South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 12–18

ISSN No: 2454-9614

A Survey on Enhancing Privacy in Geosocial Application using LocX

P. Kruthika[a], T. Sounder Rajan[a*], N. Sharmila[a,b]

[a)] *Department Of Computer Science and Engineering, KSR Institute for Engineering and Technology, Tiruchengode, Tamilnadu, India.*
[b)] *Department Of Computer Science and Engineering, KSR Institute for Engineering and Technology, Tiruchengode, Tamilnadu, India.*
[c)] *Department Of Computer Science and Engineering, KSR Institute for Engineering and Technology, Tiruchengode, Tamilnadu, India.*

*Corresponding Author: P. Kruthika

E-mail: kruthika9293@gmail.com,
Received: 01/11/2015, Revised: 22/12/2015 and Accepted: 25/02/2016

Abstract

Geo social networks are the new trend in the social networking now a day. With the advance in the smart phone and internet technology they are achieving more popularity than before. These geo social networking sites make use of the location information of the users. So location privacy of the users is a very big concern. Without adequate privacy protection, however, these systems can be easily misused, *e.g.*, to track users or target them for home invasion. So an added privacy must be provided in order to preserve the location of the users. In this paper we compare the different location privacy settings that can be introduced in geo social applications and different methods that are now adopted to provide security to the users.

Keywords: Security, Location privacy, Tor, Longitude, Location to Index Mapping, PIR protocol, location-based social applications.
Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Geo social networking is a new mode of social networking and is an emerging trend today **[1].** People always use to collect information by asking other people even when they have access to large amount information such as the Internet and libraries. This is because people are good resources reservoirs. Social networking becomes so popular because of this main reason. Now in social networking geo social networking works with the location information and data provided by different users and this can be utilized by people to get valuable information about different places and things. Best examples of geo social networking sites are Foursquare and SCVNGR. Since these geo social networking sites make use of the location information of the users to locate places and reviews, this is a great threat to the location privacy of the users. Many location based attacks, economic damages, harassments have

been reported so far due to the lack in privacy setting in these geo social applications **[2], [3].** Since these applications have a large number users now a days it need more stronger privacy setting than the open to all policy available now. In the current scenario for proving location security for the users the geo social networks adopts mainly three techniques.

First one is introducing some kind of error to the latitude and longitude of a particular location while storing this to servers. The second method is storing the location information in trusted servers. Third one is usage of heavy weight cryptography and private information retrieval techniques.

Each of these techniques has its own demerits. The first method needs both the user and server to add error to the accurate data. It won't provide accurate information for the needy and is not a trustworthy method, but it is most widely method used today. The second method i.e., depending on trusted servers is a good option but it also has some drawbacks such as a software bug, hardware misconfiguration etc., can expose the private data to risk. The third method that is using heavy weight cryptographic methods is more expensive and more complicated to be implemented into mobile devices.

2. Related work

Location-based services are emerging as the next killer app in personal wireless devices, but there are few safeguards on location privacy **[4].** In fact, the demand for improved public safety is pushing regulation in the opposite direction. The challenge with wireless location privacy is making it easy to share the right information with the right people or service at the right time and, conversely. In addition, the corporate world can discover and match a person's location trail to create unwelcome spam. Disclosure of location information may cause embarrassment or humiliation.

Information about a person's movements or activities can result in financial losses. Positioning technologies have the potential to intrude on personal privacy. Information about a person's movements or activities can result in financial losses. Managing privacy in the network is one of the most challenging aspects of wireless location privacy. Different privacy risks related to location are Economic damages, Location-based spam, Harm to a reputation i.e., Information about a person's movements or activities can result in financial losses. The Cyber marketers could bombard a mobile device with customize voice and data ads for stores, restaurants, and other businesses as an individual strolls through a mall. Disclosure of location information may cause embarrassment or humiliation. If taken out of context, location information could also lead others to make incorrect inferences that unjustly tarnish a person's reputation.

There are different ways in which privacy can be preserved. The main thing among them is the selection of positioning system. Positioning systems fall into one of three categories. In the *network-based* approach, infrastructure receivers such as cell towers their own position, as is the case with a GPS unit. In terms of privacy, client-based positioning is fundamentally better than network-based or network-assisted tracking because it does not

reveal any location information to the network unless the user decides to communicate. Another measure is the use of intermittent connectivity. For example, Figure 2.1 shows a model in which mobile devices avoid revealing precise location information by retrieving geographically coded records one set at a time rather than individually through separate queries. *Intermittent connectivity* is a powerful mechanism **[4],** but it is only useful for specific kinds of services in which data changes relatively slowly.

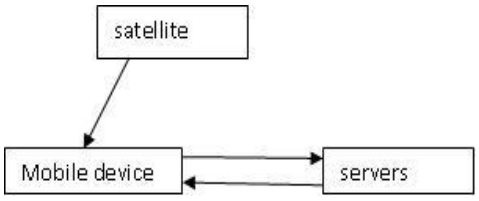

Fig 2.1 Intermittent Connectivity

Another method is providing strong user interface so that the users will be aware that their location information is used by the applications **[1].** Fixed home agents are another method by which location information can be hidden. For certain types of geo-social services, such as services like testing if a friend is nearby, some recent proposals are there which have a guaranteed location privacy with the usage of expensive cryptographic techniques such as secure two party computation

2.1 Longitude

Longitude is a work which adopts this technique **[4].** Longitude transforms locations coordinates to prevent disclosure to the servers. In Longitude, the secrets for transformation are maintained between every pair of friends in order to allow users to selectively disclose locations to friends. Longitude eases privacy concerns by making it possible to share a user's location data blindly and allowing the user to control who can access her location, when and to what degree of precision. This is with the help of cryptographic algorithms and this can be adapted to mobile phones also. Here in the system model it consists of a location-sharing service provider and the set of users registered with the provider. The provider store location along with some data. The user can determine which other users should view their data's. The security model assumes that the server is honest but curious about user's detailed location and information. The longitude protocol is based on proxy encryption **[9].** Here the user register with the service provider, the service provider provide them with some cryptographic elements. This can be saved safely in the user devices.

Whenever a user a wants to know about the location information of user B, user A sends a request to user B along with his own public key. If user B wants to revel his information to A, user B computes a re-encryption key using user A's public key and his own private key and also decides how accurate the location should be for user A and generates a corresponding precision mask The re-encryption key and the precision mask are sent to the service provider C, and act as an authorization policy that allows A to retrieve B's location. Friend revocation methods are used if the user doesn't wants to share his information with other users. In simple revocation method the user can ask the provider not to share the location to other user. If the provider colludes then B can use strong revocation by

updating his keys. Updating only changes two components in his keys and leaves the other parts unchanged. B also updates the re-encryption keys for all friends except A.

2.2 The Onion Router

One of the most widely used system for providing online anomaly to the user is software known as Tor **[5].** Tor is a circuit-based low-latency anonymous communication service. Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable trade-off between anonymity, usability, and efficiency **[6].** People use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Using Tor protects against a common Internet surveillance known as "traffic analysis." Knowing the source and destination of a user's Internet traffic allows others people to track the user's behaviour and interests.

The Tor network is an overlay network; each onion router (OR) runs as a normal user-level process without any special privileges. Onion Routers maintain among them a transport layer security connection. Each user run local software known as onion proxy and establishes circuits across the network, and handle connections from user applications. To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken **[7].** Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Traffic flows down the circuit in fixed-size *cells*, which are unwrapped by a symmetric key at each node i.e., like the layers of an onion and relayed downstream. When the packet reaches the last relay it will be fully unwrapped and then send to the destination.

2.3 PIR Protocol

PIR **[8]** resulted in protocols that allow a client to privately retrieve information from a database, without the database server learning what particular information the client has requested. It uses PIR protocols and eliminates the need for any trusted third party.PIR technique is the first to provide provable privacy guarantees against correlation attacks.

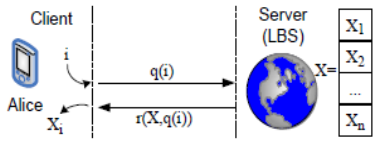

Fig.2.2

Most techniques are expressed in a theoretical setting, where the database is an *n*-bit binary string *X* (see Figure 2.2). The client wants to find the value of the *ith* bit of *X* (i.e., *Xi*). To preserve privacy, the client sends an

encrypted request $q(i)$ to the server. The server responds with a value $r(X, q(i))$, which allows the client to compute Xi. PIR does not disclose *any* spatial information. As opposed to CR-based methods (which only perturb location, but still disclose the CR), no location information is disclosed. Instead, the data (i.e., POIs) are retrieved based on object index, by employing the provably private PIR protocol. This approach prevents any type of attack based on user location.

PIR protects against correlation attacks. Assume that *u* asks a continuous query as he moves. Existing methods generate one cloaking region *CRi* per location, but all *CRi* will include *u*. By intersecting the set of users in all *CRi*, an attacker can identify *u* with high probability; this is called *correlation attack*. Note that this attack is possible because the CR reveals spatial information. Since the PIR framework does not reveal any spatial information, *u* is protected against correlation attacks. PIR does not require any trusted third party, since privacy is achieved through cryptographic techniques. Existing techniques, on the other hand, need: (i) An anonymizer, which is a single point of attack, and (ii) A large set *U0* of subscribed users, all of whom must be trustworthy, since malicious users may collude to reveal the location of *u*. Furthermore, users in *U0* must accept the cost of sending frequent location updates to the anonymizer, even if they do not ask queries.

2.4 Location to Index Mapping

Location to index mapping is another approach towards location privacy of users **[9].** Here in this system the data and location are partitioned into two components and are stored in separate servers. The authorized person with the necessary credentials can only access the location information of the users. The location is stored in a server called as index server via another un-trusted server called as proxy server. Proxy server is used in order for preventing the index server from uniquely identifying the client devices. Here the location information is transferred to another coordinate system and this is known as transformed location. Each user will be provided with an element which consists of a shift, a rotation angle, and an encryption key. Here in this system this element will be shared with trusted friends circle.

The location is transformed using the shift and rotation in the secret element of the particular user. This transformed location will be encrypted by the encryption key of the particular user and will be stored in the index server via the proxy server in a unique index. The data is encrypted and stored into the data server directly in previously defined unique index. A person who has the decryption key, rotation and shift only can retrieve the data from the index and data servers. If user B want to know about the location information and corresponding data that A has put on the server, then user B with the right elements need to transform the specific location to be known to the transformed coordinate of user A and this need to be send to the proxy server and from proxy this request will be redirected to the index server and the corresponding index for the data will be retrieved to the user B. With this index user B can request for data corresponding to the index in the data server and the encrypted data will be retrieved to the user. Using the decryption key user can decrypt the information related to the particular location.

3. Comparison

There are different problems associated with the location based networking such as different real time problems that people facing. Different solutions such as intermittent connectivity, improving the user interfaces of the application with notifications etc. are some of the good methods to assure location privacy to the users. Longitude is a good measure towards location privacy **[4].** Here the information is shared among needy users only. The major drawback of the system is the complex encryption, which will be time consuming but provide more privacy to the user. Also in Longitude, the secrets for transformation are maintained between every pair of friends in order to allow users to selectively disclose locations to friends.

The second generation onion router or Tor provide anonymity for user and is a strong shield against traffic analysis. This approach seems to provide privacy as the server only sees location data but not the identity of the user behind that data **[6].** However, recent research has revealed that hiding the identity of the users alone is not sufficient to protect location privacy. Attacks can be done at the rear end of the circuit were node send the packet fully decrypted to the source station **[7].** Even if Tor is used, it is possible for an attacker with access to the location data to violate our privacy and unlink ability requirements. Computational PIR Protocol**[8]** address for the correlation attacks, BNC(bench mark) and AHG(Aggregate Hilbert Grid) in this information are stored in DB and retrieved via queries using secure PIR , Louis, Lester, Pierre Protocol the person checks for the availability of their friends and share the information . A person checks for the availability of their friends and share the information.

Location to index mapping method is a novel approach towards location privacy of the users **[9]**. It makes use of the location transformation method that is introduced in the Longitude protocol and also it introduces a mechanism which split the data and location into two parts and storing these data and location in different servers. Transformation along with splitting of data and location provides the system with more security. It adds little computational and communication overhead to existing systems. This system is a bigger step towards overcoming the location privacy of the user.

Both longitude and location to index mapping make use of the location transformation of the users. But in longitude the cryptographic elements are maintained between each pair of friends and friends can be un-trusted entities so revocation methods need to be implemented. Different revocation techniques are used in Longitude based on whether the service provider colludes or not. Blocking of the un-trusted entities can be done with the help of the service provider if the provider does not collude and if the provider collude the cryptographic elements for every entity except the un-trusted entities. But in location to index mapping this problem is not there since friends are considered as trusted entities. The Table 3.1 shows different characterizes of both longitude and location to index mapping.

Table 3.1 Comparison of Characteristics

Characteristics	Longitude	Location to index mapping
Location transformation	yes	Yes
Splitting of data and location	no	yes
Cryptographic element for each set of friend	yes	no
Proxy re-encryption	yes	no
Public and private key elements	yes	no
Entity set	Trusted/untrusted	Trusted
Revocation	yes	no

4. Conclusion

Geo social networking is one of the most emerging trends today. With the advance in the networking technology lots of privacy related issues are also emerging in the real world. In this paper we discussed different privacy related issues and some solutions which can be adopted in the existing system. Longitude is protocol that introduced location transformation and works on two ways secure key. Longitude's proxy re-encryption scheme is provably secure and the cryptographic functions optimized for mobile platforms but have computational overhead. Tor is software that can be used for providing online anonymity. But new research found that attacks can be made between the final relay and the destination. Location to index mapping is a new mechanism which adopts the location transformation from longitude protocol and also introduces splitting of location and data into two parts and storing it in different servers. The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. This adds little computational and communication overhead to existing systems. Location to index mapping takes a big step towards making location privacy practical for a large class of emerging geo-social applications.

References

[1] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection, *"Computer*, vol. 36, no. 12, pp. 135–137,2003
[2] F. Grace, "Stalker Victims Should Check For GPS," Feb. 2003, www.cbsnews.com.
[3] "Police: Thieves robbed homes based on facebook, social media sites," WMUR News, September
[4] http://www.wmur.com/r/24943582/detail.html. 2010.
[5] Changyu Dong, NarankerDulay,"Longitude: a Privacy-preserving Location Sharing Protocol for Mobile Applications"
[6] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *USENIX Security Symposium*, 2004
[7] www.torproject.org.
[8] S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbour Search with Strong Location Privacy," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.
[9] Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Fellow, IEEE, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao," Preserving Location Privacy in Geosocial Applications".