Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis on Preserving Location Privacy

Rohan J. Patil*, Prof. K. K. Joshi, Prof. Sowmiya Raksha
Department of Computer Engineering and Information Technology
Veermata Jijabai Technological Institute
Mumbai, India

Abstract—The rapid growth of location-detection devices results in many innovative location based applications. However, untrusted location servers can lead to disclosure of user's private information. This paper gives a comprehensive survey of selected level of privacy in location based services that have been published in the different research journals. The survey throws light on the threats in location based applications and remedies for them.

Keywords— location privacy; anonymity; Spatial Cloaking; Obfuscations; Dummies

I. INTRODUCTION

The mobile location based services are growing with the rapid increasing use of smart phones. Now a days these location-based services area standard feature on many mobile devices. The main reason for rapid growth of location services is availability of GPS phones, their reduced prices, and app stores.

Location Based Service (LBS) has been widely used due to the tremendous use of location-detection devices, such as tablets, global positioning system devices, smart phones and so on. A LBS database server provides brief and personalized results to users according to their precise location information. An example of such services includes range query like "show me a list of hotels within 5km distance from my current location", and nearest neighbor query like "where is the nearest ATM". However, Users often show unwillingness to disclose their location information to untrustworthy LBS server because location information is sensitive and attackers may obtain more private knowledge of the user.

If location information is in the wrong hands it may severely hurt users. Real world examples of such incidents where LBS users are harmed by attacker economically [1], physically [2], and legally , by tracking users location information. Past studies have shown some algorithms can expose sensitive information of users such as location of home and office even if location-based services have used anonymized GPS traces [3,4]. Further, anonymized GPS traces with reverse white page lookups leads to disclosure of real identities of users. It is possible for attacker to infer user's mode of transport and can predict the route taken by users using some advanced attacks [6],etc. These attacks are successful even on applications that sporadically send location information to servers [5], even though there are several defenses like temporal and spatial cloaking of user location [13].We observe that the main reason behind location-based social applications becoming vulnerable is their dependency on user's location coordinates and user's trust on applications running on untrusted third-party servers where location coordinates are stored as plain-text. These servers store this location coordinates and based on it provide application-specific results to the users. However, as the location coordinates are stored as plain text it can reveal sensitive location information about users, and due to software bugs, operator errors or due to active attacks the location data on servers can be easily leaked out in large amounts, thus compromising location privacy of thousands of users.

Traditionally, mobile networks were used customer's location for data transmission and voice broadcast but now a days this location information is extensively used for providing different Location Based Services. Privacy is the most important factor for the people and is the most important feature the developers to keep in mind while developing the applications. Over the last few decades many research have been done on the location privacy but still contradiction and challenges in it conquer these risk. The techniques and methodology varied according to the application of location based service.

The extent of location privacy depends upon the information processing and temporal sequence. These activities include, (1) how data is collected; (2) how its retention or storage done; (3) how data is used; (4) and how revelation of location associated information is done. Various techniques used in the last few years to prevent the location privacy threats are cryptographic methods, spatial k-anonymity, cloaking or obfuscation, Private Information Retrieval protocol, dummy location, Trusted third party protocol, simple and multiple pseudonym and so on. This paper focuses the review of literature available on location privacy. It describes the different techniques used in the location privacy in the last few years in the research community and merits and demerits of these techniques.

II. CHARACTERISTICS OF LOCATION BASED SERVICES

A Location-Based Service (LBS) is a mobile computing application that provides services to users based on their geographical location. First generation LBS were reactive and client-server focused, where typically user would ask an

application some information and in return would get a response. The next generation LBS are proactive and interactive between users. For example: users may subscribe for certain services such as, relevant information can be sent to users based on their location rather than users having to manually search for it.

There are five basic components of LBSs[12]:

Mobile Device: Smart Phones, PDA, Laptops fall into this component. They are the tools the user can use to make any service request.

Communication Network: To send the user request to LBS providers and bring back the response, a mobile communication network is needed.

Positioning Component: For LBSs, user position detection is one of the key components. User's position can be detected by GPS or communication network.

Service and Application Provide: The service provider processes the service request. Such services calculate the user position and find a suitable result for user query based on the user location.

Data and Content Provider: Usually service providers do not always store all the information that maybe requested by the user. Therefore LBS result data will be usually requested from maintaining authority, or business and industry partners.

Some capabilities of LBS that are also very important from user point of view:

- **High Performance**: Delivering answers in second if querying information from internet and databases.
- **Scalable architecture**: Support thousands of concurrent users and terabytes of data.
- **Reliable**: Capable of delivering up to 99.999 percent up-time.
- **Current**: Support the delivery of real-time, dynamic information.
- **Mobile**: Availability from any device and from any location.

III. DIFFERENT TECHNIQUES USED TO PRESERVE LOCATION PRIVACY

A. K-Anonymity

K-anonymity approach is the most popular approach to location privacy, which anonymises data through deviation techniques before forwarding it to the LBS providers. Gruteser and Grunwald[13]first studied Location *k*-anonymity .But this work has several drawbacks. First, it assumes a system-wide static *k* value for all mobile clients, which affects the service quality for those mobile clients whose privacy requirements can be satisfied using smaller *k* values. Second, their approach fails to provide any quality of service guarantees with respect to the sizes of the cloaking boxes produced. This is because, the quadtree-based algorithm anonymizes the messages by dividing the quadtree cells until the number of messages in each cell falls below *k* and by returning the previous quadrant for each cell as the spatial cloaking box of the messages under that cell.

Bettini et al. [14] has introduced a technique aimed to support k-anonymity method and proposed a framework for evaluating the risk of distributing sensitive location-based information .The authors put forward the thought that the geo-localized history of the requests submitted by a user can be considered as a quasi-identifier, i.e. a set of characteristics that can be linked with external information, thus dropping the uncertainty over the identity of the user. Gruteser and Grunwald [13] propose a middleware architecture and an algorithm to adjust location information resolution to conform with a specific k-anonymity requirement. Gedik and Liu [14] proposed another k-anonymity model in which every user can define the minimum level of anonymity and the maximum acceptable temporal and spatial resolution for her location measurement. They have proposed a message perturbation engine which will provide location anonymity of user's requests through identity removal and spatio-temporal obfuscation of location information. Mokbel et al. [7] has put forwarded a framework where each user defines her privacy preferences through a parameter k and area A_{min}, where k is the k-anonymity requirement of the user ,and an area A_{min} is the minimum acceptable resolution of her location information.

K anonymity mainly helps to maintain the truthfulness of the user's information. Multilevel databases used in the k anonymity techniques, the different level arrangement has facilitate to store the data at different security classification and also user's holding dissimilar security authorization but unfeasible to consider every possible attack. In other concern numerous holder share same data and suppression reduce the quality of the data so a feasible approach is needed to conquer the disadvantage of K anonymity.

B. Mixzones

Alastair R. Beresford and Frank Stajano have proposed Mix zone model. The main aim of mix zones is to stop tracking of long-term mobile user's activities, but still permit the operation of many short-term location-aware applications[8].

The mix zone model anonymizes user identity by restricting the positions where users can be located. The model provides: 1) a middleware mechanism which provides anonymized location information to third-party applications,and 2) a quantitative run-time estimate of the level of anonymity provided by the middleware with a particular set of applications.To gain a proper understanding of the privacy properties of mix zones it is important to find out how hard it is to break the anonymity the system provides. The mix zone approach for calculating anonymity does this : the degree of success in playing the role of attacker - attempting to recover the long-term user identities hidden by the constantly changing pseudonyms - is an inverse measure of the anonymity offered by the system.

C. Location Obfuscations

Location obfuscation can be defined as "the means of deliberately degrading the quality of information about an individual's location in order to protect that individual's location privacy." [9] The main notion behind obfuscations is for the system to change or hide the original location of the user while still being able to provide user with the appropriate level of service. In addition to that, depending on the amount of information that he is willing to give its real position ,the user must have a way to determine the level of alteration that its location will suffer .From the techniques in [11], the noise-based technique are used to add Gaussian noise to the samples in order to generate a new location. Even though this method is the easy to implement, it may have disadvantages; For example, the noise which we have added may tend to leave the new obfuscated point closer to the center than a uniformly random position. Three metrics are used for evaluating the efficiencyof these techniques: maximum, minimum and average distance between original and obfuscated points, which gives an important indication of the alteration introduced in the path.

Duckham and Kulik [9] put forward a framework which provides a mechanism that balances the user's needs for the location privacy and high-quality information services. The authors have proposed to degrade the quality of the location information and to provide obfuscation features by adding n points at the same probability to the real user position. In general, all these obfuscation solutions has some common demerits .First, they don't offer a quantitative estimation of the given privacy level hence making them difficult to integrate into a full fledged LBS application. Second, it uses a single obfuscation technique based on the enlargement of the location area whose effect can be easily undone by the attacker.

D. Dummies

In order to conquer the problem of traceability in Location Based Services, a new type of anonyms technique proposed in the literature [15] is Dummies location. It sends the location information of the user including noise to the service provider. This noise consists of false location of the user's called dummies. Then service provides creates a reply message for each received position data.The user only extracts the necessary information from the reply message. In this manner, service providers cannot differentiate between true position data and other positions from a set of positions data if all dummies have temporal consistency. Hidetoshi Kido *et al*., [15]has proposed the dummy generation algorithm with two set of models are Moving in Neighborhood and Moving in a Limited Neighborhood accomplished in different external server.

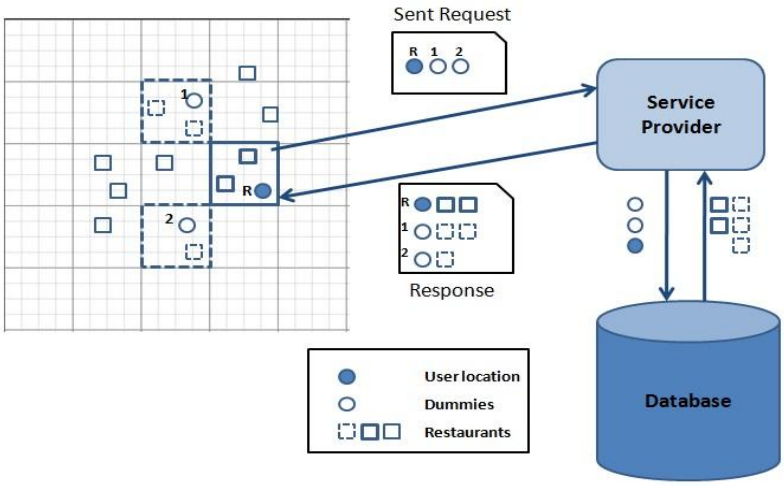

Figure 1 Anonymous lbs using dummies

E. Location spatial cloaking

The centralized model[16,10,17] of spatial cloaking uses a centralized trustworthy third party, named as location anonymizing server. The location anonymizing server act as a middleware between users and LBS database servers. The anonymizing server collects exact location information and obfuscates them into a cloaked region. In [16], the proposed spatio-temporal cloaking algorithm assumes a unified k-anonymity requirement which gives less flexibility to the users. In Clique Cloak algorithm[17], it enables a personalized k-anonymity requirement and it requires large computation overhead for calculating the clique graph and it is quite limited to a narrow range of small k.

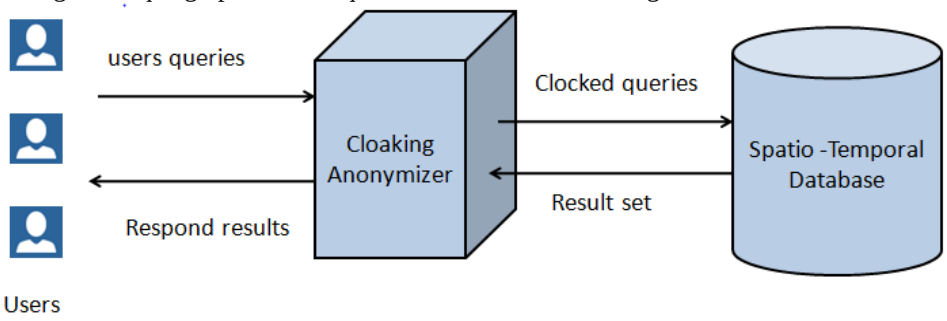

Figure 2 Cloaking method for lbs

The New Casper [10] utilizes an adaptive grid-based pyramid structure to find proper cloaking region but may often produce a larger cloaked region than what is expected. Also, when the number of mobile users is huge or they are moving fast, the system will meet its performance bottleneck.

F. Cryptography

Cryptography techniques are also used by many researchers for preventing position traceable problem, it has capability of sharing information with high security, data integrity in several database and intense authentication in mobile network. In privacy model cryptography can be used in both online and offline trusted third party. Trusted third party schemas are mostly based on spatial K- anonymity and cloaking or obfuscation for securing the association between user identity and location. Hilbert based algorithm [17] and Icliqueclock [18] are the recent studies focused on giving better model to conquer the various disadvantage faced in the location privacy frame work. The main difference between these two algorithm are Hilbert is based on the geographic related algorithm and icliquecloak based on the geometry based algorithm, icliquecloak is adapted from the K anonymity and cloaking algorithm.

Table 1 Comparison between different techniques used in lbs

Technique	Advantages	Disadvantages
K anonymity[13,14,7]	Location Privacy	No identity privacy, Unlink ability
Mixzone[8]	Location and sampling accuracy	Operation Lack in multiple responder
Obfuscation[9,11]	High server efficiency, Location privacy	No identity privacy, Unlink ability
Dummies[15]	Easy to integrate with existing mobile network	Operation Lack in multiple responder
Cloaking Algorithm[16,10,17]	Accuracy, Flexibility	Unlink ability
IcliqueCloak[17]	Many responders	Possibility of attack
Hilbert Based[18]	Quick query processing time Location privacy	High cost

IV. CONCLUSIONS

Current studies focuses on the location user privacy and a simple framework for interconnecting the mobile network and privacy model server. There are well-known models like k anonymity and cloaking algorithm utilized in various literatures though we require an efficient and effective tool to tackle the location privacy threats. This paper surveyed various techniques used in the research area of preserving location privacy of the Location Based Service (LBS).

Location privacy research is still in fundamental level. Even though inventive model have been proposed to resolve the privacy problem in Location Based Service (LBS), there are still many challenges faced by research group. The various disadvantage of existing model should be taken into consider while inventing a new structure of algorithm. On one side, interlinking of mobile network and secure framework still has many challenges to be addressed, on another side there is lack of technology in multiple responder's problem.

REFERENCES

[1] Schilit, B., Hong, J., And Gruteser, M. Wirelesslocation privacy protection.
[2] Grace, F. Stalker victims should check for gps, Feb. 2003.
[3] Golle, P., And Partridge, K. On the anonymity of home/work location pairs. In *Proc. of Pervasive* ,2009.
[4] Hoh, B., Et Al. Enhancing security and privacy in traffic-monitoring systems. In *IEEE Pervasive ComputingMagazine* ,2006.
[5] Krumm, J. A survey of computational location privacy. *Personal and Ubiquitous Computing* ,2008.
[6] Froehlich, J., And Krumm, J. Route prediction from trip observations. *Society of Automotive Engineers* ,2008.
[7] Mokbel, M.F., C.Y. Chow and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy",VLDB Endowment, 2006.
[8] Beresford Alastair R. and Frank Stajano. *Mix Zones: User Privacy in Location-Aware Services.* Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, 2004.
[9] Duckham, M. and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy", Pervasive Computing, pp. 243-251, 2005.
[10] Mokbel, M.F., C.Y. Chow and W.G. Aref, "The New Casper: A Privacy-aware Location-based Database Server", in IEEE 23rd International Conference on Data Engineering, ICDE 2007, IEEE, 2007.
[11] Ardagna, C.A., et al., "An Obfuscation-based Approach for Protecting Location Privacy", IEEE Transactions on Dependable and Secure Computing, vol. 8, No. 1, pp. 13-27, 2011.

[12] Steiniger S., Neun M., Edwardes A.; Foundations of Location BasedServices; Lesson 1 CartouCHe 1- Lecture Notes on LBS, V. 1.0

[13] Gruteser Marco and Dirk Grunwald. Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. Proceedings of the 1st International Conference on Mobile Systems, Applications and Services. ACM, 2003.

[14] Gedik, B. and L. Liu, "Protecting Location Privacy with Personalized *k*-anonymity: Architecture and Algorithms", IEEE Transactions on Mobile Computing, vol. 7, No. 1, pp. 1-18, 2008.

[15] Kido Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh. *Protection of Location Privacy Using Dummies for Location-Based Services.* Data Engineering Workshops, 2005. 21st International Conference on. IEEE, 2005.

[16] Ardagna, C.A., et al., Privacy-enhanced location-based access control. Handbook of Database Security,2008.

[17] To Quoc Cuong, Tran Khanh Dang, and Josef Küng. *A Hilbert–Based Framework for Preserving Privacy in Location–Based Services*. International Journal of Intelligent Information and Database Systems. 2013.

[18] Pan Xiao, Jianliang Xu, and Xiaofeng Meng. *Protecting Location Privacy against Location-Dependent Attacks in Mobile Services.* Knowledge and Data Engineering, IEEE Transactions on. 2012.

