IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 4 (Mar. - Apr. 2013), PP 46-49
www.iosrjournals.org

Generating random regions in Spatial cloaking algorithm for location privacy preservation

Mrs. Suchita R. Shastry, Prof Dr.P.K.Deshmukh, Prof.Dr.A.B.Bagwan,
Department of Computer Engineering, Rajarshi Shahu College of EngineeringUniversity of Pune Tathawade, Pune 411033. India.

Abstract: *Location based Servers (LBS) include services to identify a location. Network users expect to access services relevant to their locations, and preserve their privacy without disclosing their exact location. The spatial cloaking method provides the solution where exact location of user gets hazy. In peer to peer network (P2P), communication between the peers becomes time consuming and communication overhead. In this paper we have proposed the method where instead of communicating with peers, user directly communicates with LBS. we have presented two algorithms where first algorithm which where the LBS provide the direct list of in ascending order. The second algorithm for query processing generates the region of different shapes which minimizes the chances of getting the user disclosed to adversary.*
Index Terms—*Location Based Service(LBS), Privacy Preserving, Spatial Cloaking, k- anonymity,*

I. Introduction

The explosive growth in the usage of smart phones and the increased availability of wireless and GSM connection has allowed users to connect to the Internet, use web services or other types of custom services, send and receive data from any place and at any time. Network users expect to access services relevant to their locations, even as preserve their privacy without disclose their exact locations. The well-known privacy preserving method is the spatial cloaking technique where exact user locations are blurred into a cloaked region to meet the privacy requirement. This is applied by using K-anonymity [1], and cloaked region. In mobile P2P networks where no centralized servers are possible, an LBS provider collaborates with other peers via multi-hop communication to blur her location into a cloaked area.

II. Location Based Services (Lbs)

Location-based services are a general class of computer program-level services used to include specific controls for location and time data as control features in computer programs. LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. The increased availability of wireless and GSM connection has allowed users to connect to the Internet, use web services, user can access the information anytime and anywhere Moreover, the developments in positioning technologies like GPS, wireless positioning, GSM etc has allowed for tracing users' location, storing it, processing and even easily rendering it on a map. Cellular phones, global positioning system (GPS) devices and radio-frequency identification (RFID) chips [4] results in a location- dependent information access paradigm, known as location-based services. Typical examples of LBS include local business search, e-marketing, social networking, and automotive traffic monitoring. Although LBS provide valuable services for mobile users, revealing their private locations to potentially untrusted LBS service providers pose privacy concerns. In general, there are two types of LBS, namely, snapshot and continuous LBS. For snapshot LBS, a mobile user only needs to report its current location to a service provider once to get its desired information. On the other hand, a mobile user has to report its location to a service provider in a periodic or on-demand manner to obtain its desired continuous LBS.

Protecting user location privacy for continuous LBS is more challenging than snapshot LBS because adversaries may use the spatial and temporal correlations in the user's a sequence of location samples to infer the user's location information with a higher degree of certainty. A classic example of LBS applications using SMS is the delivery of mobile coupons or discounts to mobile subscribers who are near to advertising restaurants, cafes, movie theatres. In LBS, mobile users have the ability to issue location-based queries to the location-based database server.

III. Spatial Cloaking

Since LBS is provided for users based on their exact location information, a major threat about the user's location privacy has been raised. Recently, spatial cloaking has been widely used to tackle such a privacy

breach in LBS. The basic idea of the spatial cloaking technique is to blur a user's exact location into a cloaked area such that the cloaked area satisfies the user specified privacy requirements. A *cloaking area* is defined as an area which includes the current position of a mobile device for the purpose of hiding an exact position. Based on using a cloaking area, the adversary cannot easily breach a mobile user's privacy since the exact current position is abstracted.

K- Anonymity

In spatial cloaking, user location is enlarged into a cloaked region that is then used for querying the server. One of the main goals in those studies is to provide *k*-anonymity. A message from a client to a database is called location anonymous if the client's identity cannot be distinguished from other users based on the client's location information. The *k*-anonymity model with respect to location information was defined as follows: A query message from a user to a server is called *k*-anonymous in location-based services if the user cannot be identified by the server based on the user location from the other $k - 1$ users where k is a user-specified anonymity set size. This is the most popular privacy requirements for the spatial cloaking technique. To achieve k-anonymity, i.e., a user is indistinguishable among other k−1 users.

IV. System Model

Mobile users adopting the spatial cloaking algorithm can protect their privacy without seeking help from any centralized third party. Other than the shortcomings of the centralized approach, our work is also motivated by the following facts: 1) the computation power and storage capacity of most mobile devices have been improving at a fast pace.

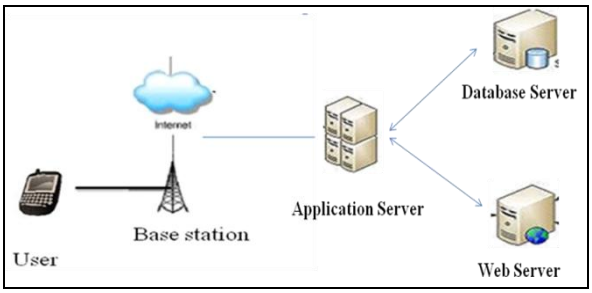

Figure 1: System Architecture

A trusted third party called anonymizer is basically required to achieve *k*-anonymity with respect to location information since it is hard to construct a cloaked region including *k* users' queries in a distributed manner. In order to provide *k*-anonymity, many techniques were proposed based on the assumption of a trusted anonymizer. Fig. 3 illustrates three-tier architecture with a trusted anonymizer. All queries and answers are relayed through the anonymizer. Given a query, the anonymizer removes the user's identifier, applies cloaking to replace the user location with a cloaked region, and then forwards the cloaked region to the location server. However, in real applications, the assumption of a trusted anonymizer is not desirable. First of all, we should consider major redesign of technologies (e.g., protocols or trusted mechanism) or business models. It may be not easy to share private service information including map or Point Of Interest (POIs) with other business entities including the anonymizer since the information in location-based services is generally valuable. Second, we should consider the problems inherent in a **Figure1.** Application server is used to serve web based applications and enterprise based applications(i.e sevlets, jsps and ejbs...). because application server contains web server internally. Web server is used to serve web based applications.(i.e servlets and jsps)

Users of these services query the LBS to retrieve information about data (points of interest, POI). The main issue arising in this environment is that the users reveal their locations to the untrusted LBS. In turn, this information may lead to the identity of the users through publicly available information, physical observation, mobile device tracking, etc. The nature of the POIs (e.g., HIV clinics) may disclose sensitive personal information to the LBS. However given a cloaked region including user location, finding the nearest POI to the user location cannot be achieved by range search with a fixed region.

A. Query Processing at the LBS

The two most common spatial queries are the Range Query and the Nearest- Neighbor (NN) Query. Given only an ASR and the query type/parameters, the LBS needs to search for the POIs that satisfy the query for any possible user location within the ASR. Typically, the LBS stores the POIs in secondary storage, indexed by an R-tree . If an R-range query is given, the LBS compute CS as the union of all POIs that fall inside the ASR or are within distance R from its boundary. In the example of Figure 2(a), the LBS expand the ASR

(shown with a dashed contour) by R, and perform an ordinary range query. The CS contains P1, P2, and P3. If a K-NN query is given, the CS contains the union of K nearest POIs 3 to any point within the ASR. To derive the CS for a NN query (i.e., K = 1) in Figure 2(b), the LBS needs to retrieve (i) all objects located inside the ASR (i.e., P1) and (ii) the NN of any location along the boundary of the ASR (i.e., P2, P3, P5).

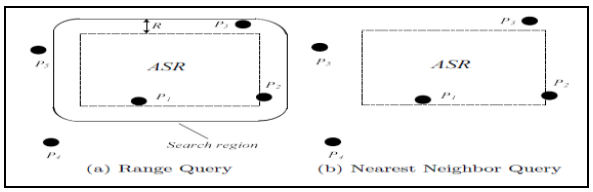

Figure2: Types of query processing at LBS

The latter component is processed using the linear NN method of for each of the 4 edges of the ASR; the input to this method is one or more line segments, for which NNs are found in a single R-tree traversal.

V. Proposed Framework

Proposed framework is basically based on processing of range search query.

A. Protocol

In [8], user has its own privacy requirement *Amin* that specifies its desired level of privacy. *Amin* specifies the minimum resolution of the cloaked spatial region. This region is known to adversary, but cannot exactly locate the user's location. The used a function D(P) which calculates smallest closing disc for set of points P where P is ={p1, p2, ・ ・ , pn} be a set of n points (called sites) . in [8] , the framework proposed which calculate the set of nearest neighbors from which user has to select the most nearest site to him.
In this paper we propose framework is basically based on processing of range search query where LBS directly send the set which has shortest distance at first in the list to the user. Protocol between the user and the LBS is described in **Algorithm 1.**

B. Query processing

The query processing is based on computation of Voronoi diagram for POIs. We formally define the problem as follows: Given a set $S_{def} \equiv \{p_1, p_2, ..., p_n\}$ of n distinct points convex polygon P with m vertices, find a set of the nearest neighbors N_P for P.

We propose the query processing algorithm using a local Voronoi diagram relevant to the cloaked region. Using the specific shape like circular, square, rectangle, continues, adversary may identify the location after a frequent use. So we propose a algorithm which changes the shape of the cloaked region after every execution. The procedure to compute the query with a polygon P is designed in **Algorithm 2.**

Algorithm 1: Cloaking protocol

1. Generate cloaking region.
2. Send this region to LBS.
3. LBS computes set of nearest neighbor which is set of all points of user's interest which intersect the boundary.
4. LBS send the set to user which is in the ascending order of the distance to the user.

Algorithm 2: Query processing algorithm
Input: a set *S* of *n* points, a convex polygon (circular, polygon , square etc)*P*
Output: *NP*
1: Find the smallest enclosing disc *D*(*P*) for the convex polygon *P*.
Let *r* and *c* be the radius and the center of *D*(*P*), respectively.
2: Initialize *d* as ∞.
3: **for** *si* ∈ *S* **do**
4: **if** *d* > *dist*(*c*, *si*) **then**
5: *d* = *dist*(*c*, *si*)
6: **end if**
7: **end for**
8: *r**= 2 . *r* + *d*
9: **for** *si* ∈ *S* **do**
10: **if** *r** ≥ *dist*(*c*, *si*) **then**
11: Insert *si* into the set of candidate points *SP* .
12: **end if**
13: **end for**
14: Compute the Voronoi diagram *V or*(*SP*) for *SP* .
15: **for** *si* ∈ *SP* **do**
16: **if** a cell *V* (*si*) ∈ *V or*(*SP*) intersects with *P* **then**
17: Insert *si* into *NP* .
18: **end if**
19: **end for**
20: **return** *NP*

C. DESIGN GOALS

The goal of our system is to exploit the privacy issue of location Based System, to achieve cloaking region in mobile environment. Our mechanism is to achieve the following objectives as:

1. Avoiding involvement of no. of peers in the network and communication between the peers.
2. **Anonymization success rate** as compare to P2P network as it is only one user in anonymity region.
3. **To minimize average communication overhead per query**. : it measures the total size of all the messages involved caused by a query's anonymization process;
4. **Average anonymizing time per query.**

VI. Conclusion

In this paper we proposed an algorithm for spatial cloaking which first minimizes the use of third party trustworthy server and directly communicates with LBS. peer to peer network, where the peer who wants to communicate with LBS will communicate with other peer in the network which increases the communication overhead. This paper proposes the direct communication without use of peers, which minimizes the communication overhead of peers.

Also algorithm 1 output the sorted list of nearest neighbor. Algorithm 2, processes the query for nearest neighbor, and calculates the cloaked region. The region generation is the main issue because generating the similar shape of region can override the privacy. This algorithm generates the different shapes of regions at different executions, so that there are very less chances of getting the exact location of user. As we are working on this project, the experimental results are yet to be evaluated.

References

[1] A Dual-active Spatial Cloaking Algorithm for Location Privacy Preserving in mobile Peer-to-Peer Networks ,Yanzhe Che, Qiang Yang, Xiaoyan Hong, 2012 IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks.
[2] B. Gedik and L. Liu. A Customizable k-Anonymity Model for Protecting Location Privacy. In ICDCS, 2005.
[3] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In MobiSys, 2003.
[4] M. Mokbel, C. Chow, and W. Aref, "The new casper: query processing for location services without compromising privacy," in *Proc. of Int. Conf. on Very large data bases*, pp. 763–774, VLDB 2006.C. [5] M. F. Mokbel, C.-Y. Chow, and W. G. Aref. The New Casper: Query Procesing for Location Services without Compromising Privacy. In VLDB, 2006.
[6] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. of Int. Conf. on Distributed Computing Systems*, pp. 620–629, IEEE, ICDCS 2005.
[7] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location based queries in distributed mobile systems," in *Proc. of Int. conf. on World Wide Web*, pp. 371–380, WWW 2007.
[8] A Spatial Cloaking Framework Based on Range Search for Nearest Neighbor Search, Hyoungshick Kim Computer Laboratory, University of Cambridge, UK hk331@cam.ac.uk