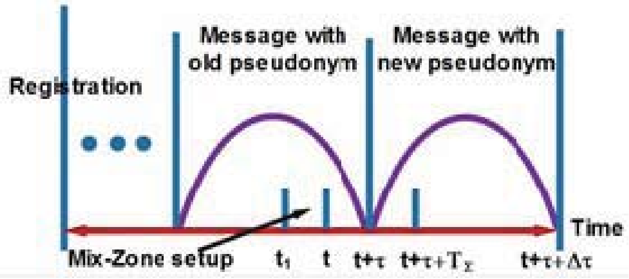

Fig. 4. DMLP Process

In [15], Fig 4 DMLP Process are discussed which involves registration, mix zone setup, encryption and signature. In registration phase, the vehicle registers with the trusted authorities using authentication methods like Kerberos. In mix zone setup phase, mix zone are setup by changing the expired pseudonym with the request message of new pseudonym. After receiving the command message, vehicle sends the encrypted safety messages in encryption phase. In signature phase, the vehicle signs safety messages with public or private keys.

The road network constraints are not considered in Mix zones. B. Palanisamy et al proposed Mobimix, a road network-based framework which preserves the location privacy of users. Some of the factors for effective mix zone construction are: geometry of the mix zones, spatial population of users, spatial and temporal resolution and spatial constraints on road networks. With the consideration of these factors from [16], Mobimix provides effective Mix zone construction. Features of the Mobimix model involves: a formal analysis of vulnerabilities on applying theoretical mix zones, developing mix zone model, mix zone construction approaches, developing attack resilient mix zones and placement of the mix zones. In theoretical mix zones some rules are defined and applying these on road network involves some constraints. Road networks have spatial and temporal constraints. Distribution in VANET can be classified into random distribution and uniform distribution. Random distribution in road networks will have stronger unlinkability. So, to achieve stronger unlinkability, the vehicle should spend random time period inside the mix zone. B. Palanisamy considers the timing and transition attacks and analyses the performance of mix zones construction techniques. Mix zone placement is a NP- hard problem.

J. Freuidger et al [17], proposed a novel based metric to analyse the mixing effectiveness of possible mix zone locations. Optimal Mix zone placement can be analysed with combinatorial optimization techniques. Freuidger defines mix zone is a region of predetermined shape and size, which can be established at any place. The mixing effectiveness of mix zones are found before deploying mix zones with flow-based metric. It theoretically evaluates the mixing effectiveness. Mix zones are placed with optimization to maximize the overall probability of attacker tracking mobile nodes with cost and traffic constraints.

In [18], Liu X et al propose a new metric to make the system resilient to inferential attack. The attacker can able to track the users by means of side information i.e. inferential attack. Multiple mix zones are placed to preserve the location privacy of the users. Since Mix zone placement is a Np hard problem, two optimization algorithms are used which is based on the mix zone uniformity. Uniform traffic mix zone placement algorithm is used when the user does not have any knowledge about the traffic. Non –uniform traffic mix zone placement algorithm is used. When the user has some knowledge about the traffic.

Suguo Du et al. proposed a location privacy prevention approach which enables the vehicle to generate a signed message to enhance the level of the location privacy. Also, the reputation is given to the interacting vehicles in the network based upon the behavior of the vehicles to increase the co-operation level [19]. [20] Boualouache et al. proposed silence and swap an approach for changing pseudonym at road intersections. This approach uses two protocols in which one allows the vehicles to change pseudonyms based on roadside units while the other aims at securing mix zones [20]. To mitigate selfish vehicles in the network, a motivation-based approach is proposed [21]. This approach provides incentives to the vehicles during the process of pseudonym change in order to motivate the interacting vehicles and also to avoid the selfish vehicles.
Boualouache et al. proposed an approach to prevent linking attack by considering the impact of density of the vehicles and no of pseudonym notifications during the mix zone formation. [23]. To sustain unstable density of the vehicles a virtual-based mix zone approach is proposed [22].

IV. CONCLUSION

VANETs have emerged as a new ad-hoc network allowing for the V2V and V2I communication. VANET enhances the road safety for the user, infotainment dissemination for driver and passenger. In the wireless communication medium, vehicles are prone to many types of threats and attacks. Therefore, securing VANETs is a great challenge compared to another network. This paper deals with the review of various pseudonym strategies and mix zone establishment techniques for privacy preservation.

REFERENCES

[1] S.Mathews and Y. B. Jinila, "An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet," in Electronics and Communication Systems (ICECS), 2014 International Conference on. IEEE, 2014, pp. 1–6.

[2] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.

[3] A. Pfitzmann and M. Kohntopp,¨ "Anonymity, unobservability, and pseudonymity a proposal for terminology," in Designing privacy enhancing technologies. Springer, 2001, pp. 1–9.

[4] F. Dotzer, "Privacy issues in vehicular ad hoc networks," Lecture notes in computer science, vol. 3856, pp. 197–209, 2006.

[5] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Hpdm: A hybrid pseudonym distribution method for vehicular ad-hoc networks," Proce-dia Computer Science, vol. 83, pp. 377–384, 2016.

[6] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym schemes in vehicular networks: A survey,” IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228–255, 2015.

[7] R. S. Raw, M. Kumar, and N. Singh, “Security challenges, issues and their solutions for vanet,” International Journal of Network Security & Its Applications, vol. 5, no. 5, p. 95, 2013.

[8] A. Khandelwal and S. Harit, “A comparative analysis of privacy preser-vation techniques through pseudonyms in vanet,” Imperial Journal of Interdisciplinary Research, vol. 2, no. 5, 2016.

[9] R. Shokri, J. Freudiger, and J.-P. Hubaux, “A Unified Framework for Location Privacy,” no. July, pp. 1–19, 2010.

[10] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, 2003

[11] A. R. Beresford and F. Stajano, “Mix zones: User privacy in location-aware services,” Proc. - Second IEEE Annu. Conf. Pervasive Comput. Commun. Work. PerCom, pp. 127–131, 2004.

[12] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, “Mix-Zones for Location Privacy in Vehicular Networks,” ACM Work. Wirel. Netw. Intell. Transp. Syst., 2007.

[13] A. M. Carianha, L. P. Barreto, and G. Lima, “Improving location privacy in mix-zones for VANETs,” Conf. Proc. IEEE Int.Performance, Comput. Commun. Conf., 2011.

[14] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, “Wireless location privacy protection in vehicular Ad-Hoc networks,” Mob. Networks Appl., vol. 15, no. 1, 2010.

[15] B. Ying, D. Makrakis, and H. T. Mouftah, “Dynamic mix-zone for location privacy in vehicular networks,” IEEE Commun. Lett., vol. 17, no. 8, pp. 1524–1527, 2013.

[16] B. Palanisamy and L. Liu, “Attack-resilient mix-zones over road networks: Architecture and algorithms,” IEEE Trans. Mob. Comput., vol. 14, 2015.

[17] J. Freudiger, R. Shokri, and J. P. Hubaux, “On the optimal placement of mix zones,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5672 LNCS, pp. 216–234, 2009.

[18] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, “Traffic-aware multiple mix zone placement for protecting location privacy,” Proc. - IEEE INFOCOM, pp. 972–980, 2012.

[19] Suguo Du, Haojin Zhu, Xiaolong Li, Ota, K., &Mianxiong Dong. (2013). MixZone in Motion: Achieving Dynamically Cooperative Location Privacy Protection in Delay-Tolerant Networks. IEEE Transactions on Vehicular Technology, 62(9), 4565-4575.

[20] Boualouache, A., & Moussaoui, S. (2014). S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs. 2014 International Conference on Advanced Networking Distributed Systems and Applications, 1(1), 78-85.

[21] Ying, B., Makrakis, D., & Hou, Z. (2015). Motivation for Protecting Selfish Vehicles' Location Privacy in Vehicular Networks. IEEE Transactions on Vehicular Technology, 64(12), 5631-5641.

[22] Boualouache, A., Senouci, S., & Moussaoui, S. (2016). VLPZ: The Vehicular Location Privacy Zone. Procedia Computer Science, 83(1), 369-376.