Spatial Cloaking algorithm for location privacy preservation.

Suchita R. Shastry, Dr. A. B. Bagwan, Department of Computer Engineering, University of Pune.

Abstract -Location based Servers (LBS) include services to identify a location also responsible for answering the queries, may disclose user's sensitive information. Mobile users expect to access services relevant to their locations, and also want preserve their privacy without disclosing their exact location. The spatial cloaking method provides way the where the location of the user get blurred. Location Anomymizing Server (LAS) is trusted third party which cloaks the user's location and sends to LBS. 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. Also mobile client is directly communicating with LBS without the interference of third party trusted server, location Anonymizing server (LAS). In this paper, 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. Hence adversary cannot disclose the user's exact location.

Index terms -Location Based Service (LBS), Location Anonymizing Server (LAS), Privacy Preserving, Spatial Cloaking, k-anonymity.

1. INTRODUCTION

1.1 Location Based Services

GPS-enabled mobile phones and palm-tops, has lead to a growing market of location-based services (LBS). Users of these services query the LBS to retrieve information about data (points of interest, POI) in their vicinity. Location-based services (LBS) providers require users' current locations to answer their location-based queries, e.g., range and nearest-neighbor queries. Since LBS are provided for users based on their exact location information, a major threat about the user's location privacy has been raised. Revealing personal location information to potentially untrusted service providers could create privacy risks for users. Location Based Service (LBS) has been widely used due to the explosive deployment of location-detection devices, e.g. smart phones, global positioning system (GPS) devices and radio-frequency identification (RFID) chips, as well as the rapid growth of the positioning technologies, e.g. cell phone positioning, GPS positioning and positioning through Wi-Fi access points. A LBS database server provides tailored and personalized services to users in accordance with their precise location information. An example of such services includes Range query, e.g. "show me a list of restaurants within 2km distance from my current location", and Nearest Neighbor query, e.g. "where is the nearest hospital". However, location information is sensitive under some circumstances and users are often unwilling to disclose such information to untrustworthy LBS servers as malicious adversaries may obtain more private knowledge of the victims.

1.2 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. Information sharing scheme, [1] enable the mobile users to share their gathered peer location information with nearby peers. If mobile user get information from peer, she does not need to search the network and hence can reduce communication overhead. Mobile P2P [1] is highly adhoc environment in which mobile users can only communicate with other peers through multihop routing. But it has limitation like user mobility, limited transmission range, multihop communication, network partitions. Cloaking algorithm [3], in which cloaked regions are generated according to features of spatial network.

In P2P where centralized servers are not possible and also there is participation of third party trusted server Location Anonymization Server (LAS), the Dual Active spatial cloaking [2] algorithm is suggested, which work in on demand mode, Proactive mode and Dual active mode.

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 [6].

2. RELATED WORK

The paper [1] has explained privacy issue of LBS and represented a dual-active spatial cloaking algorithm for mobile P2P environment. The dual-active algorithm enables peers to achieve required anonymity goal with less time per query by two main mechanisms:

1) Using peer location information collected through potentially multi-hop query propagation;

2) Using stored location records for a period of time.

The two mechanisms effectively reduce the communication cost and alleviate the network partition problem. This algorithm allows peers not only actively collect but also actively disseminate location information to others.

The paper [3] has explained the architecture with using third party ie LAS. It is responsible for cloaking at least k-user's locations for protecting location privacy. LAS is responsible for generating the regions for at least k-users. The cloaked regions are generated according to feature of spatial network. The cloaked regions are very efficient for reducing query results and improving cache utilization of mobile devices.

Three-tier architecture is with a trusted anonymizer. The figure1 shows the architecture where all queries and reply are given by trusted third party server (LAS). The LAS removes the user's identifier from a query, applies cloaking to replace the user location with a cloaked region, and then forwards the cloaked region to the LBS [4].

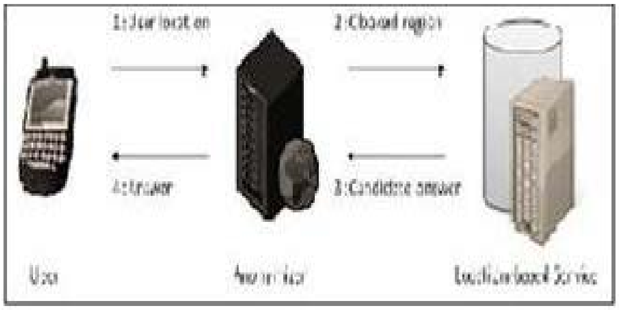

Figure 1: Three tier architecture with trusted third party

Many techniques are proposed to provide k-anonymity [7] [10]. But in real applications, the use role of LAS is not desirable. The direct communication of client mobile with LBS .This is two- tier architecture, where it is assumed that all the users are trustworthy

An algorithm a framework, called "SpaceTwist" in [4], aims to improve on the approaches offers location privacy. POIs are retrieved from the server incrementally. 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. This approach is capable of offering location privacy. This paper has not used middleware LAS, also no cloaked region is applied.

For nearest neighbor search [8], a user queries a server for nearby points of interest (POIs) with his/her location information. The aim is to protect the user's sensitive information against adversaries including the location-based service itself. Most research efforts have elaborated on reasonable trade-offs between privacy and utility. We propose a framework based on range search query without a trusted middleware.

Location privacy techniques that work in traditional client-server architectures [9] without any trusted components other than the client's mobile device.

3. Motivation of the dissertation

Spatial cloaking is most secure method used in mobile networks environment. But some existing algorithms for spatial cloaking have limitations. First some architectures uses three tier architecture with trusted third party anonymizing LAS server .But it is not possible all situation.

In P2P network environment, communicating with peers cause major communication overhead and chances of leakage of information. Hence communication among all trusted users will be done by sending request once.

The documentation considers two tier architecture in which client directly communicates with LBS. Only registered client straightway communicates with LBS. The time required for sending and receiving a query is reduced. As LBS is trusted, use of anonymous user is eliminated. The time for per query processing is also reduced.

The algorithm consists of communication done by using basic protocol, described briefly as:

The client communicates to trusted LBS directly without using LAS. The user sends a query to LBS.

LBS plots registered users in specified area. User create the region based on r input type for proposed request whose location is l(x, y) then check the condition for region. LBS process a query and send the result to client.

Also the query processing is done to the LSB server side as:

First LBS sends the list of peers and then list of Point of interest (POI) and Users closest to POI efficiently solve the nearest neighbor queries in cloaked area.

4. Proposed Method

Papers [1], [2] has used peers in mobile adhoc networks, limitations like. Mobile clients communicate among each other and cooperate to blur their accurate locations into a spatial cloaking region without the participation of any third parties. Strategies in searching anonymizing candidate peers have suffered from unpredictable long delay in finding k-anonymity and low anonymization success rate.

Two tier client server- architecture, where there is no participation of third party LAS server. It is always not possible to implement the third party server [3]; also always it is not trustworthy. Hence client server architecture is simple, easy to implement.

As client communicates to LBS directly, Client has to register to LBS. Hence all the users are registered. So the concept of k-anonymity has eliminated. In the same way there is no question of finding the anonymous peers, the delay required in multi-hop communication and anonymity success rate. In [1], peers gathers information and forward the peer information to the neighboring peer. In this there are sending and receiving information from the peers takes time and communication overhead. This limitation is overcome by using direct communication of client and server. Similarly there is no question of leakage of information and no matter of user mobility, limited transmission range.

Peer search [3],[4] which is required for locations which client is using for cloaking purpose. The peer search is applied by using the nearest neighbor algorithm. Paper [4] proposed two different algorithms for query processing.

Paper [5] examines privacy issues in snapshot queries and proposes a method that guarantees that all queries are protected. But in this paper we are dealing with only snapshot queries.

The layout of architecture where there is no trusted third party server (LAS). The architecture consists of mobile client, LBS and the database server. LBS processes query and send back the result to the user. User selects the optimum result. Here wherever the user next time login to the LBS, the authenticity is checked for him. System architecture consists of the mobile devices with positioning capabilities, LBS and database server. The figure 2. Shows layout of the architecture.

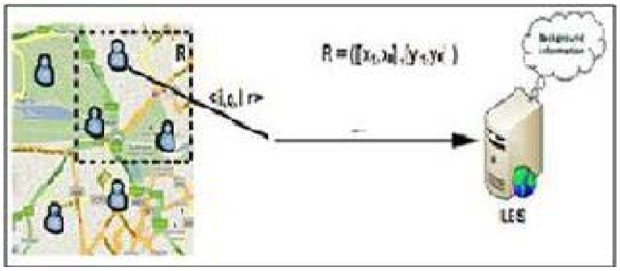

Figure 2: Two tier architecture model

- Mobile client:

Mobile devices include mobile phones, PDA, and devices with positioning system. Its physical location is computed from GPS, Wi-Fi. The client first registers to the LBS. Mobile users specify the privacy requirement about user interface to the mobile device. It sends request consist of the Identification, query, positions, and the region to be generated to the LBS. It is forwarded to LBS. After observing for a typical query the location component of the query may not be the current mobile user's location.

For example, Bob is at Point X and Bob submits a query requesting the closest buses to Point Y. In this case, there is no need for Bob to reveal that she is at Point X.

- Location Based Server (LBS):

The physical location computed by the mobile device is sent to the LBS server with the query. The role of the LBS is to privatize location. On the receipt of the request, LBS check the authenticity of the mobile user, process the request and generate the result set. It is filtered, precise result set in ascending order which sent back to user. The service provider has the ability to process a given cloaked region and also process an exact point. The service provider is not responsible for privacy policies of the mobile clients.

- Database server:

At the back-end of the system, a privacy-aware query processor is embedded inside the location- based database server in order to tune its functionalities to deal with cloaked spatial regions for user locations and user queries rather than exact point locations.

4.1 Proposed Framework

The system works in two modules:

1. Client module

- Registration
- Query for peer search send to LBS.
- Query request for POI sent to LBS

- Receives result and finding the optimum result.
- Plot result and shape of the region on map.

2. LBS server module

- Registration of client
- Authentication
- Receive and process query request for peer search.
- Process the query request for result (POI).
- Send the result set to client.

4.2 Mathematical Model

1. User sends his geo location in the form of(x, y):

Where x is latitude and y is longitude.

2. Let number of users (P1,P2.........Pk) are registered region to LBS.

x1≤x ≤xk and y1 ≤y ≤yk where x1, y1 are lower bounds, xk, yk are upper bound for latitude and longitude for all k users.

3. Latitude and Longitude calculation from service method GenratePeer().

double maxLatitude = Lat + (miles / 69.11);

double minLatitude = Lat - (miles / 69.11);

4. Region generation will follow the Euclidian distance formula in Query Processing

The users(P1, p2,........Pk) with their geo locations . hence the general formula is given as:

Dist((x, yk),(y,yk)) = SQRT((x-x1)2 +(y-y1)2 +……..+(x-xk)2 +(y-yk)2)

Where x and y are latitude and longitude of user location.

And xk, yk are geo locations of nearest kth user.

4.3 Program Structure:

The whole dissertation is divided in to the five main components.

1. Client Login.

User can register to the LBS, where he has to specify accountid, username, password and mail_id.

2. User specifies a query for Peers in the specified range send to LBS.

Only registered user can send the query. Peers are required for cloaking purpose.

3. LBS returns the set peers to client.
4. Client selects the nearest peer depending upon the distance. user selects the peer's geo locations for cloaking purpose.
5. Client sends a query for POI which includes ID, query, position of user, region type to LBS.
6. Based on 'r', user create region for proposed request whose location is l(x, y).
7. LBS sends the result set of POIs.
8. Client selects nearest POI.

5. Goals and Objectives

- Direct communication of client and server avoids the involvement of no. of peers and provide the communication overhead of peers in peer to peer (P2P) environment as in [1].
- As all users are registered, we will curtail the concept of anonymous users.
- Success rate of peers are calculated by dividing the number of users who successfully generate the cloaked region in a given time by the total user number.
- Average peer time per query: this is the mean time between user initials a query and generates a cloaked region. It indicates the response time of anonymization process for each algorithm;

- Sharing of information among the users may directs to the of security question
- Average communication overhead per query gets minimized.

6. EXPERIMENTAL RESULTS

The table shows experimental results for number of peers generated in given region.

Response Time of query in (seconds)	No. of peers	Data Size(kb)	Region(Miles)
4	4	2.14	5
8	20	7.23	15
5	11	5.87	10
17	250	25.18	100
11	45	15.65	20

7. SUMMARY AND CONCLUSIONS

The proposed algorithm of spatial cloaking has implemented using client server architecture without using trusted third party server. The mobile client directly communicates with the LBS server. The registered client could only be communicating to server. This would avoid the entry of unauthorized client. Client requests for peer generation to LBS, for cloaking purpose. All these are only registered users used for cloaking purpose. The LBS sends the list of nearest peers to client in the specified region. The type of region of different shapes generated by client would be helpful. This would be advantageous to client to prevent himself from getting disclosed to the adversaries. This is because a similar region at all the time is query formation makes to disclose the identity of the user. Query formation for peers and result generation is done by using K-nearest Neighbor. The average time required for processing a query is minimizes. As no peers are involved in communication, overhead of communication of peers is minimized.

8. 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] Spatial cloaking for anonymous Location –services in mobile based Peer to Peer environment, Chi Yin Chow, Mohamed F. Mokbel, Xuan Liu.

[3] A cloaking Algorithm based on spatial networks for loaction privacy, po-yi Li, Wen Chih Peng, Tsung wei weng, Wei Shinn ku, Jinling Zu, J-A Hamilton, , 2008 IEEE International conference on Sensor networks, Ubiquitous, and trustworthy computing.

[4] SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query , Man Lung Yiu , Christian S. Jensen , Xuegang Huang , Hua Lu, Department of Computer Science, Aalborg University,DK-9220 Aalborg, Denmark

[5] TRANSACTIONS ON DATA PRIVACY 5 (2012) 333 AT376 333 Mobile Systems Privacy: ′ MobiPriv ′ a Robust System for Snapshot or Continuous Querying Location Based Mobile Systems.

[6] B. Gedik and L. Liu, ′ Protecting Location privacy with personalized k-anonymity architecture and

algorithm ′ , IEEE TRANSACTION ON MOBILE COMPUTING7(1), 1-18 2008.

[7] The New Casper: Query Processing for Location Services without Compromising Privacy Mohamed F. Mokbel ChiYin Chow, Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN, Walid G. Aref ,Department of Computer Science, Purdue University.

[8] A Spatial Cloaking Framework Based on Range Search for Nearest Neighbor Search , Hyoungshick Kim, Computer Laboratory, University of Cambridge, UK

[9] Location Privacy Techniques in Client-Server Architectures, Christian S. Jensen, Google Inc., Mountain View, CA 94043, USA, Hua Lu2, Department of Computer Science, Aalborg University, Denmark, LNCS 5321,pp-31-52, 2009, http://springerlink.com