International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 11237-11249
© Research India Publications
http://www.ripublication.com

A Review of Protecting Location Privacy In Location Based Service

Ajay Nadargi[1] **and Mythili Thirugnanam**[2]
[1] *Research Scholar, School of Computing Science and Engineering, VIT University, Vellore, Tamilnadu, India*
avn.sit@sinhgad.edu
[2] *Associate Professor, School of Computing Science and Engineering, VIT University, Vellore, Tamilnadu, India*
tmythili@vit.ac.in

Abstract

Mobile devices equipped with positioning capabilities can ask location-dependent queries to Location Based Services (LBS). To protect privacy, the user location must not be disclosed. Location Based Services are information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device. Location-based services propose several opportunities for Business and public purpose. Information of users can be misused thereby raising the issues of security both for the personal privacy and national security. In LBS the individual's location privacy has turn into a key concern for persistent computing research. In such a context, privacy concerns are increasing and call for sophisticated solutions able to guarantee different levels of location privacy to the users. The quality of the location-based service an individual receives is directly linked to the quality of information which that individual is willing to reveal about his or her location. This paper surveys the most related techniques for guaranteeing location privacy to LBS users. The rigid separation between techniques which rely on Trusted Third Parties (TTP-based) and those which do not (TTP-free) is highlighted. Also, the convenience of both approaches on the location measurement and its location privacy in these services are discussed.

Keywords: Location Privacy, Location-based Service, Trust, Anonymizer, Obfuscation

Introduction

Privacy is internationally recognized as a fundamental human right. Location aware pervasive computing environments provide the ability to automatically sense, communicate, and process information about a person’s location, with a high degree of spatial and temporal precision and accuracy. Location is an especially sensitive type of personal information, and so safeguarding an individual’s location privacy has become a key issue for pervasive computing research. This addresses the issue of protecting sensitive information about an individual user’s location, at the same time as providing useful location-based services to that user. This approach focuses on negotiating a balance in the levels of privacy and utility for a location-based service.

Overview of LBS

The physical location of users is rapidly becoming easily available as a class of personal information that can be processed for providing new online and mobile services, generally called Location-Based Services (LBSs). The quality of the location-based service an individual receives is directly linked to the quality of information which that individual is willing to reveal about his or her location.

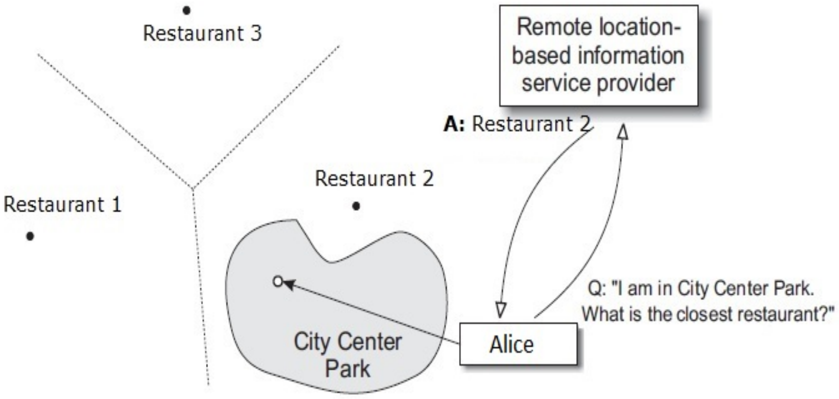
Restaurant 3
Remote location-based information service provider
A: Restaurant 2
Restaurant 2
Restaurant 1
Q: "I am in City Center Park. What is the closest restaurant?"
City Center Park
Alice

Figure 1: Scenario of an obfuscated location-based information service

Example

In Figure 1, Alice wishes to access information about the address of the closest restaurant, via a remote location-based service provider. Although there are three nearby restaurants, he would like to protect his privacy by providing only an approximate location to the information service provider. For example, the Alice can obfuscate his exact location by revealing only that he is in the “City Center Park.” In this case, the service provider should still be able to correctly reply with the address of “Restaurant 2”.

Privacy Issues in LBS: Data or information privacy refers to the evolving association between technology and the legal right to, or public expectation of, privacy in the collection and sharing of data about one's self. It is possible to access mobile users’ location information anytime and anywhere. But in the meantime, user location privacy security causes a potentially grave new threat, and may suffer from some attack which could not presume. Location privacy issues raised by such applications have attracted more and more attention. The rest of the paper is organized as, In Literature Review Section, discussed several location privacy preserving methods. In Location Privacy Relevance Section, describe location privacy relevance. In Summary Section, briefly summarize the privacy techniques.

Literature Review

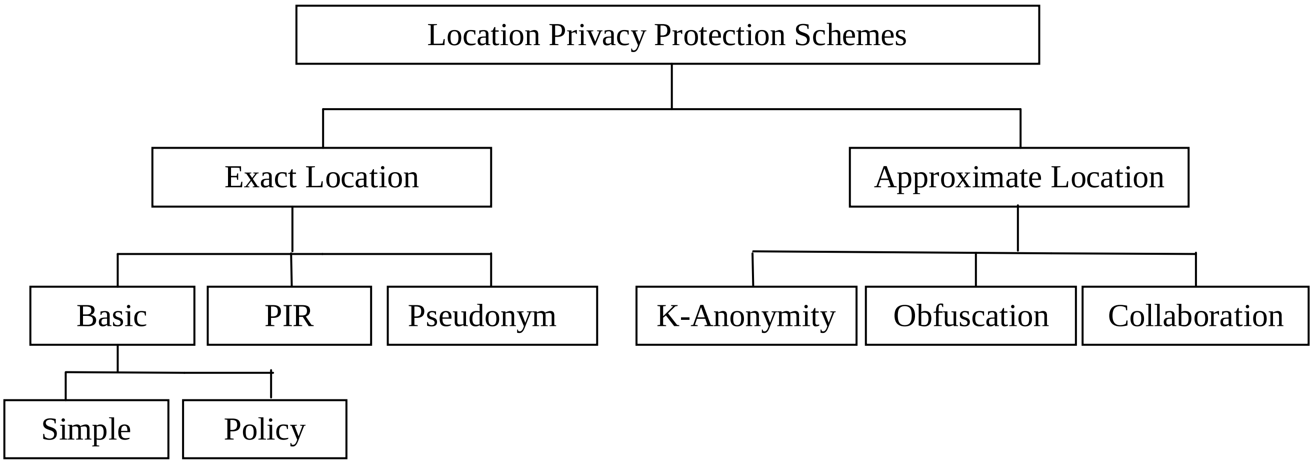

Figure 2: Location Privacy Methods Classification

Simple Communication Scheme

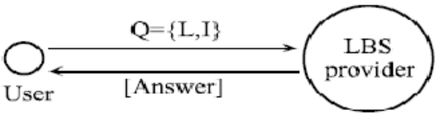

Figure 3: Simple communication scheme with an LBS user and an LBS provider

In the simplest form of communication between an LBS user (U) and an LBS provider (P), the former sends a simple query (Q) containing an ID, his location (L) and a request for information (I) that he wants to retrieve from P. Thus, a simple query sent from U to P can be Q = {ID_U,L, I} = {ID_U, x_U, y_U, "Where is the closest bus station?"} (cf. Figure 3). By sending their current locations to P, LBS users assume that P manages their data honestly and refrains from any misuse. However, LBS providers cannot always be trusted and more complex communication schemes are needed. With the aim to protect the privacy of LBS users, a number of methods have been proposed. For the sake of clarity, classified those methods depending on the way they manage the locations of the users. First, consider the methods that do not distort locations, and then move to the ones that use approximations. Agusti Solanas et al. [11] explain study of classification privacy method which shown in Figure 2.

Exact Location Schemes

Classify under this category all the methods that do not distort the location of LBS users to protect their privacy. These methods are very common because most of them are conceptually simple. In addition, due to the fact that they do not modify the location of the users, the obtained results are optimal. Apart from the basic/simple scheme described above, consider three non-disruptive schemes:

- Policy-based schemes
- Pseudonymizers
- Private Information Retrieval (PIR)-based schemes

Policy-based schemes

The architecture of these schemes is like the simple scheme with a single user and a provider. However, in this case the provider adheres to a set of privacy policies. Consequently, the user has the right to ask for compensation if the provider does not fulfill his duties.

Pseudonymizers

These schemes add a trusted third party (a pseudonymizer) to the basic model. The pseudonymizer mediates between users and providers. Users send their queries to the pseudonymizer, which replaces the real identity of the users (e.g. their IP addresses) by a pseudonym. This way, providers cannot identify users because they become hidden behind the pseudonymizer. Notwithstanding, users must trust pseudonymizers because they have full access to their real locations and identities. Also, if users send several queries from the same location (e.g. from their residence), providers can determine their real identities by using e.g. a public telephone directory. These attacks are known as Restricted Space Identification (RSI) and Observation Identification (OI).

PIR-based schemes

Ghinita et al. [17] proposes PIR schemes. Private information retrieval (PIR) is a difficult problem mainly studied by the databases and cryptography communities. The goal of PIR is to allow a user to obtain a record (i) from a database without revealing i. The main problem of these methods is their high computational complexity. In addition, the LBS provider must implement very sophisticated protocols to exchange information with users.

Approximate Location Schemes

The methods that distort the real locations of the users assume that the modification of the locations prevents the provider from learning private information of the users. Consider three main categories:

- K-Anonymity
- Obfuscation
- Obfuscation by collaboration

K-Anonymizers:

Divanis et al. [7, 9] introduced k-anonymity which protect micro data. The main idea of k-anonymity applied to LBS is to hide a user amongst k – 1 other user. To do so, k-anonymizers are used. They are TTPs to which users send their queries. After collecting some queries, k-anonymizers build groups of k users and compute a fake location (e.g. a centroid) that represents all the members of the same group. Then, the real locations are replaced by the centroid of the group and the provider cannot distinguish which user in the group sent the query. Although the k-anonymity property is very interesting and increases the privacy level of the users, this approach has all the problems of the TTP-based approaches and, in addition, the obtained results are not accurate.

Obfuscation-based schemes

These methods are generally run by a single user and no TTPs are required. The main idea behind them is to reduce the accuracy of the location. For example, instead of sending the real location, users send a squared area. By doing so, providers just know that a given user is located inside that area but they do not know exactly where. By means of increasing the size of the area, location privacy is also increased but results become worse.

Collaboration-based schemes

In this kind of methods, the goal is the same as in obfuscation methods and k-anonymizers. However, the strategy is different. Users collaborate to exchange location information that they use to disguise their real location. By collaborating, users avoid TTPs and improve the results of single-user obfuscation methods.

In paper Marius Wernke [3], Classification of attacks is shown in Figure 6. The Classification of attackers according to knowledge exploits to derive private information. The distinguish between single position attacks, context linking attacks, multiple position attacks, attacks combining context linking and multiple position attacks, and attacks based on compromising a TTP component. Peer to Peer cloaking has been demonstrated by Tazima [6]. Authors in papers [18][19] talks about K-anonmity based location privacy. The paper [18] by Bu_gra Gedik and others, describes a scalable architecture for protecting the location privacy. Mobile clients can specify the smallest level of anonymity that is expected. Experiments show that the personalized location k-anonymity model, and its location perturbation engine, can achieve high protection to location privacy threats. And this is achieved with small performance overhead. Emmanoil's [10] and Ge Zhong [15] discussed about distributed location privacy. Privacy from operators is achived by splitting the request and reply, messages. It is pointed that users can jointly determine the cloaked area for anonmizing privacy provided that users trust each other [15]. Use of cryptography in the form of signatures has been demonstrated by the author. Fizza and Rasheed [4] proposed a cloud server based architecture named as Privacy Preserving Cloud-based Computing Platform (PPCCP) for location based services. The main component of architecture is a cloud-based server PPCCP. This server is like a bridge between users and LBS servers. They proposed a secure architecture PPCCP to utilize location-based services anonymously using a cloud-based server which need not to be trusted. In Thomas Liebig [2] paper overcomes limitations of previous works and provides a privacy preserving aggregation framework for distributed data streams. Individual location data is obfuscated to the server and just aggregates of k persons can be processed. This is ensured by use of Pailler's homomorphic encryption framework and Shamir's secret sharing procedure. In result obtain anonymous unification of the data streams in an un-trusted environment. In Min Li paper [1], proposed a privacy-preserving query method, which successfully provides more precise proximity services and solves the location privacy issues on 3D smooth surface. In this paper, introduce the geodesic distance and put forward a more precise proximity range measurement method based on the triangle fractal.

Location Privacy Relevance

The shape of a location measurement: the area returned by a location measurement is planar and circular. User location information, in fact, is affected by an intrinsic measurement error introduced by sensing technologies, resulting in spatial areas rather than geographical points. This represents a particular case of the general requirement of considering convex areas and a good approximation for actual shapes resulting from many location technologies (e.g., cellular phones location). According to this, a location measurement is defined as follows.

Location Measurement

Ardagna et al. [5] tries to calculate location measurement. Let $(x_{\underline{u}} , y_u)$ be the real position of a user u. A location measurement for u is a circular area $A = (x_i, y_{i,} r_i) \subseteq \Pi r^2$ returned by a sensing technology such that (x_i, y_i) are the coordinates of the center of A_i, r_i is its radius, and the following conditions hold:

1. $P((x_u, y_u) \, □ \, A_i)) = 1;$ (Eq.1)
2. $P((x_u, y_u) \, □ \, A)),$ *where* $A = (x, y_, \delta r) \subset A_i$ (Eq.2)

is the neighborhood of position (x, y) with δr an infinitely small radius, is uniformly distributed.

Equation (1) comes from observing that sensing technologies based on cellular phones usually guarantee that the real user position is within the returned area. Equation (2) states that the probability that the real user position falls within a neighborhood A ⊂ Ai of a random point(x, y) is uniformly distributed. In other words, the real user position could be randomly located everywhere inside Ai with uniform probability.

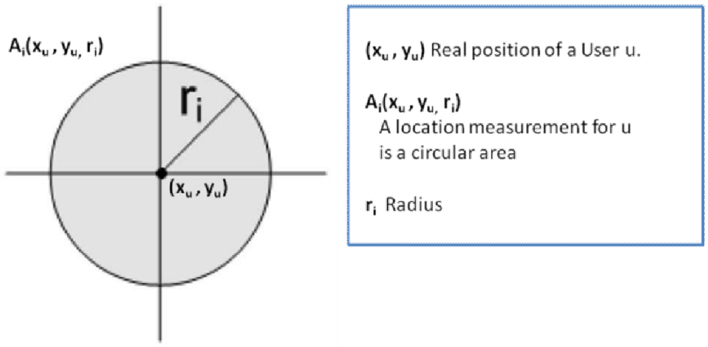

Figure 4: Location Measurement

As shown in Figure 4,
(x_u , y_u) **:** Real Position of a User u.
$A_i(x_u ,y_u, r_i)$ **:** A location measurement for User u is a circular area.
R_i **:** Radius

The goal of work is to design a solution that protects the location privacy of the users according to their preferences and application context. To this end, the location privacy must be measured and quantified with respect to the accuracy of the location measurement: the more accurate the measurement, the less the privacy. The accuracy of a location measurement returned by a sensing technology depends on the radius of the measured circular area, which, in turn, depends on the unavoidable measurement error of the sensing technology. To evaluate the quality of a given location measurement, its accuracy must then be compared with the best accuracy that sensing technologies are able to provide. Several works describe and discuss different location techniques and their best accuracy which is always expressed by defining the radius of the area returned if the best accuracy is achieved. Introduce a metric, called relevance that provides both a dimensional technology-independent measure of the location accuracy and a measure of the privacy of a location measurement. The relevance associated with a location measurement is formally defined as follows:

Relevance

Let $A_i = (x_i, y_i, r_i)$ be a location measurement for a user and r_0 be the radius of the area that would be produced if the optimal accuracy is achieved. The relevance associated with Ai, denoted as R_i, is the ratio r_0^2/r_i^2.

In other words, R_i models the relative accuracy loss of a given measure (e.g., due to particular environmental conditions) with respect to the optimal accuracy r_o that the location techniques would have achieved in perfect environmental conditions. R_i is the only relevance value that depends on physical values (i.e., measurement errors).

By definition, such a relevance

- tends to 0, when the location measurement is extremely inaccurate;
- is equal to 1, when the location measurement has achieved the best accuracy that the location techniques allow; and
- is in the range (0,1); otherwise, the higher the value, the higher the accuracy.

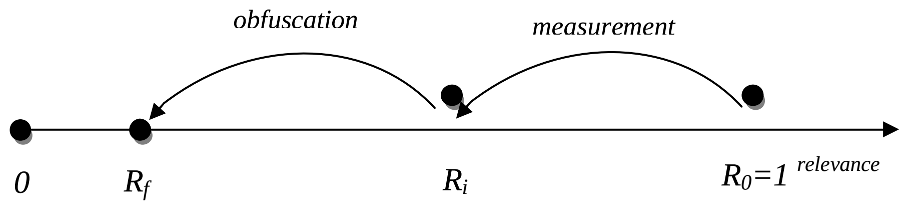

Figure 5: Relevance degradation due to the intrinsic measurement error and obfuscation

The location privacy associated with a location measurement Ai can then be defined as follows:

Location Privacy

Let A_i be a location measurement with relevance R_i. The location privacy of A_i is 1-R_i. In this scenario, users can specify their privacy preferences in term of a final relevance R_f that a location measurement must not exceed. A typical way to let users specify their privacy preference is based on the concept of minimum distance. For instance, a user can define “100 meters” as his/her privacy preference, meaning that he/she can be located with accuracy not better than 100 meters. Considering measurements that produce circular areas, such a preference corresponds to an area of radius 100 meters at least. Although this solution is certainly intuitive and easily understandable by users, it suffers from some drawbacks. In particular, a minimum distance is meaningful in a specific application context only and is suitable when the obfuscation is performed by scaling a location measurement to a coarser granularity. Propose a solution based on the specification of a final relevance R_f that does not depend on the application context and provides strong robustness. The final relevance R_f together with the initial relevance R_i associated with A_i are used to derive the accuracy degradation that needs to be introduced for privacy reason.

Accuracy Degradation

Let Ai be a location measurement with initial relevance R_i, and let R_f be the final relevance requested by the user. The accuracy degradation to be applied to A_i, denoted as λ, is the ratio R_f /R_i. Given a location measurement and an accuracy degradation, problem is to transform (obfuscate) the location measurement in such a way that the resulting area satisfies the privacy preference R_f defined by the user.

Obfuscation

Let (x_u ,y_u) be the real position of a user u; A_i with relevance R_i be a location measurement for u, and R_f be the final relevance to be satisfied. Transform A_i into an obfuscated area A_f such that the following conditions hold:

1. A_f has relevance R_f (Eq.3)
2. $P((x_u , y_u) \in A_f)) > 0$ (Eq.4)

Equation (3) requires the obfuscated area to satisfy the privacy preference of the user. Equation (4) requires the obfuscated area to include the real user position and implies that A_i and A_f cannot be disjoint. The transformation of a location measurement Ai into an obfuscated area A_f is performed by applying a set of basic obfuscation techniques that change the radius, or the center, of the original location measurement. As illustrated in Figure 5, the transformation of A_i into A_f introduces relevance degradation in addition to the natural degradation due to the intrinsic measurement error. Note that if $R_f >= R_i$, no obfuscation is applied to the location measurement, since the measurement error introduced by a sensing technology already satisfies the privacy preference of the user.

Summary

Summarization of existing protection approaches in location based services has been done , which mentioned in Table 1. The existing protection approaches is categorized into two types such as exact and approximate. In exact location, do not modify the location of the users and in approximate distort the real locations of the users to maintain their privacy. There is a comprehensible difference between TTP based schemes and the TTP free ones. While TTP based schemes are the most common ones, TTP-free schemes seem superior in terms of privacy due to the following shortcomings of intermediate TTPs: (a) TTPs are critical points which can be attacked; (b) TTPs are bottlenecks; (c) There must be lots of users subscribed to a TTP for the latter to be able to calculate suitable cloaking regions. In general TTP-based schemes are weak as users rely on a single trusted entity. This entity can be copied by a fake TTP created by the attacker, in which case all the information shared by users with the bogus TTP falls in the hands of the attacker. TTP-based schemes are easier to implement than collaborative-based methods because the entire communications required by users to avoid the use of a TTP is not necessary. However, obfuscation-based methods are also easy to implement. The advantage of all existing protection approaches in location based services provides location privacy and results also well but some of them provide more location privacy means the increasing the size of the area, location privacy is also increased but results become worse as compared to simple privacy.

Table 1: Location Privacy Methods

	Pseudonym	**Policy**	**PIR**	**k-Anonymity**	**Collaboration**	**Obfuscation**
1. Type	Exact	Exact	Exact	Approximate	Approximate	Approximate
2. Distort Location	No	No	No	Yes	Yes	Yes
3.TTP Based	Yes	Yes	No	Yes	No	No
4.Concept	Provide Fake data, Replace Real ID by Fake ID	Bind Set of Privacy Policies	Cryptographic Tech.	No need of User Policy & ID , Replace Real Location by CR, K-user located	Broadcast Location, Request of other user location, K-user located	User Real Location Replace by Circular Area, Variable Center & Radius, Generate Anchor
5.Disadvantages	RSI, OI Attack	RSI, OI Attack	High Computational Complexity	Centralized Arch, DoS Attacks	Malicious User added	No k-User located
	Bottleneck, Single Point of Failure, Weak, User Subscribed to TTP, Disclose Personal Information					
6.Advantages	Privacy	Privacy	More Privacy	Privacy	Non-Centralized Communication, Avoid DoS Attack, More Privacy	Non Collaborative , Find Closest Point, Hidden User Location, More Privacy

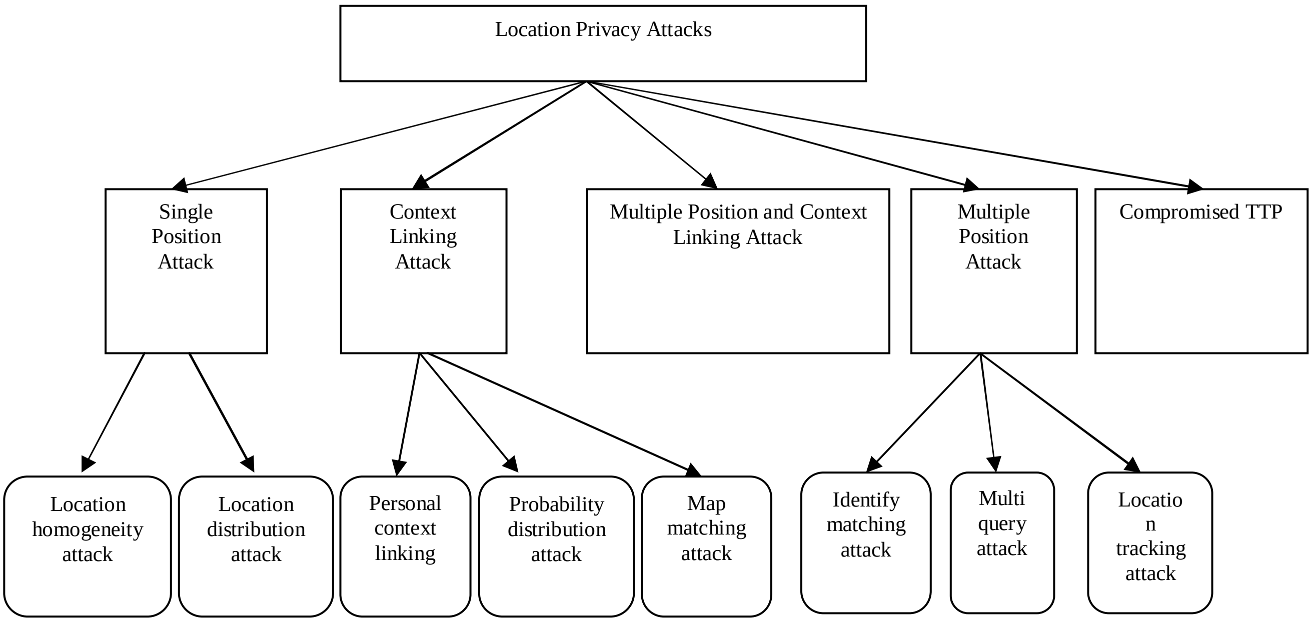

Figure 6: Classification of Location Privacy Attacks

Conclusion

Location-based services promise to make it easier to connect with family, friends, and associates. But in their current form, the services make it too easy for people and organizations to access your private information without your explicit consent. While many perhaps most of these third parties won't misuse this information, others won't be so trustworthy. Look out for various obfuscation techniques that help in keeping the personal information to share is restricted only to its target’s use. In this paper, we have discussed the ordinary threat models used in LBS privacy protection, summarized the existing privacy metrics, and also presented privacy protection solutions with a focus on location perturbation and obfuscation schemes.

References

[1]. Min Li , Ruijin Wang, Zhiguang Qin and Cong Wang, 2014, *“Privacy-Preserving Proximity Based Services”*, International Journal of Hybrid Information Technology , Vol.7, No.4 , pp.139-152

[2]. Thomas Liebig, , 26-28 November 2014, *“Privacy Preserving Aggregation of Distributed Mobility Data Streams”*, TU Dortmund University, Germany, 11th International Symposium on Location Based Services, LBS 2014, Vienna, Austria

[3]. Marius Wernke, Pavel Skvortsov, Frank Durr, 2014 "A classification of location privacy attacks and approaches", Springer, Pers Ubiquit Comput 18:163–175

[4]. Fizza Abbas, Rasheed Hussain, Junggab Son and Heekuck Oh, 2013 IEEE, *"Privacy Preserving Cloud-based Computing Platform (PPCCP) for using Location Based Services"*, ACM 6th International Conference on Utility and Cloud Computing

[5]. Tanzima Hashem, Lars Kulik, 2011, "Don't trust anyone'': Privacy protection for location-based services", Pervasive and Mobile Computing 7, 44–59doi:10.1016/j.pmcj.2010.04.006

[6]. Tanzima Hashem, Lars Kulik, 2011, "Don't trust anyone'': Privacy protection for location-based services", Pervasive and Mobile Computing 7, 44–59doi:10.1016/j.pmcj.2010.04.006

[7]. Aris Gkoulalas–Divanis, July 2010, *"Providing K–Anonymity in Location Based Services"*, SIGKDD Explorations Volume 12, Issue 1

[8]. Chowdhuryi S. Hasan and Sheikh I. Ahamed, © 2010 IEEE, *"An Approach for Ensuring Robust Safeguard against Location Privacy Violation"*, 34th Annual Computer Software and Applications Conference,

[9]. Wenyan Zhang, Ximing Cui, Dengfeng Li, Debao Yuan, Mengru Wang, 2010, *"The Location Privacy Protection Research in Location-based Service"*, College of Geoscience and Surveying Engineering China University of Mining & Technology (Beijing), cutmb Beijing, China

[10]. Emmanouil, Panayiotis, Spyros and Konstantinos, 2010, *"A Distributed Privacy-Preserving Scheme for Location-Based Queries"*, IE 978-1- 4244-7265-9.

[11]. Agusti Solanas, Antoni Martınez-Balleste, © 2009 IEEE, *"Location Privacy Through Users' Collaboration: A Distributed Pseudonymizer"*, 2009 Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies,

[12]. Yan Sun, Thomas F. La Porta, and Parviz Kermani, March 2009, *"A Flexible Privacy-Enhanced Location-Based Services System Framework and Practice,"* IEEE Transactions On Mobile Computing, Vol. 8, No. 3,

[13]. Fei Xu, Jingsha He, Xu Wu and Jing Xu, 2009 *"A Method for Privacy Protection in Location Based Services"*, IEEE Ninth International Conference on Computer and Information Technology, DOI 10.1109/CIT 2009.28

[14]. Song Wang and X. Sean Wang, 2009, *"AnonTwist: Nearest Neighbor Querying with Both Location Privacy and K-anonymity for Mobile Users"*, Tenth International Conference on Mobile Data Management: Systems, Services and Middleware

[15]. Ge Zhong and Urs Hengartner, 2009 IEEE, *"A Distributed k-Anonymity Protocol for Location Privacy"*, DOI 928-1-4244-3304-9.

[16]. Agusti Solanas, Josep Domingo-Ferrer, and Antoni Martınez-Ballest, 2008,*"Location Privacy in Location-Based Services: Beyond TTP-based Schemes"*, Av. Paısos Catalans 26 E-43007 Tarragona, Catalonia, Spain

[17]. Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, © 2008 IEEE, *"Private Queries in Location Based Services: Anonymizers are not Necessary"*, SIGMOD'08, Vancouver, BC, Canada. Copyright ACM 978-1-60558-102-6/08/06,

[18]. Bu_gra Gedik, and Ling Liu, January 2008, *"Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms,''* IEEE Transactions on Mobile Computing, Vol. 7, No. 1

[19]. John Krumm, Microsoft Research, 2008 *"A survey of computational location privacy"*, Springer DOI 10.1007/s00779-008-0212-5

[20]. C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, 2007, "Location Privacy Protection Through Obfuscation-based Techniques" , Dipartimento di Tecnologie dell'Informazione Universit`a di Milano – 26013 Crema – Italy