International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on Location Privacy in Location Based Services

M. S. Patil[1], S. H. Sutar[2]

[1]PG scholar, Department of Computer Engineering, MIT College of Engineering, Pune, Maharashtra, India

[2]Assistant Professor, Department of Computer Engineering, MIT College of Engineering, Pune, Maharashtra, India

Abstract: ***Now a day's use of smart phones and tablets is drastically increased. Various services are available to us by just one click on our mobile devices one such a service is Location Based service .User send the query to service provider to get services like nearby restaurant, friends in vicinity, share his/her location with other friends,rendezvous point to meetetc .But getting a desired service is not enough as location privacy is always one of the greatest concerns of the user. There are various threat to privacy when user shares his/her location. The information can be misused for stalking, home invasion, political loss etc. Various methods were introduced in past to deal with privacy concerns. This paper explores different methods to deal with privacy concerns.***

Keywords: Privacy, Location Based services

1. Introduction

The rapid abundance of smart phone technology has enabled user to utilize context aware services on their mobile phones. One such service is Location Based Service (LBS). Using the current locationof user different services are offer to him/her. Location based services are again of two categories the one in which services are offer based on users current location by service provider like weather condition, route navigation etc. while others are location sharing based services like recommendations for nearby coffee shop, restaurant for dinning , rendezvous point to meet, friend finder etc. Facebook Places, Banjo, Foursquare are some of the Location based service provider which are getting popular now a days.

Even though various LBS are getting popular now a day's, the success of any service is based on trust of the user on service provider. The location of user is getting share with service provider, there is a possibility that this information might be get misused to carry out activities that affect user like stalking, home invasion, political affiliation etc. When user shares his/her current location with service provider a malicious person may track it. Any location information shared by user might be collected by malicious user and he may link it with publicly available database. Knowledge that he inferredfrom it might be used to carry out malicious activities. Hence there is need to provide privacy to location information. Various methods were introduced in past to provide location privacy. We discuss some methods here

A) Anonymity

One of the popular method used to achieve location privacy is K-anonymity. The basic principle of it is to hide the user among other k-1 user so that probability of identifying the user get reduces to 1/k, where k represents minimum number of users in cloaked region. In this method anonymizer server is placed between user and LBS server. User sends his/ her query over secure link to Anonymizer. Anonymizer removes the identity information such as network address and then forwards the cloaked region generated following cloaking algorithm to LBS. Anonymizer creates cloaked region containing k-1 user along with the user who issue the query. This cloaked region is then sent to LBS server. Server find out the query result for each of the user in cloaked region and send result back to the anonymizer. There different methods to create a cloaked region, here we had discuss some of the methods.

We first discuss interval cloak method [1].The user sends his/her location to anonymizer over authenticated and encrypted connection. Anonymizer decrypts the message, remove identity information and apply spatial-temporal cloaking algorithm to generate a cloaked region. The location information is represented as ([x1,x2],[y1,y2],[t1,t2]), where([x1,x2][y1,y2]) represents area where user is located and [t1,t2] represents time interval for which user is in that area. The anonymizer creates a cloaked region containing k-l user along with user who issues the query by using quad tree algorithm. The quad tree algorithm recursively partition space into quadrant until quadrant contains the requester and other user having count is less than k. The previous quadrant that satisfies the threshold requirement is return. Whenever a query is made the quad tree is traverse until quadrant satisfying anonymity requirement get detected. In this method the value of k is always fixed. But some time for particular region number of users are less than k, hence temporal cloaking is needed to apply so that the number of user becomes k in the cloaked region. To achieve this anonymizer has to wait until number of user in cloaked region equal to k. The method is easy to implement but delay associated with sending a request to server while archiving k-anonymity in temporal cloaking causes degradation in quality of service. Also this method fails to preserve anonymity for outliers.

The second method is Casper method [5].Casper framework mainly consists of location anonymizer and privacy profile query processor. Location anonymizer does the same work of creating cloaked region using quad tree, but using the privacy profile of the user. Casper provides flexibility to user to decide the value of k and A_{min} in their privacy profile. Here A_{min} represent accepted resolution of cloaked spatial region. The anonymization scheme is based on pyramid data

structure containing grid of location cells. Cells are arranged in ascending resolution towards higher level and each cell in higher level corresponds to four cells in lower level. Anonymizer contains the hash table containing information about user id and cell id in which user lies. If it satisfies the user privacy profile then the cell is forwarded to LBS otherwise vertical and horizontal neighbor of cells are getting checked when service is requested. If the combination cells with its neighbor satisfy the spatial requirement then it is forwarded to LBS. Even though this method provides better level of privacy than previous method this method shows degradation in query performance if the size of quadrant gets bigger.

One more method to archive Anonymization is using clique cloak algorithm [3]. Clique cloak algorithm group together number of requests and then pass it to LBS server. Each user has his privacy profile which specifies its anonymity requirement - value of k, space dimension tolerance and time dimension tolerance used while creating cloaked region. Each user is associated with some Constraint Area. A constraint area prevent the LBS server from sending the client useless information on locations outside the constraint area. Using the constraint area of multiple user minimum bounding Rectangle (MBR) is created such that MBR contain at least k users along with requestor. Clique is created by considering users in MBR as vertices and joining them by edges. Then message is removed from anonymizer and forwarded to LBS server in the form of cloaked region. This algorithm ensure that a cloaked spatial region R contains at least k users and all these k users report R as their cloaked regions make it free from location distribution attack / query sampling attack. But this method requires high computational cost as creating and searching a clique in graph takes time. Also this method degrades quality of service as some request cannot be anonymized as they doesn't form clique and will be drop when their life time expires.

B) Mix Zone

Mix zone[2] method to achieves privacy is using Pseudonyms. 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. Whenever user enters in mix zone new pseudonyms is assign to it. Mix zone is area where location of user is kept hidden. No application can trace user movement in this area. Server does not receive traceable identity within this area but instead of this they receive pseudonyms. Using pseudonym communication between user and application is carried out through intermediary to prevent linking of pseudonyms with underlying user identity. As there might be number of users in mix zone who enters and leaves in same time zone and therefore upon emerging from the mix zone, an adversary cannot know which one of the users has cameout. The drawback of this method is it lacks when used for multiple responders.

c) Location transformation:

Location transformation is one of the methods to archive location privacy in which instead of sending the actual location co-ordinates to LBS server, transform values are send. As the locations are transformed malicious user won't be able to infer actual location of user. There are various method to carry out transformation, it can be carried out by transformation using scaling, rotation, translation of location co-ordinates or changing the 2-D space co-ordinates in 1-D space.

The one of the novel way of blindly evaluating KNN queries is using one way space transformation [6]. To archive this Static point in 2-D space as well as dynamic query points are mapped into other space using a one –way transformation and query is evaluated on transformed space. They uses Hilbert curve for transformation it preserves the proximity of points in 1-D space similar to 2-D space. This approach provides a-anonymity, u-anonymity. a-anonymity ensure while evaluating KNN query the location of query point should not get revealed, while u-anonymity ensures that user issuing the query remain indistinguishable from among the entire set of user.

Another method is multiple transformations which is used to provide location privacy to moving objects [9]. Multiple transformations make relative distance hard to infer as compared to single transformation function. The transformation used by author is a combination of scaling, rotation and translation. The Group of agents are placed between user and LBS server. Whenever user wants to update his/her location information at server the data is passed through one of the agent which carried out identity and location transformation. As multiple functions are used in agent for carrying out transformation the count related to function is updated. Multiple functions and multiple agents are used to avoid correlating request from particular agent by server. Here agent is thin intermediate server as it doesn't store users current location but only keep the track of function applied during transformation and also function get removed if it is not used by any user as count reaches to zero. Whenever user wants to issue query the query is send to all agent. Each agent form super query and then forward it to server. The server compute the result send it to agent which again carry out retransformation and send the result back to requestor. In this way this technique prevents the service provider from knowing the exact locations of users and also protects information about user movements. But drawback this method is lot of computation is needed to carry out to achieve privacy.

D) Dummies

In this approach along with sending actual location of the user certain false location i.e. Dummies are also send to service provider. Because of this LBS server won't able to distinguish between real user and dummies.LBS server run the query for each of the location and returns the result. At user side user filter out replay for dummies and use replay only for his/her current location

In the first method author propose two algorithms to generate dummies. If dummies are generated randomly when continuous position data is send to service provider, observer can easily find out difference between real user and dummies as distance travel in particular time is fixed and dummies violate this property. To overcome this problem author proposes two algorithms moving in neighborhood and Moving in a Limited Neighborhood. In moving in

neighborhood algorithm the next position of dummy is decided in neighborhood of position. Communication device memory stores the previous location of dummies. While in moving in limited neighborhood algorithm next position of dummy is based on density of region. In this technique user can get the position of other users in same region so if density is high, device regenerate new dummies. The advantage of this method is it is easily integrate with existing mobile network. But if long term observations are done by malicious user he/she can detect trajectory of user and once trajectory is users location can get inferred. Hence it reduce level of privacy [4].

To overcome this problem author of paper [7] suggest three parameter that to be consider while creating dummies to avoid detection of trajectory. Three parameters are short term disclosure, long term disclosure, distance deviation. These three parameters provide protection to user's trajectory. Short term disclosure parameter specifies requirement for protecting the current user location while long term disclosure specifies the requirement for protecting users trajectory. Distance deviation specifies the average deviation among the user and dummies trajectory. User set up this three parameter in their privacy profile. There are two schemes to create trajectory using privacy profile

- Random pattern: In this the starting point and the destination of a dummy are recognized and based on this grid cells between the starting point and the destination are form. Then a dummy will move randomly from the starting point towards the destination making it difficult for the adversary to identify the user pattern.
- Rotational pattern: In this pattern intersection between users and dummies trajectory is carried out. A new trajectory for dummy is created by rotating the known users trajectory.

E) Cryptography and No third party trusted server

Until now we reviewed various methods that uses intermediate trusted server to carry out location transformation or to create cloaked region. But advancement in cryptography made it possible to achieve location privacy without using trusted third party.

The Private Information Retrieval (PIR) using special secure hardware[8]. The main idea of PIR to let the user privately retrieve the information from database without letting know the server what particular information user has requested as well as what information is returned.User sends the PIR queries to server and server send the cipher version of blocks containing requested POIs. The cipher version of block is only deciphered by user only. It provides high level of privacy. But Special type of hardware is required to implement this method make this method costly.

One of the novel approach to archive location privacy in geo-social application is Locx[10]. Geo-social applications are based on location sharing system. In Geo-social application location information can be infer from geo-tag also, hence along with providing privacy to location, data privacy is also needed to provided to geo-tag and location information generated by them(comments, recommendation etc.).Hence LocX separate data and location co-ordinate different servers data server and index server. Because of this attacker won't be able to link the location and data, hence won't be able to back track the user. In this method user share some secrets with each other that include symmetric key and transformation parameter.

Whenever user wants to update his/her location information, application first generates random index. Encrypt the index and data using symmetric key.Then transform the co-ordinates using his/her transformation parameter. Then encrypted index and transform parameters are stored at index server and index and encrypted data is stored at data server. When friend of user want to access the information when he comes to same location, he/she query the server for information First application transforms the current location using friends transformation parameter of which data he wants and then query the index server either circular or range query then index server run the query and sends encrypted index.

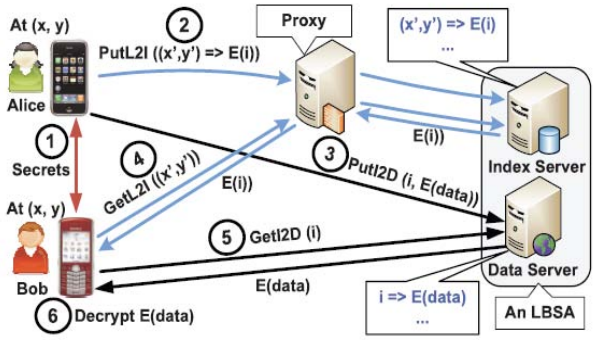

Figure 1: LocX system [10]

Application receives encrypted index and decrypts index and again query data server for data. Data server finds matching index and returns corresponding encrypted data to application. Again application decrypts data and represents it to user. In this way system provides location privacy to user without injecting any error in result and also does not rely on any trusted third party.

2. Conclusion and Future Work

Each method we studied here has some advantages and disadvantages. With advancement in cryptography technique made it possible to drop the trusted third party between user and LBS server, avoid transformation of location co-ordinates.LocX is one of the good options to archive privacy in Geo-social application but it result into high computational and communication overhead. To overcome this problem we propose a system which also store location co-ordinate and data at different server at index server and data server respectively but instead using transformation method the proposed system will store the co-ordinate in encrypted form. The proposed system uses asymmetric key cryptography method. The up loader one who wants to update data, upload co-ordinate at to index server as encrypted index and encrypted co-ordinate and upload encrypted data at data server. Whenever his friend wants to access data when comes to same location it query the index server and index server will return list of index and for that list of index corresponding data is requested from data

server. Data server again sends encrypted data to requester and requester decrypt it and use it.

Reference

[1] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proc.First Int'l Conf. Mobile Systems, Applications Services,2003.
[2] Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004.
[3] Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems, 2005
[4] 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.
[5] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Proc. IEEE 23rd Int'l Conf. Data Eng., 2007.
[6] Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, 2007.
[7] You T-H, Peng W-C, Lee W-C (2007) Protecting moving trajectories with dummies. In: International workshop on privacy-aware location-based mobile services (PALMS 2007),
[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management Data,2008
[9] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Location Privacy in Moving-Object Environments," Transactions on Data Privacy, vol. 2, no. 1, pp. 21-46, 2009
[10] Krishna P. N. Puttaswamy , Shiyuan Wang , Troy Steinbauer , Divyakant Agrawal , Amr El Abbadi , Christopher Kruegel , Ben Y. Zhao, , Preserving Location Privacy in Geosocial Applications, IEEE Transactions on Mobile Computing, v.13 n.1, p.159-173, January 2014