ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 146

2nd International Conference on Artificial Intelligence: Technologies and Applications (ICAITA 2018)

Modelling and Simulation on Location Privacy Preserving Based on Dynamic Periodic Pseudonym

Depei Wu[1], Xinling Zhou[2] and Lei Peng[2,*]

[1]Shenzhen Hangsheng Electronic Co. Ltd, Shenzhen 518055, Guangdong Province, China

[2]Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, Guangdong Province, China

[*]Corresponding author

***Abstract*—The location-aware privacy preserving is the key issue to connected vehicles, since they share many traffic information when driving, which possibly leak their location privacies at the same time. In this paper, we propose a novel method of dynamic periodic pseudonym (DPP) improve the location privacy security without loss of location precision, via breaking the link between vehicle's identity and real-time location. The main idea of DPP is that vehicle can change the pseudonym at appropriate time when the calculated privacy leak probability beyond the predefined threshold, overcoming the weakness of constant period of changing pseudonym. In this paper, the privacy leak probability is modelled as gamma distribution, and convolute with the constant pseudonym period, to achieve the effect of adaptive changing. Finally, the simulation shows the effectiveness of the DPP under the different privacy leak environment.**

Keywords—location-ware privacy preserving; gamma distribution; dynamic periodic pseudonym; vissim

I. INTRODUCTION

With the rapid development of automotive electronics, network and information technology, intelligent connected vehicles (ICV) have become the development trend of Automotive Technology. A combination of computation devices, sensors, real-time control and communication networks enables V2X communication, covering the communications between vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-pedestrian and son on [1], this allows highly automated driving and cooperative response to traffic conditions. ICV can improve traffic efficiency, reduce pollution, and mitigate car accidents. As a vital role in Intelligent Transport System (ITS), connected vehicles are used to collect and share roadway state information, including parking spaces, congestion points and so on. However, the precise location and identity contained in sharing information will expose the vehicular track and other sensitive information, it thus becomes feasible for adversary to keep track of vehicular movements by collecting the sharing information. Even more, adversary can further reveal the driver's very private information (e.g, hobbies, home address, health status) through the spatio-temporal analysis of these positions. Therefore, it's the key issue for precise location sharing system to solve the privacy disclosure.

Many strategies of privacy protection have been proposed, mainly including pseudonym technology and location hiding technology. Pseudonym technology [2] [3] is a promising way to protect the vehicular identity. In order to break the link between identity and location, fake identity is used to replace the real identity when sending information. Vehicle changes the pseudonym from time to time to avoid the tracking of their positions. Sam et al. [2] proposed the strategy that pseudonyms were generated by oneself and changed at the road intersection. The most representative pseudonym technology is confusion region technology. The scheme of mixed zone is proposed [3], pseudonym only changes in the defined area. Location hiding technology mainly utilizes the algorithm to hide the precise location, a false location is used to replace the real location [5], such as the iconic representative position. As well as the position generalization [6], location suppression [7] and other technologies are proposed. The attacker can't get the precise location information. The most representative location hiding technology is the K-anonymous. Sweeney [4] proposed the fuzzy area, which was generated with anonymous algorithm to replace the real precise location. The fuzzy area contains at least K mobile units in a certain location area, which makes it difficult to distinguish the accurate location of a particular mobile unit.

Due to the mobility and flexibility of vehicle, the privacy protection agreement must deal with these dynamic changes. Because accurate location is required, the false location and other location hiding technologies are not feasible, which will blur location information. The long-term pseudonym is not enough to protect vehicular privacy. Once the pseudonym is linked to the true identity through inference attack, the vehicular entire trajectory is exposed. In this paper, we use dynamic pseudonym technology to achieve vehicular privacy protection. The vehicular security can't be guaranteed by using periodical pseudonym changing strategy, since the vehicular privacy may largely leaked before the pseudonym constant period T. Considering the weakness of periodical pseudonym changing, we propose a scheme of dynamic periodic pseudonym (DPP), and we show the effectiveness of our method by simulation.

The rest of this paper is organized as follows. In Section II we describe some related work. DPP scheme is introduced in Section III. In Section IV we present simulation, the simulation results show the effectiveness of our scheme. Conclusion is given in Section V.

II. RELATED WORK

Pseudonym technology is widely used to protect the identity and location privacy. As early as 1981, the pseudonym strategy had been raised by Chaum [10]. However, long-term pseudonym make it easy for adversary to link the real identity and pseudonym with auxiliary information [12] [13]. Ma et al. [12] demonstrated that the attacker who had a small amount of auxiliary information can associate true identity with long-term pseudonym. Mudhakar et al. [13] pointed out that an adversary can effectively perform pseudonym attack if there are readily available side information.

In view of the shortcomings of the long-term pseudonym, a variety of effective pseudonym changing strategies have been proposed. Zhu et al. [9] proposed a dynamic pseudonym mechanism, pseudonyms and pseudonym certificate sets are generated by the trusted institutions. The valid period of each pseudonym is stable time T and pseudonym cyclical changes. The concept of silent period is adopt in [14-16]. The silent period is a time period or a region. During the silent period, sending information is not allowed. Pseudonym changes in the silence period to avoid the attacker's tracking. There is also a strategy of mixed zone for Pseudonym changing. Beresford et al. in [2] proposed pseudonym changing in the mixed zone. The region is divided into ordinary communication area and mixed zone, like the silent period method, sending information is not allowed in the mixed zone, pseudonym must be changed before vehicle leaves the mixed zone. The shortcoming of the silent period and the mixed zone is the restriction of sending information, which may not meet with the requirement of real-time service and sharing information in time [8], the uniform mixed zone setting can't meet individual needs.

The cooperative strategies of pseudonym changing are also proposed by the researchers. The mobile node simply sends a pseudonym changing request to its neighbor nodes, and then forms the dynamic zone with the neighbor nodes to change pseudonym [17]. Mingyan et al. [18] proposed the dynamic mixed area provided by the control server, the server informs the vehicle to enter the mixed area, vehicles change pseudonym at the mixed area. But the cooperation of vehicles is the key factor in the successful pseudonym changing strategy. Selfish vehicles tend to do not change their pseudonym if they reach the desired privacy level. The vehicle refuses to cooperate with other vehicles while changing the pseudonym [11], which results in reducing the privacy protection level.

Unlike aforementioned strategies, our DPP strategy can adaptively change pseudonym with the vehicular privacy disclosure.

III. MODELLING ON DPP

In this section, we introduce the DPP strategy with three parts. 1) system model; 2) the method of the pseudonyms generation; 3) the method and algorithm of DPP strategy.

A. System Model

The location sharing system in ICV is mainly composed of vehicle units, servers and trusted institutions (TA). Vehicle is equipped with a variety of sensors to collect information, and the precise locations are provided by the vehicle's global positioning system (GPS). The vehicle unit can communicate with TA and server via 3G/4G or WiFi signals. TA in this system is completely credible, which is responsible for the registration of vehicle and server. The vehicle can request pseudonym sets and certificate sets from TA. As well as TA can revoke malicious vehicle with the revocation module. The server receives the sharing information from vehicle and determines whether to accept the information after verifies the correctness of the vehicular identity and the integrity of the information.

The security sharing model is mainly achieved in the vehicular system. A sending information from vehicle can be represented with a triplet (ID, l, t), ID represents the identity of the vehicle, l indicates the vehicular precise location, timestamp t is the moment of information sending. This triplet indicates that the vehicle is in l location at moment t. Collecting a series of information can get the vehicular travel trajectory.

The ID should be changed to protect the privacy in the security sharing model. Based on the existing periodical changing pseudonym scheme, the vehicular system periodical changes the pseudonym. This model can be represented by a set equivalent formula

$$f_n(x) = \frac{p}{T}(x\%T) \tag{1}$$

where P is the threshold of privacy disclosure, this formula represents the result of the pseudonym changing with fixed period T. Figure 1 shows the equivalent mode.

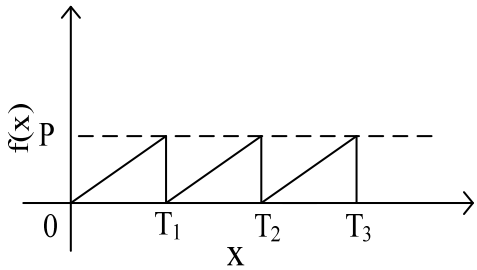

FIGURE I. EQUIVALENT MODEL OF PERIODICAL PSEUDONYM CHANGING FOR VEHICLE SYSTEM

B. Pseudonym Generation

In order to hide the vehicular identity, we adopt the pseudonym strategy. Pseudonyms generation can rely on TA, as well as can be generated in their own vehicle system. In this paper the pseudonyms in DPP are provided by TA [9]. Before the travel, driver applies for the pseudonym set and the corresponding pseudonym certificate set from TA, and then

stores them in the vehicular safe location, the vehicle uses the multiple pseudonyms to send information to server.

C. DPP Scheme

Using pseudonyms is an effectively way to break the link of identity and location. But the vehicular security is not guaranteed by using periodical pseudonym changing strategy, if the vehicular privacy has been largely leaked before the pseudonym inherent period T. The scheme of DPP is proposed to protect the vehicular privacy. During one pseudonym period, the vehicle system decides the appropriate time to change pseudonym on the impact of privacy disclosure. The vehicle system immediately changes the pseudonym, if the vehicular privacy disclosure has reached the threshold before T.

Vehicle randomly shares information during a pseudonym period, the number of sending information and the sending interval time will result in difference of vehicular privacy disclosure. We set the function g(x) to represent the vehicular privacy disclosure. The Gamma distribution is a classical continuous probability function that represents statistics proposed by Euler, and has been widely used in analysis, probabilistic, partial differential equations and combinatorial mathematics. We use the gamma distribution function to measure the vehicular privacy disclosure. g(x) can be expressed as (2)

$$g(x)=\int_0^t \frac{e^{-\frac{x}{\beta}}x^{\alpha-1}}{\beta^{\alpha}\Gamma(\alpha)}dx \tag{2}$$

where α is information sending counts that will lead to the leak of the real identity. β is the interval time for sending information.

Vehicular privacy disclosure has an impact on valid period of the pseudonym. The convolution function describes the interaction of two functions. Therefore, the convolution function sets to y(x), it can be used to measure the impact of privacy disclosure on the valid period of the pseudonym. During one pseudonym period, the equivalent formula of periodical changing pseudonym can be represented as (3), the privacy disclosure g(x), which is used as an activation function of convolution, is convoluted with f(x) as (4)

$$f(x)=\frac{p}{T}x \tag{3}$$

$$\begin{aligned} y(x) &= f(x)*g(x) \\ &= \frac{P}{T}x*\int_0^t \frac{e^{-\frac{x}{\beta}}x^{\alpha-1}}{\beta^{\alpha}\Gamma(\alpha)}dx \\ &= \int_0^t \left(\frac{P}{T}\tau\times\int_0^t \frac{e^{-\frac{x-\tau}{\beta}}(x-\tau)^{\alpha-1}}{\beta^{\alpha}\Gamma(\alpha)}d(x-\tau)\right)d\tau \end{aligned} \tag{4}$$

During one pseudonym period, if the vehicular privacy leak reaches the privacy disclosure threshold, the system immediately changes the pseudonym. If not, the system keeps the pseudonym until T expires.

IV. SIMULATION

In this part, in order to evaluate the effectiveness of the proposed scheme, we performed a set of simulation. Vissim is an effective tool for simulation and modeling of traffic scenes. Vissim9 is used as a simulation platform to simulate the process of sending information during vehicle moving. In Vissim software, simulation scenario represents Shenzhen Science and Technology Park Area which is the rectangle area of <113.95856,22.538184> to <113.951883,22.544059>. The number of vehicles traveling in the set area is set to 500, and the vehicle sends precise position information during traveling.

FIGURE II. SCREEN SHOT OF THE SIMULATION IN VISSIM

The number of sending information and the sending interval time will result in difference of vehicular privacy disclosure, and vehicular privacy disclosure has an impact on validity period of the pseudonym. That is to say, the sending information counts and the sending interval time will cause the difference of the pseudonym changing time. We set two parameters for simulation: α and β. α is the information sending counts that will lead to the leak of the real identity, β is the interval time for sending information. In order to observe the impact of two parameters on the pseudonym changing time, we assume that the vehicular pseudonym constant period T is 5 minutes, the vehicular privacy disclosure threshold is 1 in the experiment.

We evaluate the privacy disclosure and pseudonym changing time provided by parameter β. In Figure 3, the impact of β on the privacy disclosure is showed, the simulation result indicates the vehicular privacy disclosure gradually increase over time. The little privacy is leaked when sending interval time is small. Figure 4 evaluates the impact of parameter β on pseudonym changing time. When sets α=4, β=0.5, the vehicular privacy disclosure has reached the privacy disclosure threshold about at the moment t=3.3, therefore the system should change pseudonym at time t. When β=2, the privacy disclosure doesn't achieve threshold during the pseudonym period T, the system keeps the pseudonym until t=T. The simulation results in Figure 3 and Figure 4 indicates that the vehicular privacy is quickly leaked if sends information frequently, pseudonym should be changed in time. The vehicular privacy gets better protected with pseudonym changing at appropriate time. The simulation result indicates the effectiveness of DPP scheme.

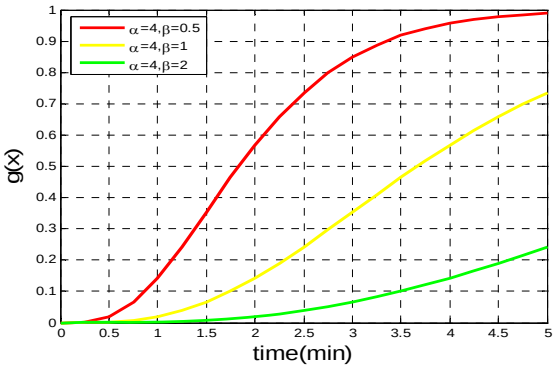

FIGURE III. THE IMPACT OF B ON THE PRIVACY DISCLOSURE

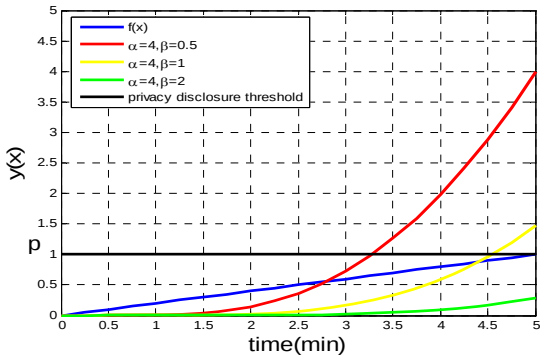

FIGURE IV. THE IMPACT OF B ON THE PSEUDONYM CHANGING TIME

V. CONCLUSION

Protecting the location privacy for intelligent connected vehicles when sharing accurate location has been considered as an important problem. In this paper, considering the weakness of constant period of changing pseudonym, a DPP scheme is proposed. We establish the model of privacy disclosure by Gamma distribution, and utilize the convolution algorithm to determine the moment of pseudonym changing based on the impact of the vehicular privacy disclosure. The simulation results indicates that the vehicular privacy gets better protected with pseudonym changing at appropriate time. As the future work, we will provide a show of the effectiveness of this strategy in real scene.

REFERENCES

[1] Zhu, Z., et al. "Recent advances in connected vehicles via information-centric networking." Iet International Conference on Intelligent and Connected Vehicles IET, 2017.

[2] Sam M. M, N. Vijayashanthi, and A. Sundhari. "An Efficient Pseudonymous Generation Scheme with Privacy Preservation for Vehicular Communication." International Conference on Intelligent Computing Applications IEEE, 2014:109-117.

[3] Beresford, F. Stajano. Location privacy in pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(1): 46–55.

[4] L. Sweeney. k-anonymity:A model for protecting privacy[J]. International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557–570.

[5] Shin H, Atluri V, Vaidya J. A Profile Anonymization Model for Privacy in a Personalized Location Based Service Environment[C]// International Conference on Mobile Data Management. IEEE Xplore, 2008:73-80.

[6] Xu T, Cai Y. Exploring Historical Location Data for Anonymity Preservation in Location-Based Services[C]// INFOCOM 2008. the, Conference on Computer Communications. IEEE. IEEE, 2008:547-555.

[7] Freudiger J, Shokri R, Hubaux J P. Evaluating the Privacy Risk of Location-Based Services[M]// Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2011:31-46.

[8] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in Vehicular Networking Conference (VNC), 2013 IEEE, Dec 2013, pp.71–78.]

[9] Xiaoyan Zhu, Haotian Chi, Shunrong Jiang, Xiaosan Lei, Hui Li.Using Dynamic Pseudo-IDs to Protect Privacy in Location-Based Services[J].Mobile and Wireless Networking Symposium,2014:2307-2312.

[10] Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–90, 1981.

[11] J. Freudiger, M. H. Manshaei, J.-P.Hubaux, and D. C. Parkes, "Non-cooperative location privacy," Dependable and Secure Computing,IEEE Transactions on, vol. 10, no. 2, pp. 84–98, 2013.

[12] Y. Ma, D. K. Yau, N. K. Yip, and N. S. Rao, "Privacy vulnerability of published anonymous mobility traces," in ACM MobiCom 2010.

[13] M. H. Mudhakar Srivatsa, Hawthorne"Deanonymizing mobility traces:using social network as a side-channel," in ACM CCS 2012.

[14] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung, "Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks," IEEE International Conference on Communications, 2009. ICC '09, pp.1-6, 2009.

[15] Krishna Sampigethya, Mingyan Li, Leping Huang, and Radha Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE Journal on Selected Areas in Communications, Vol.25, No.8, pp.1569-1589, 2007.

[16] Kanta Matsuura, Hiroshi Yamane, Kaoru Sezaki, "Enhancing wireless location privacy using silent period," IEEE Wireless Communications and Networking Conference(WCNC 2005), pp.1187-1192, 2005.

[17] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," Proc. Fifth ACM Workshop Privacy in Electronic Soc. (WPES), 2006.

[18] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," Vehicular Technology, IEEE Transactions on, vol. 64, no. 12, pp. 5631–5641, 2015.