International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Security and Privacy Aware Location Based Service System

Sneha Sonwane[1], **D. A. Phalke**[2]

[1]D.Y.Patil College of Engineering, Savitribai Phule Pune University, Akurdi, Pune, Maharashtra, India
[2]D.Y.Patil College of Engineering, Savitribai Phule Pune University, Akurdi, Pune, Maharashtra, India

Abstract: ***Recently, Smartphone devices are highly accurate at determining location knowledge that it enables many users to provide various location sensitive services. But on the other side, such position data of user may include deeply personal information. The protection of location privacy is one of the most significant problems in location-based services. However, a user's location can be tracked without her consent or knowledge. The user may also cheat by transmitting a fake location, enabling the user to access a restricted data or content erroneously. Unfortunately, LBSs have raised concerns about system security and users' privacy which leads to issues hindering the wide acceptance of LBS applications is the lack of appropriate methodologies offering fine grain privacy controls to a user without affecting vastly the usability of the service. There have been a number of privacy-preserving and content-protecting models and algorithms proposed in the past few years, including a generalized need to specify one's privacy requirement without understanding its implications on the service quality. These methods are discussed for gathering the work done on the protecting privacy of location based services resulting in user's to have secured private data.***

Keywords: Location privacy, service quality, location-based services, Privacy-supportive LBS, mobile data management

1. Introduction

A location-based service (LBS) is a software application for an IP-capable mobile device that requires knowledge about where the mobile device is located. Location-based services can be based on query that mean user fires a query and provide the end user with useful information such as the nearest ATM or they can be push-based and deliver coupons or other marketing information to customers who are in a specific geographical area.

Location-based services have two important requirements for successful realization privacy and usability. Privacy can be defined as a personally assessed restriction on when and where someone's position is deemed appropriate for disclosure. Usability have two types of meanings: first will be privacy controls should be intuitive yet flexible. Second is the intended purpose of an application is reasonably maintained. But general location based application needs to be supplied with user's private information. However, a user's location can be captured without her consent or knowledge, which can be dangerous for user's privacy.

This is one of the most significant problems in today's application world. The spatial and temporal resolution of location data sent to the server is lowered has been proposed as an early solution. Although this technique is effective in protecting privacy only and the quality of desired services can be severely affected. Location privacy preservation has received significant interests over the past decade, both all over across policy makers and academic researchers.

2. Related Work

In this section, we describe the data used in this paper and relevant background knowledge on privacy and anonymity of location based services.

- Location Obfuscation
- APPLAUS
- LocaWard
- Oblivious transfer and PIR
- I-Clique Cloak Algorithm

We will explain every method in detail in following sections.

3. Location Obfuscation

An individual may deliberately degrade the quality of information about their location in order to protect his or her privacy, a process called obfuscation.

Obfuscation concerns about minimizing the accuracy of the quality of information in some way, to protect the content privacy [1]. It is observed that obfuscation is very effective technique for protecting an individual's location privacy within a pervasive computing environment.

This method provides a computationally efficient mechanism for balancing an individual's need for high-quality information services against that individual's need for location privacy. Here it is considered that the obfuscation of location information, using imperfection of data, to protect an individual's location privacy.

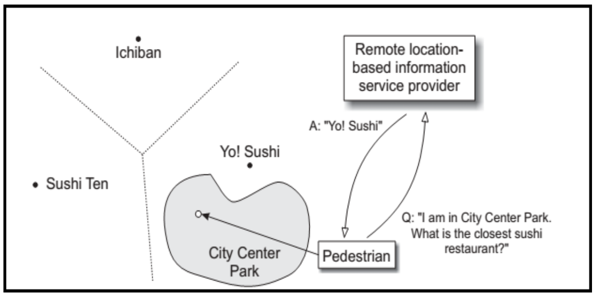
Ichiban
Remote location-based information service provider
A: "Yo! Sushi"
Yo! Sushi
Sushi Ten
Q: "I am in City Center Park. What is the closest sushi restaurant?"
City Center Park
Pedestrian

Figure 1: Idealized example of an obfuscated location-based information service [1]

Key aspects of perturbation process, called obfuscation, are: 1) to allow users to express their privacy preferences in a simple and intuitive way and 2) to enforce the privacy preferences through a set of techniques robust against a relevant class of de-obfuscation attacks. With respect to regulation, privacy policies, anonymity and pseudonymity, this approach have the advantages that obfuscation:

- Is flexible to be for particular purpose to specific user requirements and contexts;
- Obviates the need for high levels of legal and policy infrastructure;
- Enables an individual's identity to be revealed, facilitating authentication and personalization;
- Combats data mining by not revealing an individual's precise location.

Obfuscation is achieved by the use of dummy queries or cloaking regions.

3.1 Dummy formation

In the dummy query method, a user hides her actual query (with the true location) among a set of additional queries with incorrect locations. Among all the locations in the query set an actual location of the user is integrated. The additional processing carries extra data at the LBS, which are an output of the dummy queries, should be addressed while using this method. Cheng et al. has proposed a model for data to augment uncertainty to location data using circular regions around all objects [9]. To apply our anonymous communication technique in LBSs, the following two important issues are shown:

- Realistic dummy movements
- Reduction of communication costs

A new anonymous communication technique for LBSs in which a user sends position data including noise to the service provider is provided. The noise consists of a set of false position data called 'dummies'. The locations of the first dummies are decided randomly because the algorithms use the previous location of dummies.

3.1.1. Moving in a Neighbourhood (MN)

The next position of the dummy is decided in a neighbourhood of the current position of the dummy. In this algorithm, the communication device of the user memorizes the previous position of each dummy. Then the device generates dummies around the memory. They use imprecise queries that hide the location of the query issuer and yield probabilistic results. The results are modelled as the amount of overlap between the query range and the circular region around the queried objects.

3.1.2 Moving in a Limited Neighbourhood (MLN)

The next position of the dummy is also decided in the neighbourhood of the current position of the dummy. However, the next position is limited by the density of the region. This algorithm is adaptable in cases where the communication device of the user can get the position data of other users. First, the user device gets the other user's position data. Next, the device generates dummies around the memory that are the same as the MN algorithm. If there are many users in the generated region, the device generates the dummy again. The process is repeated several times.

Yiu et al. propose an incremental nearest neighbour processing algorithm to retrieve query results [7]. The process starts with an anchor, a location different from that of the user and it proceeds until an accurate query result can be reported. The work focuses on reducing the communication cost of the repeated querying mechanism.

3.2 Location Anonymity

Trusted third-party-based approaches rely on an anonymizer that creates spatial regions to hide the true location of users. The use of spatial and temporal cloaking to obfuscate user locations was first proposed by Gruteser and Grunwald [12]. Continuing on, Gedik and Liu develop a location privacy architecture where each user can specify maximum temporal and spatial tolerances for the cloaking regions [13]. Drawing inspiration from the concept of k anonymity in database privacy [10], Gedik and Liu enforce a location k-anonymity requirement while creating the cloaking regions.

This requirement ensures that the user will not be uniquely located inside the region in a given period of time [11]. Ghinita et al. propose a decentralized architecture to construct an anonymous spatial region and eliminate the need for the centralized anonymizer. Mobile nodes in this method utilize a distributed protocol to self-organize into a fault-tolerant network which is overlaid, from which a k-anonymous cloaking set of users will be generated. Kalnis et al. proposed all obfuscation methods needs to satisfy the property of reciprocity. That will prevent inversion attacks at which place knowledge of the underlying anonymizing algorithm can be used to identify the actual object. Parameter specification remains the biggest hindrance to real-world application of these techniques.

Anonymity concerns the dissociation of location information about an individual from that person's true and valid identity proof. A distinction is normally found between true or verified anonymity, where an every single individual is not possible to distinguish from all other individuals in a set and pseudonymity, where he maintains a secret identity (a pseudonym) that cannot be related to their actual identity.

A variety of research has addressed the problem of maintaining anonymity and pseudonymity within the context of location-based services. Unfortunately, anonymity and pseudonymity are not a complete answer to privacy concerns in pervasive computing because:

- Anonymity presents a barrier to authentication and personalization, which are important for a range of applications.
- Pseudonymity and anonymity are vulnerable to data mining, since identity can often be inferred from location

4. APPLAUS

Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. Proposed method allows person to cheat by transmitting his fake location through his device, which will enable unauthorized person to access a restricted resource erroneously or provide bogus alibis [3]. To address this issue, This system propose A Privacy-Preserving LocAtion proof Updating System (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs and update to a location proof server. APPLAUS which does not rely on the wide deployment of network infrastructure or the expensive trusted computing module is proposed.

Location-sensitive applications require users to prove that they really are (or were) at the claimed locations. In many cases most mobile users have smartphone devices which are capable of discovering their locations; some of the LBS using customers can cheat on their actual locations and which results in lack of secure mechanism to provide their current or past locations to applications and services [12].

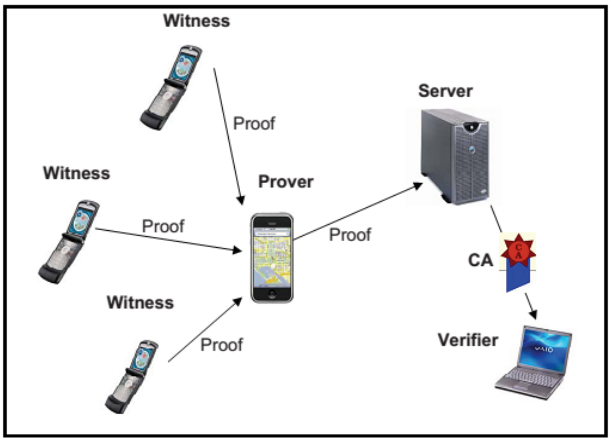

Figure 2: Location Proof Updating Architecture and Message Flow [2]

Periodically changed pseudonyms are used by the mobile devices to protect source location privacy fake people, and from the location proof server which cannot be trusted. This system even developed user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels.

It used statistically changed pseudonyms for each device to protect source location privacy. For extra knowledge, this is the first work to address the joint problem of location proof and location privacy.

Experimental outputs and simulation implementation results have shown that scheme can provide location proofs effectively while preserving the source location privacy at the same time [6].

4.1 Protocol

When a prover needs to collect location proofs at time t, it executes this effective protocol so that it can obtain location proofs from the nodes which are in neighbour within its Bluetooth communication range. Each node uses its **M** pseudonyms $\mathbf{P}_{\mathbf{j=1}}^{\mathbf{M}}$as its identity throughout the communication.

1. The prover broadcasts a location proof request to its neighbouring nodes through Bluetooth interface according to its update scheduling. The request should contain the prover's current pseudonym **P**prov and a random number **R**prov.
2. The witness decides whether to accept the location proof request according to its witness scheduling. Once agreed, it will generate a location proof for both prover and itself and send the proof back to the prover. This location proof includes the prover's pseudonym **P**prov, prover's random number **R**prov, witness's current timestamp **T**witt, witness's pseudonym **P**witt, and their shared location L. This proof is signed and hashed by the witness to make sure that no attacker or prover can modify the location proof and the witness cannot deny this proof. It is also encrypted by the server's public key to prevent from traffic monitoring or eavesdropping attacks.
3. After receiving the location proof, the prover is responsible for submitting this proof to the location proof server. It will also include its pseudonym **P**prov and random number **R**provin the message.
4. An authorized verifier can query the CA for location proofs of a specific prover. This query contains a real identity and a time interval. The CA (Certification Authority) first authenticates the verifier and then converts the real identity to its corresponding pseudonyms during that time period and retrieves their location proofs from the server.
5. The location proof server only returns hashed location rather than the real location to the CA, who then forwards to the verifier. The verifier compares the hashed location with the claimed location acquired from the prover to decide if the claimed location is authentic.

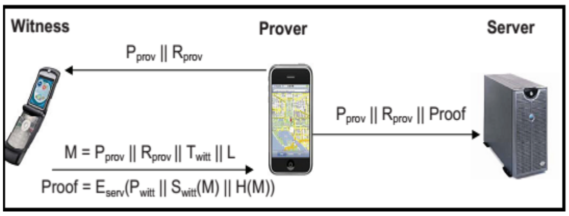
Witness
Prover
Server
$P_{prov} || R_{prov}$
$P_{prov} || R_{prov} ||$ Proof
$M = P_{prov} || R_{prov} || T_{witt} || L$
Proof $= E_{serv}(P_{witt} || S_{witt}(M) || H(M))$

Figure 3: Location Proof Updating Protocol [2]

5. LocaWard

This is a new location-based rewarding system, called LocaWard, where mobile users collect location-based tokens from token distributors and then redeem those tokens at token collectors for rewards. Tokens behave as virtual currency. The token distributors and collectors are any commercial entities who wish to attract customers through such a promotion system, such as stores, restaurants and car rental companies. Systems develop a security and privacy aware location-based rewarding protocol for the LocaWard and prove the completeness and soundness of the protocol. Moreover, it can say that the system is resilient to various attacks and mobile user's privacy gets well protected in the meantime [2].

The proposed system consists of a trusted third party (TTP), mobile users (MUs), token distributors (TDs), token collectors (TCs), and a central controller (CC). The TTP issues each MU with a real identity and a corresponding certificate. A legal MU is able to obtain a location-based token when it visits a commercial entity that participates in the system, i.e., a TD. The tokens at various TDs have the same format but can have different indicated values. With all the collected tokens, an MU can redeem these tokens for beneficial rewards not only at the same store or brand stores, but also at any other retailers or commercial entities, TCs, that have joined the system.

Then, a security and privacy aware location based rewarding protocol is designed for the proposed LocaWard system. Specifically, the protocol is composed of three parts: identity initiation, token distribution and token redemption.

In identity initiation, the TTP issues each MU with an identity and a corresponding certificate. Each MU keeps its identity private and generates a new pseudonym for each token request or redemption. The certificate is used for a user's identity authentication without revealing its real identity.

In token distribution, a TD needs to verify if an MU requesting a token is a legal user in the system without knowing its real ID. After that, the TD issues the MU with an anonymous token which can be redeemed at any TC for rewards. The TD then generates corresponding audition information for the token and sends it instead of the token itself to the CC for future token verification.

In token redemption, a TC first verifies whether the current MU trying to redeem a token is a legal system user, without knowing its real ID. Then, the TC checks to see if the token to be redeemed is intact and has not been tampered. After that, the TC checks if the token does belong to the MU. Later the TC verifies whether the value of the token claimed by the MU is true and if so, distributes the corresponding rewards to him/her. Therefore, no one else other than the TTP can know an MU's real identity. As the CC and TCs only have the knowledge of token audition information, they do not know the content of any token [8].

Since a TD/TC is only aware of the location of the tokens it issued/accepted and there is no central server to store all the historical location information, no entity could figure out any specific MU's location history.

Furthermore the system proves that the system is resilient to various attacks such as multitoken request attack, duplicate token redemption attack, impersonation attack, token tampering attack and colluding attack. And also shows that the MUs' privacy is well protected. It validated the efficiency of LocaWard in terms of computation, communication, energy consumption and storage costs through extensive experiments.

6. Oblivious Transfer and PIR

This approach presents a solution to one of the location-based query problems. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POIs) and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset [4]. It is a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. Due to the nature of the data being exchanged between the user and the server, the frequent changing of the user's name provides little protection for the user's privacy.

This protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR [11], to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

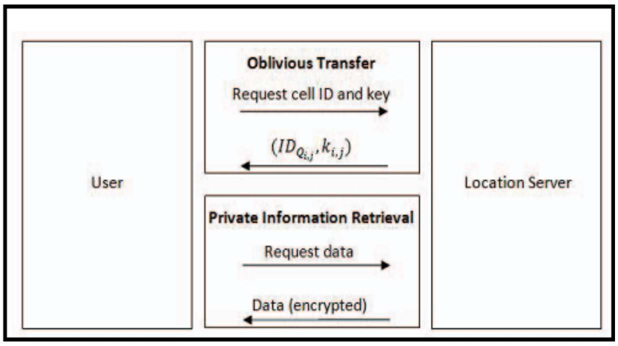

Figure 4: Overview of System Protocol [4]

This protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage. In other words, users cannot gain any more data than what they have paid for.

Some centralized approaches require the LBS to change its operation by, for example, mandating that it process modified queries or that it store data differently. Centralized interventions or substantial changes to the LBS operation would be hard to adopt, simply because the LBS providers would have little incentive to fundamentally change their operation. Indeed, if a revenue stream is to be lost by user data not being collected, then not many LBS providers can be expected to comply. Misaligned incentives have been identified as the root of many security problems [5].

7. I-Clique Clock Algorithm

Here consider the scenario where different location-based query requests are continuously issued by mobile users while they are moving. It is shown that most of the existing k-anonymity location cloaking algorithms are concerned with snapshot user locations only and cannot effectively prevent location-dependent attacks when users' locations are continuously updated.

Therefore, adopting both the location k-anonymity and cloaking granularity as privacy metrics, they have proposed a new incremental clique-based cloaking algorithm, called I Clique Cloak, to defend against location-dependent attacks [10]. The main idea is to incrementally maintain maximal cliques needed for location cloaking in an undirected graph that takes into consideration the effect of continuous location updates. Thus, a qualified clique can be quickly identified and used to generate the cloaked region when a new request arrives. The efficiency and effectiveness of the proposed I Clique Cloak algorithm are validated by a series of carefully designed experiments.

The results of implemented system have shown that the price paid for defending against location-dependent attacks is small.

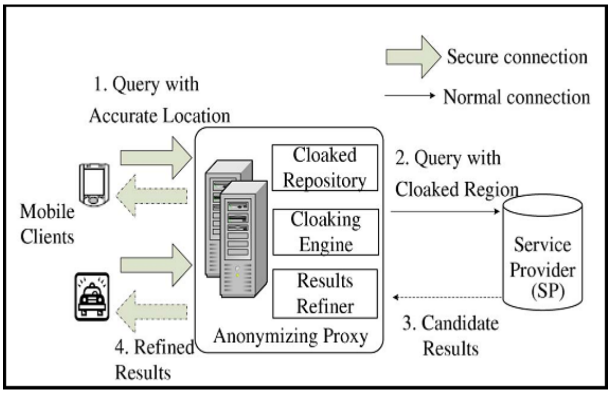

Figure 5: System architecture for clocking region [13]

Algorithm 1: ICliqueCloak Algorithm
Input: A set of requests awaiting for anonymization, a new query requestu.
Output: A set of cloaked requests.

Step 1: Incrementally update the max-clique set for the new request u.
Step 2: Find the cloaking set CS_{ti} satisfying location k anonymity from the max-clique set.
Step 3: Generate the cloaked region for CS_{ti}.
Step 4: Update the max-clique set upon request Cloaking or expiration.

8. Comparison

Table 1: Comparison between different approaches

No	*Approach*	*Advantages*	*Disadvantages*
1	Location obfuscation	Allow users to express their privacy preferences	Degraded quality of service to user
2	APPLAUS	Provides location proofs effectively also preserves the source privacy	Computation time is costly and colliding attacks detection ratio is low
3	LocaWard	Resilient to various attacks such as multi token request attack	Do not provide security to general LBS
4	Oblivious Transfer and PIR	Computationally and also in communication more efficient	The overhead of the primality test is larger
5	IClique Cloak	Effectively prevent location-dependent attacks when locations are updated	The cost for location dependent attacks is small

9. Conclusion

A detailed survey of Privacy approaches for Location based services in particular is done giving their major advantages and limitations. Also inclusive study of each approach individually is completed. The study gives a baseline for additional research in privacy of user's personal location data and a user can decide the impact of location inaccuracy on the service accuracy before giving away his actual location.

References

[1] Matt Duckham and Lars Kulik, A Formal Model of Obfuscation and Negotiation for Location Privacy, Germany: Springer-Verlag, 2001.
[2] Ming Li, Sergio Salinas and Pan Li, LocaWard: A Security and Privacy Aware Location-Based Rewarding System, IEEE Transaction On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014

[3] Zhichao Zhu and Guohong Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System," IEEE Transaction On Mobile Computing, Vol. 12, No. 1, January 2013.

[4] Russell Paulet, Md. GolamKaosar, Xun Yi, and Elisa Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries," IEEE transaction on knowledge and data engineering.

[5] Reza Shokri, George Theodorakopoulos, PanosPapadimitratos, Ehsan Kazemi, and Jean-Pierre Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration," IEEE transaction on Dependable And Secure Computing, Vol. 11, No. 3, May-June 2014.

[6] Zhichao Zhu and Guohong Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services", IEEE INFOCOM 2011.

[7] Hui Zang and Jean Bolot, "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study", MobiCom'11, September 19–23, 2011, Las Vegas, Nevada, USA.

[8] Rinku Dewri, Member and Ramakrisha Thurimella," Exploiting Service Similarity for Privacy in Location-Based Search Queries", IEEE Transaction on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

[9] Hidetoshi Kido, Yutaka Yanagisawa and Tetsuji Satoh, "An Anonymous Communication Technique using Dummies for Location-based Services".

[10] Xion Pan, Jianliang Xu and XiafengMeng,"Protecting Location Privacy against Location-Dependent Attacks in Mobile Services", IEEE transaction on Knowledge and data engineering, Vol. 24, No. 8, August 2012.

[11] M.L. Yiu, C.S. Jensen, X. Huang and H. Lu, "Space Twits: Managing the Trade-offs Among Location Privacy, Query Performance and Query Accuracy in Mobile Services", Proc., 24th Int'l Conf. Data Eng., pp. 366-375,2008.

[12] M. Gruteser and D. Grunwald, "Anonymous Usage of Location Based Services through Spatial and Temporal Cloaking,"Proc. First Int'l Conf. Mobile Systems, Applications and Services, pp. 31-42, 2003.

[13] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," IEEE Trans.Mobile Computing,vol. 7, no. 1, pp. 1-18, Jan. 2008.

Author Profile

Sneha Sonwane received the B.E. degree in Computer Engineering from Bharati Vidyapeeth College of Engineering for Women, Dhankawdi, Katraj, Pune in 2012. And she is now pursuing her M.E. degree from D.Y. Patil College of Engineering, Akurdi, Pune.