Location Based Spatial Query Processing In Peer to Peer Network

Bhavana Tathe[1], Megha Dhere[2],Pranita Wadavkar[3], Prof.N.P.Karlekar [4]

[1]*Department Of Computer engineering,Sinhgad Institute Of Technology,Lonavala*
[2] *Department Of Computer engineering,Sinhgad Institute Of Technology,Lonavala*
[3] *Department Of Computer engineering,Sinhgad Institute Of Technology,Lonavala*
[4] *Department Of Computer engineering,Sinhgad Institute Of Technology,Lonavala*
[1]tathebhavana@gmail.com
[2]dheremegha@gmail.com
[3]pranita.w35@gmail.com
[4]nkarlekar@gmail.com

***Abstract*— The main purpose of this paper is to tackles a major privacy threat in location-based services where users have to report their current exact locations to the database server in order to obtain their desired services. For example, a mobile user asking about her nearest hospital has to report her exact location. With untrusted service providers, reporting private location information may lead to several privacy threats. In this paper, we present a peer-to-peer (P2P) spatial cloaking algorithm where mobile and stationary users can entertain location-based services without revealing their exact location information. The main idea is that the mobile user will form a group from her peers via single-hop communication and/or multi-hop routing before requesting any location-based service. The entire group of peers is computed as the region that covers location requested by user and this term is called as spatial cloaked area. This proposed P2P spatial cloaking algorithm supports two modes of operations viz. the on-demand mode and the proactive mode. As per the experimental results the P2P spatial cloaking algorithm operated in the on-demand mode has lower communication cost and better quality of services than the proactive mode, but the on-demand incurs longer response time.**

***Keywords*—- Location based services, location privacy and spatial cloaking.**

I. INTRODUCTION

Location-based services (LBS) can provide a wide variety of important services for mobile users that have been proven through many commercial products or research prototypes. Examples of these services include transportation services (e.g., \What is the shortest route from my current location to my home"), convenience services (e.g., \Where is my nearest grocery store"), and emergency control (e.g., \Dispatch the nearest ambulance to the patient"). 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 requirement. The most popular privacy requirements for the spatial cloaking technique are K-anonymity, i.e., a cloaked area contains at least Kusers, and minimum area Amin, i.e., the size of a cloaked area is at least Amin. Since a location-based database server does not know the user's exact location information, the database server can only return an answer set that includes the exact answer to the user.

LBS servers as malicious adversaries may obtain more private knowledge of the victims, e.g. an adversary can guess an individual's home address by tracking his location at non-working time. In order to preserve the user privacy, the spatial cloaking technique has been well studied in literature. The main idea behind the spatial cloaking technique is to deploy a third trustworthy party, i.e. location anonymizing server, between users and LBS database servers. The LAS gathers enough location information and blurs them into a cloaked region which meets the user's privacy requirements, such as *k-anonymity* (i.e. user cannot be identified from the other *k*-1 users), or the minimum cloaked region area, denoted as *Amin* (i.e. user needs to hide inside a region at least of size *Amin*). However, in the mobile P2P networks, the 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. In the authors described the spatial cloaking algorithm operated in two different manners in P2P environment: *on-demand* mode and *proactive* mode.

II. RELATED WORK

Several existing distributed group formation Algorithms are not designed for privacy preserving in LBS, they are just searching for peers in a mobile environment. Some algorithms are limited to only finding the neighboring peers,e.g.,lowest-ID,largest-connectivity (degree) and mobility-based clustering algorithms . When a mobile user with a strict privacy requirement, i.e., the value of k − 1 is larger than the number of neighboring peers, it has to enlist other peers for help via multi-hop routing. Other algorithms do not have this limitation, but they are designed for grouping stable mobile clients together to facilitate efficient data replica allocation, e.g., dynamic connectivity based group algorithm and mobility-based clustering algorithm, called DRAM. Our work is different from these approaches in that we propose a P2P spatial cloaking algorithm that is dedicated for mobile users to discover other k−1 peers via single-hop communic ation and/or via multi-hop routing, in order to preserve user privacy in LBS. The k-anonymity model has been widely used in maintaining privacy in databases. The main idea is to have each tuple in the

table as k-anonymous, i.e.,indistinguishable among other k − 1 tuples. Although we aim for the similar k-anonymity model for the P2P spatial cloaking algorithm, none of these techniques can be applied to protect user privacy for LBS, mainly for the following four reasons: 1) These techniques preserve the privacy of the stored data. In our model, we aim not to store the data at all. Instead, we store perturbed versions of the data. Thus,data privacy is managed before storing the data. 2) These approaches protect the data not the queries. In anonymous LBS, we aim to protect the user who issues the query to the location-based database server. For example, a mobile user who wants to ask about her nearest gas station needs to protect her location while the location information of the gas station is not protected. 3) These approaches guarantee the k-anonymity for a snapshot of the database. In LBS, the user location is continuously changing. Such dynamic behavior calls for continuous maintenance of the k-anonymity model. (4) These approaches assume a unified k-anonymity requirement for all the stored records. In our P2P spatial cloaking algorithm, k-anonymity is a user-specified privacy requirement which may have a different value for each user.

The proposed P2P spatial cloaking algorithm can operate in two modes: on-demand and proactive. In the on-demand mode,mobile clients execute the cloaking algorithm when they need to access information from the location-based database server. On the other side, in the proactive mode, mobile clients periodically look around to find the desired number of peers. Thus, they can cloak their exact locations into spatial regions whenever they want to retrieve information from the location-based database server. In general, the contributions of this paper can be summarized as follows:

1. We introduce a distributed system architecture for providing anonymous location-based services (LBS) for mobile users.
2. We propose the first P2P spatial cloaking algorithm for mobile users to entertain high quality location-based services without compromising their privacy.
3. We provide experimental evidence that our proposed algorithm is efficient in terms of the response time, is scalable to large numbers of mobile clients, and is effective as it provides high-quality services for mobile clients without the need of exact location information.[1]

III. System Model

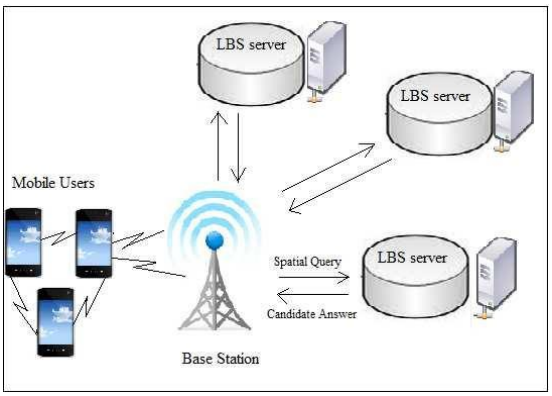

Fig1.The Overview of System Architecture

In this paper, the LBS system has two important components: mobile users and LBS database servers as shown in Figure 1. The mobile users are carrying mobile devices with positioning functionality. These mobile devices also can 1)communicate with the LBS database servers through the help of base stations; 2) communicate with other mobile users via wireless LAN or ad hoc network routing protocols, e.g.802.11n which enable outdoor users communicating at a range of 250m approximately. In this paper, we assume that the mobile users are trusted and mean no harm to the system. But the LBS database servers are not trustworthy. Thus in order to preserve location privacy, users must query the servers with a cloaked region instead. So the LBS database servers do not have the knowledge of the exact location of mobile users but a cloaked region which may contain at least *k* anonymity. The LBS servers will perform their services according to the given region and return a set of candidate answers.[2]

The users' requirements for accessing the LBS can be classified into two categories. 1) Privacy requirement: this requirement can be achieved by using two parameters, i.e. *k* and *Amin*. The *k* indicates that the user can not be distinguished with other k-1 users in the cloaking region and the *Amin* indicates the smallest size of the cloaking region. 2) Quality of service (QOS) requirement: it is possible that the privacy requirement cannot be achieved immediately. And in many cases, an application can have a tolerance on the latency towards receiving a service. To define this QOS requirement,we user two parameters, *t* and *Amax*. The *t* is a user's longest tolerant time for executing the spatial cloaking algorithm and the *Amax* is the maximum size the cloaked region can be.A strict *k-anonymity* requirement may cause a long delay for gathering enough anonymities as well as lead to a large-size cloaked region. Depending on the network density and traffic load, to fulfill both the requirements can consume bandwidth resources in transmitting candidate answers to an anonymization query. We notice that the tradeoff needs to be properly investigated between the privacy and QOS requirements.[2]

IV. Mathematical Model

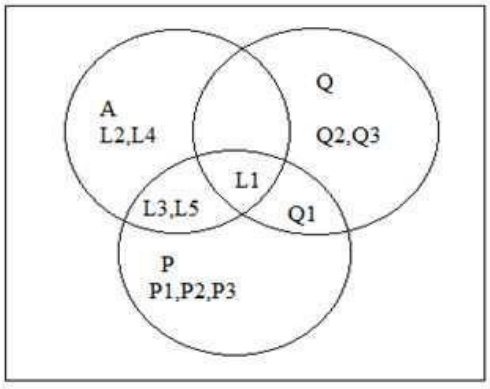

Fig2.Module Representation Using Set Theory

1.Privacy Requirements:-

Set A= {L1,L2,L3,L4,L5}
Where,
L1-Mobile user
L2-Cloaked area contains no. of user.

L3-Minimum area Amin.
L4-Initial Time.
L5-Maximum area Amax.

2. Query:-

Set Q= {L1,Q1,Q2,Q3}
Where,
L1-Mobile user
Q1-Send the query
Q2-Exeute query
Q3-Query Response

3. Spatial Cloaking:-

Set P= {L1,L3,L5,Q1,P1,P2,P3} where,
L1-Moblie user.
L3-Minimum area Amin.
L5-Maximum area Amax
P1-Blur a user exact location.
Q1-Send the query.
P2-Hide the location.
P3-Give false location.

Union :- AUQ= {L1,L2,L3,L4,L5,Q1,Q2,Q3}

AUP= {L1,L2,L3,L4,L5,Q1,P1,P2,P3}

AUQUP={L1,L2,L3,L4,L5,Q1,Q2,Q3,P1,P2,P3}

Intersection:- A∩P={L1,L3,L5}

Q∩P={L1,Q1}A∩Q∩P={L1}

V. P2P Spatial Cloaking Algorithm

The entire system area is divided into grid. The mobile client communicates with each other to discover other k −1 peers, in order to achieve the k-anonymity requirement. The mobile client can thus blur its exact location into a cloaked spatial region that is the minimum grid area covering the k − 1 peers and itself, and satisfies Amin as well. The grid area is represented by the ID of the left-bottom and right-top cells, i.e., (l, b) and (r, t). In addition, each mobile client maintains a parameter h that is the required hop distance of the last peer searching. The initial value of h is equal to one.

Algorithm 1 P2P Spatial Cloaking:

Step 1: Peer Search Step

1. Initially set number of peers required k=4, Area (A) =Amin// min area k=4
2. Broadcast a request (containing ID of user U) to all neighboring peers.//req
3. Each peer generates a new record r that contains its ID, current location and a timestamp i.e. <p, (xp, yp), tp>
4. Send record r to user U. // r is result

If ((NumPeer(List)<=k) && (Area(A) < Amax))
For (i=0; i<=NumPeer(List);i++)
get (i)th records

a. Expand the Area(A) by adding some constant value.
b. Broadcast request to the peers.
c. Receive records from peers.
d. Update number of peers in List (i.e. k).
End for
End if
If (NumPeer(List)=NULL) // if no data found

a. Select the user as having the latest timestamp.
End if

5. Send the records in List, k, location of user U, Area(A) and ID of peer having latest timestamp to central server(i.e. Location Anonymizing Server).

Step 2: Cloaked Area Step

1. If(NumPeer(List)>k)
   a. Select four peer records randomly.
   b. Determine a region A that cover all locations
2. Else
   a. Set latest timestamp = ID of user U
   b. Add some constant value to U's location.
   c. Determine region A=Amin

   End if
3. If(Area(A)>= Amin)
   a. Return Area A as user's blurred location information
   b. Also return location of peer having latest timestamp.
4. Else
   a. Extend Area A by random distance.
   b. Return Area A as user's blurred location information
   c. Also return location of peer having latest timestamp.

   End if
5. Forward the request along with location information and bounded area to Location-based server.

VI. Diagramatic Representation Of P2P Spatial Cloaking Algorithm:

Figure 2 gives a running example for the P2P spatial cloaking algorithm. There are 15 mobile clients, m1 to m15,represented as solid circles. m8 is the request originator,other black circles represent the mobile clients received the request from m8. The dotted circles represent the communication range of the mobile client, and the arrow represents the movement direction. In general, the algorithm consists of the following three phases:[1]
1.Peer searching phase
2.Location adjustment
3.Cloaked spatial region.

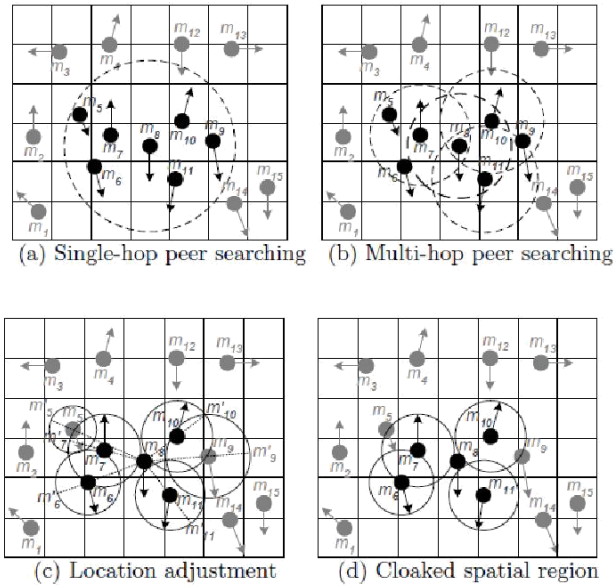

Fig3.P2P Spatial Cloaking Algorithm.[1]

VII. Experimental Results

We are developing our spatial cloaking algorithm using Android toolkit by making an app Cloak demo as shown fig.4 .For location searching we are using web services provided by Google map directly to overcome database overhead which in turns gives efficient results.

Fig.4(a) shows the current location of the user by filled blue circle(Nigeria) and the circular region includes the registered peers which are nearest to the user. User want to search nearest shipping mart in Nigeria,so in Fig4(b),user get appropriate results for his query in accordance with the peer selected by him The difference between Fig.4(a) and Fig4(b).i.e. Before Query Result user exact location can be seen as described above and After Query Result it gets blur and still he gets required results for his query through the peer selected by the user So privacy requirement of user gets fulfilled as discussed in our paper.

Fig4. (a)Before Query Result

Fig4. (b)After Query Result

VIII. CONCLUSION

This paper fully summarizes all the necessary things about the location based services, Difference between the existing and this P2P spatial cloaking algorithm. By using the algorithm, the mobile user can find the required number of peers to form a group and then user determines the minimum grid area that satisfies users privacy requirements. So, it can be concluded that user location get hidden and still query get processed through group of registered user by selecting appropriate peer amongst them.

P2P spatial cloaking algorithm can operate in two modes ,on-demand and proactive. For the on-demand mode, the mobile user only executes the algorithm when user needs to access information from the location-based database server. The mobile user adopting the proactive mode periodically executes the algorithm in background, so the mobile user can cloak his/her exact location into a spatial region whenever user needs to enlist the location-based database server for help. Comparitive study of both modes evaluates that the algorithm operated in proactive mode is more efficient considering response time than on-demand mode but generally it suffers higher communication overhead which in turn gives lower quality of service than the on-demand mode.

REFERENCES

[1] Chi Yin Chow, Mohamed F. Mokbel, Xuan Liu-A Peer to Peer Spatial Cloaking Algorithm for Anonymous Location based Services.
[2] Yanzhe Che, Qiang Yang, Xiaoyan Hong-A Dual active Spatial Cloaking Algorithm for Location Privacy Preserving in mobile Peer-to-Peer Networks.2012 IEEE Wireless Communications and Networking conference
[3] Wei-Shinn Ku, Member, IEEE, Roger Zimmermann, Senior Member, IEEE, and Haixun Wang, Member, IEEE-Location-Based Spatial Query Processing in Wireless Broadcast Environments. IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 6, JUNE 2008.
[4] Michael D¨urr, Marco Maier and Florian Dorfmeister-Vegas - A Secure and Privacy-Preserving Peer-to-Peer Online Social Network. Ludwig-Maximilians-University Munich 80538 Munich,Germany. [5]M. F. Mokbel, C.-Y. Chow, and W. G. Aref. The New Casper: Query Processing for Location Services without Compromising Privacy. In VLDB, 2006.
[6] M. F. Mokbel. Towards Privacy-Aware Location-Based Database Servers. In Proceedings of the ICDE International Workshop on Privacy Data Management, PDM, 2006.
[7] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloa king for anonymous location-based services in mobile peer-to-peer environments," Geoinformatica,vol. 15, pp. 351–380, April 2011.
[8] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," Trans. on Knowledge and Data Engineering, pp. 1719–1733, TKDE 2007.