

Overview of Privacy Protection Based on System Architecture in Mobile Social Networks

Zhuohong Zhang

Guangdong University of Science and Technology, Dongguan, 523083, China

Abstract

In recent years, with the rapid development of mobile social networks, people's daily life is increasingly dependent on location services, and security issues for location privacy have become more and more difficult. This article summarizes three privacy protection methods based on the system architecture, including a single privacy protection processor method based on the three-level system architecture, and second-time anonymization of user data through a third-party processor. The multiple privacy protection processor method based on the four-level system architecture verifies the user's identity through the security center, increases the number of privacy protection processors, and solves the system bottleneck. The differential privacy protection method based on the distributed architecture meets the anonymity needs of users' location information by balancing performance and space efficiency. Finally, according to the current research problems, put forward their own research ideas and solutions.

Keywords

Distributed architecture; Three-level system architecture; Privacy protection processor; Security center.

1. Introduction

With the development of mobile technologies such as smart phones and the rise of mobile social networking platforms, people's lifestyles have undergone tremendous changes. However, the convenience is also accompanied by many security issues. For example, when the GPS positioning function is turned on when taking a taxi online, the user needs to provide the real location information to the service provider, and the third-party service provider provides specific services. The location information cannot be deleted by the user, and the user cannot prevent a third-party service provider from analyzing its movement track based on the location information provided by the user or the user's real location information is intercepted by malicious attacks. For this type of location information leakage, certain precautions must be taken to protect privacy. This paper summarizes the protection methods of location privacy in some location services [1], and puts forward practical research ideas and solutions at the same time.

2. Single Privacy Protection Processor

2.1. Overview

Machanavaj jha la et al. [2] proposed the idea of diversity and anonymity. The location information released by users contains k sets of simulated fake data, and each set of simulated data contains a different sensitive attribute value to reduce The probability of sensitive attributes being attacked can reduce the accuracy of location information and enhance the anonymity of location information in this way. However, the user's location information has passed through at least three stages from the sending to the receiving of the client, the location

server, and the service provider. If the service provider is not trustworthy, the anonymous location information on the client cannot be a good protection.

To solve this problem, Gong Linxia et al. [3] proposed a new anonymous technology based on location privacy. The user performs the first level of anonymity on the client, and the location information is sent to the privacy protection processor for the second level of anonymity. Ensure the security of the client and server. Its location privacy protection architecture is shown in Figure 1.

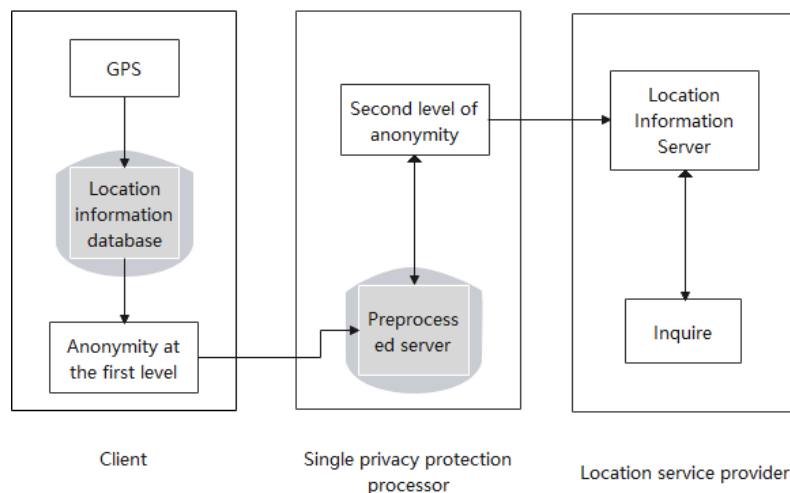


Figure 1. Location privacy protection architecture

The process of client privacy protection is as follows:

- (1) Users get their own location information from location devices m ;
- (2) According to the definition of sensitive attributes, the sensitive attributes of user location information are divided into longitude-sensitive attributes and dimensional-sensitive attributes;
- (3) According to the minimum distance grouping principle, the optimal tuple is obtained, and the l_1 -diversity principle is satisfied;
- (4) The user's real location information is divided into two parts: location information and grouping information.

The process of server privacy protection is as follows:

- (1) User location information is transmitted to the privacy protection processor after preprocessing at the client;
- (2) Use the minimum selection priority strategy to group the tuples in the location data table, and meet the l_2 -diversity principle;
- (3) After two rounds of anonymous user's location information is sent to the location service provider.

2.2. Algorithm Introduction

At present, in the process of location information service, many methods have been proposed to solve the problem of the leakage of user trajectory information. The more mature one is the k -anonymous method, that is, a user cannot be distinguished from another $k-1$ users, but this centralized anonymity strategy has certain flaws:

- (1) This anonymity method can only anonymize user information in a certain field.
- (2) Under normal circumstances, only the client or the anonymous method of the server is considered, but the server in the real world is not necessarily credible.

The main purpose of the l -diversity sensitive attribute algorithm proposed in the article is to enable an attacker to reduce the risk of being attacked by increasing the value of sensitive attributes on the basis of not being able to obtain user information based on the trajectory formed by the user's real location information, and to achieve differences in different fields. The combination determines that each user may have the same value. When mobile users need to obtain their own location information, they are anonymized before the last data. On the other hand, when the data is transmitted to the privacy protection processor, another layer of anonymization is performed. The main contributions of the article are:

- (1) Introduce the framework of location privacy protection system to provide mobile users with anonymous location-based services.
- (2) In the process of location information service, the user needs to upload the obtained location information to the server. When the server is not trusted, the attacker can easily intercept the user's location information from the server, thus increasing the trusted third party Middleware, used for multi-level anonymity processing. Propose privacy protection algorithms for client and server anonymity to prevent attackers from intercepting information from the client or server to achieve two levels of anonymity.
- (3) Strict experimental data is provided to prove that the algorithm proposed in the article has a certain effectiveness, and the privacy protection coefficient is higher than that of similar algorithms.

3. Multiple Privacy Protection Processors

3.1. Overview

The three-level system architecture can solve the user's location anonymity problem to a certain extent, and reduce the security risks of location information leakage caused by user queries. However, the user's location information is all handed over to a privacy protection processor for anonymous processing. When the number of users reaches a certain level and the user location information reaches a certain amount, the load of the processor will reach the limit. At this time, a new method is needed to solve this problem. For this problem [4], this article proposes a method to increase the number of privacy protection processors to solve the above problems, while considering query efficiency, and proposes the concept of cache area. The system architecture is shown in Figure 2.

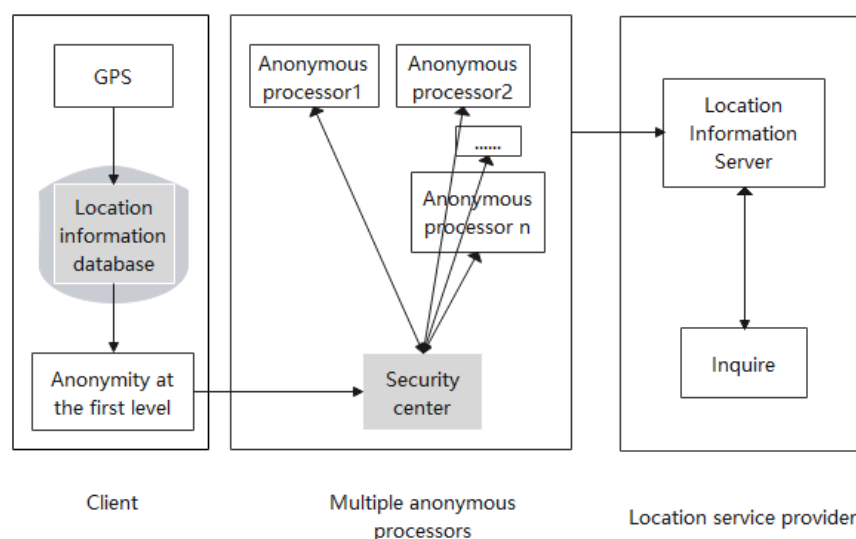


Figure 2. Multiple anonymous server architecture

3.2. Algorithm Introduction

Zheng Zhen-qing et al. [5] proposed multiple privacy protection processors to store user information based on k -anonymity technology. The algorithm reduces the frequency of users accessing the location server by adding a cache area on the mobile terminal, and assumes that there is a third-party trusted security center that attaches the security of location information to the security center.

In practical applications, it is impossible for the client to directly initiate a request for location query information, and then wait for the server to reply with the result. This mode of query takes a long time and a lot of performance. At the same time, in the three-level anonymity architecture, the anonymous tasks of the server are all assigned to the privacy protection processor. If the processor is attacked or fails to work normally, the security of the server will be greatly challenged. This article has carried out corresponding anonymous measures between the client, server, and between the client and the server to maximize the security of the location information of mobile users. The main contributions of the article are:

- (1) Considering the time efficiency of information interaction, increase the cache area of location information on the mobile client.
- (2) Taking into account the security risks and performance issues of a single privacy protection processor, add multiple privacy protection processors to make the user's location information concurrently anonymous.
- (3) In order to prevent attackers from launching targeted attacks on the database storing location information, the database is anonymized.

4. Anonymous Method of Distributed Structure

4.1. Overview

Li Rui et al. [7] proposed an anonymous method based on the distributed structure of location services, which mainly solves the current common background knowledge [6] attacks and regional center attacks. Users provide service providers with real location information to obtain corresponding services. This paper proposes a method that combines differential privacy technology with k -anonymity technology. The main idea is to first mesh the geographic space provided by the location server according to certain rules. Then it is stored through a quad tree, and the user's location information is replaced by the ID information carried by the grid to make it k -anonymous. Then the proxy user is selected by increasing the noise, and the proxy user initiates a query request. Experiments show that the scheme has certain advantages in terms of performance and safety.

4.2. Algorithm Introduction

In centralized privacy protection, the third party of the system architecture will have a single point of failure. At the same time, the third party has all the user's location information. Once the third party is attacked, all data will be intercepted. In response to these problems, a P2P distributed architecture [8] is proposed to protect location privacy. In this method, most mobile devices have computing and storage capabilities, but they also have obvious shortcomings:

- (1) Anonymity processing and information filtering of query results are all done on the client side, which causes a lot of overhead on the client system.
- (2) Location anonymity requires collaborative operations between users. If there are users who are disguised as attackers to query location information, the location information of related users will be leaked and the safety factor will be very low.
- (3) A single k -anonymous algorithm will be homogeneously attacked by an attacker, and the user's location information cannot be well protected.

In response to the above problems, this paper proposes a P2P distributed differential privacy anonymity algorithm. The article mainly proposes the use of P2P distributed architecture to anonymize the area composed of multiple users, and then add noise to the anonymized regional grid through the idea of differential privacy algorithm, so that the anonymized regional centroid is disturbed, so as to achieve The purpose of privacy protection. On the other hand, by increasing the data of points of interest [9] on the location server, the efficiency of location information query can be improved. The main contributions of the article are:

- (1) Introduce P2P distributed architecture to carry out k - anonymity algorithms to generate irregular anonymous areas constructed by multiple users.
- (2) The k - anonymous algorithm is reasonably integrated with the differential privacy algorithm to reduce the risk of location information background attacks.
- (3) Use the R-tree interest point algorithm to improve the efficiency of location information query.

The introduction of the P2P distributed architecture makes the location service architecture no longer rely on a third-party privacy protection processor, and to a certain extent solves the security problems caused by the privacy protection processor.

5. Research Ideas and Solutions

In the issue of location privacy protection, the premise of all anonymity is that all location information of the user needs to be anonymized, that is, there is no difference between personal privacy and shared information, so that even if users want to share their own location information, they need to go through a series of Anonymous processing of, resulting in redundant processing, resulting in a waste of performance and system resources. Based on this problem, I propose a new idea. Before the client anonymizes the user's location information, it is necessary to determine the user's location information attributes, and if it is personal private information, it will be anonymized accordingly. If it is shared location information, simpler processing or no anonymous processing is performed. This approach can reduce the pressure on the anonymity system to a certain extent and increase the efficiency of anonymity.

6. Conclusion

Location information services in mobile social networks have many hidden security risks. A large number of research workers at home and abroad have conducted targeted research on location privacy issues. This article summarizes several privacy protection methods, including: Based on a three-level architecture A single privacy protection processor algorithm and multiple privacy protection processor algorithms, as well as a differential privacy protection algorithm based on a distributed architecture. However, more in-depth research is needed on how to determine the attributes of user location information and how to solve the security problems caused by cloud storage.

Acknowledgments

Project: Guangdong University of Science and Technology school-level scientific research project funding(GKY-2020KYQNK-9).

References

- [1] Deng Mi-wen:Key Technology Analysis and Solution Research of Location Privacy Protection in LBS[J].Network Security Technology and Application,2019(10):35-38.

- [2] A.Machana vajjhala,J.Gehrke,and D.Kefer,l-diversity:Privacy beyond k-anonymity[C]//Proceedings of the 22nd International Conference on Data Engineering,2006,pp.15-24.
- [3] H.T.Li,L.X.Gong,F.Guo,Q.L.Miao,J.Wang:Location Privacy Protection in Mobile Social Networks Based on l-diversity[J].Journal of Information Science and Engineering.
- [4] Zhang Shao-bo,Wang Guo-jun,Liu Qin,et al:Trajectory privacy protection method based on multi-anonymizer[J].Journal of Computer Research and Development,2019,56(3):576-584.
- [5] Zheng Zhen-qing,Wu Xiao-sheng,Wang Hui,Liu Kun,Shen Zi-hao:Trajectory privacy PTPM protection method in mobile social network[J].Journal of Chinese Computer Systems,2021,42(10):2153-2160.
- [6] Zhou Qian,Qin Xiao-lin,Ding You-wei:Energy-efficient source location privacy protection algorithm based on attack perception[J].Journal of Communications,2018,039(001):101-116.
- [7] Li Rui: Research on Information Privacy Protection Based on Location Service[D].University of Electronic Science and Technology,2019.
- [8] Huang Yi,Huo Zheng,Meng Xiao-feng.CoPrivacy:Location privacy protection method for user collaboration without anonymous area[J].Journal of Computer,2011,34(10):1976-1985.
- [9] M.Jang,M.Yoon,H.Kim,et al:A privacy-aware location cloaking technique reducing bandwidth consumption in location-based services[C]//Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Querying and Mining Uncertain Spatio-Temporal Data.New York:ACM Press,2012:2-9.