Network Location Privacy Protection Based on Game Theory

Ya-feng FAN*, Hong-yue LIU and Wei-dong YANG

Henan University of Technology, Zhengzhou, Henan, China

*Corresponding author

Keywords: Car networking, Privacy protection, Privacy metrics, Game theory model.

Abstract. The purpose of this paper is to protect the privacy of vehicles and passengers. In recent years, with the rapid development of vehicle networking, the location privacy of vehicle networking involves sensitive information about vehicles as well as passengers. It is of great theoretical and practical significance to put forward the privacy protection of vehicle network location. This paper is based on identity concealment, fuzzy method, cryptography and information theory. The goal is to fully protect the privacy of the vehicle's networked location. Using the technical methods of game theory as a means, and the mechanism of vehicle location privacy protection in typical applications and the game model of vehicle network attack and defense are studied. This paper introduces some common privacy protection methods, such as pseudonym transformation method, elliptic fuzzy method and so on. Establish the model and evaluation method of vehicle location privacy attack and defense strategy based on measurement. By analyzing the application scenarios, service quality and other factors and establishing the theoretical model of car network location privacy protection based on game theory, a privacy protection method based on game theory is proposed. The innovation of this paper is that the game theory is applied to the privacy protection of the Internet of vehicles. Thus, we can get the best guessing strategy of the enemy and the best privacy protection mechanism between location quality of service and privacy protection trade-off.

Introduction

At present, the technology of vehicle network privacy protection mainly includes false data method, inhibition method, generalization method and so on. False data method is used to anonymous or covert vehicle identity information through anonymous certificates, pseudonyms and group signatures. It can separate information such as vehicle identity from vehicle location and realize the purpose of privacy protection. The generalization method is to generalize the location information into the corresponding anonymous region, so that the attacker can not accurately obtain the real location, and achieve the purpose of location privacy protection. The generalization method mainly includes: location K-anonymity / locus K-anonymity, false position / false locus, etc. Fuzzy method is mainly used to improve privacy degree by reducing position accuracy. Common fuzzy techniques include empty fuzzy method, spatial coordinate conversion method and methods based on semantic fuzziness.

Research Status

Identity Hiding

Identity hiding can make vehicle identity information anonymous or covert through anonymous certificates, pseudonyms, group signatures, etc. Identity concealment realizes the purpose of protecting vehicle location privacy by disconnecting the relationship between vehicle identity and location.

The pseudonym scheme uses virtual identity information to replace the user's real information. This virtual information prevents an attacker from inferring the true identity of the user. Because the virtual does not contain information that the user can identify, so it can protect the privacy of the user. Pan et
al. proposed a pseudonym transformation that requires the cooperation of adjacent vehicles, which can be changed when vehicles meet. Pan et al. proposed a pseudonym transformation that requires the cooperation of adjacent vehicles, which pseudonym can be changed when vehicles meet. RPCLP and MPSVLP Kana transform methods proposed by Ying et al. \cite{2} By dividing the vehicle area dynamically, the mixed area is formed. The exchange of pseudonyms can be carried out between vehicles in the mixed zone; David et al. \cite{3} use synchronous time slot Kana Pool, limit storage overhead while maximizing the confusion of the attacker, against Sybil attacks and achieve a balance between vehicle privacy and traffic safety by means of a local pseudonym transformation.

The vehicles driving form a group in which any individual can sign anonymously. As a pseudonym for the whole group, this signature method is called group signature. This signature scheme not only implements anonymous authentication, but also can track specific vehicles; Zhao et al. proposed a group signature scheme based on remainder theorem, and then proposed a group signature scheme based on Schnorr algorithm. This scheme is an efficient and reversible group signature scheme; Then SCHECHTER et al. proposed the method of using ring signature to protect privacy; The ring signature solves the problem that once the public key keeper is breached, the member information will be leaked. This scheme enhances privacy protection.

**Generalization Method**

Generalization makes it impossible for an attacker to accurately obtain a true location by generalizing the location information to the corresponding anonymous region. The purpose of the generalization method is to protect the privacy of the location. The generalization method mainly includes: location K-anonymity / locus K-anonymity, false position / false locus, etc.

Vu et al. \cite{4} divide the user's location set into groups with at least k users in each group by using the hash function of sensitive position, and better protection of location privacy; Lin et al. \cite{5} proposed a location privacy clustering k-anonymity scheme. Users can adjust from time or space to meet the personalized privacy needs; Gurung and other \cite{6} propose an anonymous algorithm based on clustering. The algorithm publishes trajectory data with strict k-anonymity and avoid the problem of path inference. Al-Hussaeni anonymous the high-dimensional trajectory flow \cite{7} through a series of sliding windows to protect privacy. Zhang et al. \cite{8} proposed a method to protect privacy by protecting points of interest in a trajectory. To some extent, this method improves the problem of reducing data quality; Forster et al. \cite{9} use enhanced k-anonymity in traffic flow analysis applications and share vehicle trajectory data in the premise of ensuring vehicle privacy and data quality.

**The Fuzzy Method**

Fuzzy method is mainly used to improve privacy by reducing position accuracy. Common fuzzy techniques include spatio-temporal fuzzy methods, Spatial coordinate conversion method, and a method based on semantic ambiguity.

Ardagna et al. \cite{10} proposed a fuzzy method to replace the real location of the user with a circular region. One or two of the three fuzzy methods (magnification, reduction and translation) are used to generate a circular region satisfying the user privacy measure; Yigitoglu et al. \cite{11} extended the semantic location fuzzy model proposed by Damiani et al; Agir et al. proposed a privacy protection scheme for users by adjusting its parameters to meet the privacy protection requirements of personalized location; Han et al. adopted the algorithm of semantic space transformation (SST) which adopted different position information modification strategies according to different levels of privacy requirements. Later, there are Mix-zones technology, suppression method, encryption method and so on.

**Privacy Protection Method based on Game Theory**

Game Theory, also known as Game Theory, is a new branch of modern mathematics and an important discipline in operational research. Game theory has been applied more and more to the research of network security, privacy protection and wireless network which provides a mathematical tool for
their information security problems and analyze the complex multiplayer competitive behavior in the network. The research of game theory in network security mainly focuses on six aspects: Security of physical and MAC layers, security of self-organized networks, intrusion detection systems, anonymity and privacy, network security economics and cryptography. We can use the game theory and probability theory to establish the vehicle network location privacy framework model to evaluate the impact of attacker attacks and the effectiveness of the protection mechanism. The technical route of the study is shown in the figure. First, the privacy protection mechanism is modeled as a defender model. The defensive model and the attack model constitute the game participant model. Further, the attack behavior and protection mechanism are mapped to the set of participants' behaviors and policies. Then using the application scenarios and requirements to determine the number of participants and the purpose of the game, and then select a reasonable game model. For example, Stackelberg game model is used to compromise the quality of service and privacy protection. And Bayesian game model is used in privacy and security compromise scenarios. We use the basis of game theory to model the process of interaction between the attacker and the defender. At the same time, the quality of service can be solved, and The Nash equilibrium point under the constraint of privacy protection and the optimal defense strategy under the corresponding attack strategy are proposed.

Shokri et al. adopt the security game model of limited information to deal with the protection of personal location privacy. Players in the game are users, location service providers and adversaries, and The privacy protection framework is shown in the figure. The game process between the user and the enemy is dynamic, and the information they can observe on each other is limited. The process is to make the privacy protection strategy of location information by the user in order to ensure the quality of service in a certain location. Using reasonable privacy protection mechanism to minimize the accuracy of the enemy guess the user's exact location information. At this time, if the enemy obtained the user's location information, it is regarded as the loss of user income.

Figure 1. Location privacy protection framework.

The location privacy protection mechanism LPPM (location privacy protection mechanism) can solve the tradeoff between the quality of location service and the risk of privacy disclosure. The user policy in LPPM is to utilize a probability distribution \( \varphi (r) \) by replacing the user's real location information \( r \) with other false location information \( r' \). Or blur the user's actual location information to \( r' (\text{fake} \ r') \) and send fake \( < r', r' > \) to the location service provider to get the related location service. The enemy's attack strategy is to which used its own guessing mechanism to observed fuzzy position information \( r' \) to guess the user's location information \( \hat{r} \).Adversary strategy is recorded as hit \( < \hat{r} | r' > \).At this point, the user's game utility function can be described as:

\[
\text{Privacy}(\varphi, \text{false}, \text{hit}, dp) = \\
\sum_{r \in r} \varphi (r) \text{fake} < r' | r > \text{hit} < \hat{r} | r > d_p (\hat{r}, r) 
\]  (1)
The dp (\( \hat{r}, r \)) in the formula indicates that under the premise of the known user privacy policy and the opponent attack strategy. The enemy utilizes its attack strategy to obtain the influence of user location information on the user's real location privacy by observing and guessing.

In this game, the user wants to maximize the protection of their privacy information. However, the enemy wants the user to have the least degree of privacy protection. In order to solve the Nash equilibrium of the game. The user's expected return on privacy is:

\[
\Pr (r') \min_{\hat{r}} \sum_{r \geq 1} \Pr < r \mid r' > d_p (\hat{r}, r) = \min_{\hat{r}} \sum_{r \geq 1} \Phi (r) \text{fake} < r \mid r > d_p (\hat{r}, r) \tag{2}
\]

The expected benefits of the adversary are:

\[
\sum_{r \geq 1} \Phi (r) \max_{r \geq 1} \sum_{r \geq 1} \text{hit} < r \mid r > d_p (\hat{r}, r) \tag{3}
\]

Solution process specification of the Nash equilibrium point is a linear programming problem. The optimal solution of the game is obtained by solving the problem. That is, get the best guessing strategy of the enemy and the best privacy protection mechanism between location quality of service and privacy protection trade-off.

**Summary**

Location privacy in Internet of Vehicles relates to vehicles' and drivers' sensitive information. So how to protect the location privacy has become one of hotspots in both academia and industry. For fully and effectively protecting the vehicle's location privacy, the project uses game theory, information theory and cryptography to study a series of key questions involving unified location privacy metrics, game framework models and vehicles location privacy-preserving mechanisms in different applications of Internet of Vehicles, with the challenge of big data analysis attack. It is believed that the research results have great significance in both theory and practice for location privacy in Internet of Vehicles and mobile Internet.

**Acknowledgement**

This research was financially supported by the National Natural Science Foundation of China (Grant No.61772173), Natural Science Project of Education Department of Henan Province (No.14A520019), Natural Science Project of Science and Technology Department of Henan Province (Grant No.182102210388) and Open Project Foundation for Hebei Key Laboratory of Network and Information Security, the Basic Scientific Research Business of Provincial Universities Special Fund Project of Henan University of Technology (2015XTCX04).

**Literature References**

[1] Naghizade E, Kulik L, Tanin E. Protection of sensitive trajectory datasets through spatial and temporal exchange[C]. In: Proceedings of the 26th International Conference on Scientific and Statistical Database Management. ACM, 2014. 40.

[2] Wiedersheim, Bj, Ma Z, Kargl F, et al. Privacy in inter-vehicular networks: why simple pseudonym change is not enough[C]. International Conference on Wireless On-Demand Network Systems & Services. 2010:176-183.

[3] Palanisamy B, Liu L. MobiMix: Protecting location privacy with mix-zones over road networks[J]. 2011, 6791(4):494-505.
[4] Komishani E G, Abadi M, Deldar F. PPTD: Preserving personalized privacy in trajectory data publishing by sensitive attribute generalization and trajectory local suppression[J]. Knowledge-Based Systems. 2016, 94: 43-59.

[5] Ying B, Makrakis D, Mouftah H T. Dynamic Mix-Zone for Location Privacy in Vehicular Networks[J]. IEEE Communications Letters, 2013, 17(8):1524-1527.

[6] Tian F G X Z X. Privacy-Preserving approach for outsourced spatial data based on POI distribution[J]. Chinese Journal of Computer. 2014, 1(37): 123-138.

[7] Kong Q, Lu R, Zhu H, et al. A Secure and Privacy-Preserving Incentive Framework for Vehicular Cloud on the Road[C]. In: IEEE, 2016. 1-6.

[8] Lin X, Lu R. Vehicular Ad Hoc Network Security and Privacy[M]. Wiley-IEEE Press, 2015.

[9] Yang W, He Y, Sun L, et al. An optimal query strategy for protecting location privacy in location based services[J]. Peer-to-Peer Networking and Applications. 2016, 9(4): 752-761.

[10] Ying B, Makrakis D, Hou Z. Motivation for Protecting Selfish Vehicles' Location Privacy in Vehicular Networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(12):1-1.

[11] Yang W, Gao Z, Wang K, et al. A privacy-preserving data aggregation mechanism for VANETs[J]. Journal of High Speed Networks. 2016, 22(3): 223-230.