ISSN 2395-1621

Location Privacy Preservation Using grid Dummy Generation

[#1] Dhananjay Bhave, [#2]Arjun Chorghe, [#3]Akshay Jagtap,[#4] Deepak Jivanavar

1 jagtap.akshy5555@gmail.com

[#1234]Navsahyadri Education Society's Group of Institutions,
University of Pune, India
.

ABSTRACT

Now a days, due to use of smart phones, LBS services can track the location of the user, If this information of location accessed by unauthorized person it can be extremely dangerous with the help of spatial cloaking and grid generation technique we can provide solution to the problem without changing architecture of LBS server and without including third party servers.

Keywords— Location Based Service, Grid based technique, Peer generation, Spatial Cloaking

ARTICLE INFO

Article History

Received : 22th May 2015

Received in revised form :

26th May 2015

Accepted :28th May 2015

Published online : 30th May 2015

I. INTRODUCTION

Smart phones has been a need for every human being in the day to day life, these devices provide various services which make the task of the user lot more easier, An example searching of the route , nearby places such as Hotels, Theaters ,Parks etc. These services what are used by the user are known as Location based services and these services are been fulfilled by the server called LBS server. LBS server accepts the query from the user which contain user's location and the search query and answers back to the user with the appropriate information. But these LBS servers were prone to attack by the private adversary companies. These issues was overcome by introducing the trusted third party server in between the user and the LBS server but using these server was causing to perform some modification in the architecture of the LBS server and also the task was time consuming. We are trying not to use LAS server, that didn't had the capacity to store large location search query. We are applying the action of security on the user phone rather than applying the technique on the server which is lot more tedious task. This can be achieved by using two techniques spatial cloaking and grid generation which provide the possible solution to the third party server.

Spatial Cloaking: Cloaking technique is used to hide location of particular person where we are avoiding the LAS server. Following are some algorithm methods are used in cloaking technique: Basic Spatial cloaking algorithm and dual active mode design. Dummy Generation technique are use to create dummy location for creating confusion for attacker. Circle Based Dummy Generation and Grid Based Dummy Generation technique are use to create fake location.

II. LOCATION BASED SERVICE

Location based services are program-level services which are used to provide the location of the particular object or the person for example- searching the nearby park from my home or searching the nearby bus station etc . Location based service make use of global positioning system, Cellular phones for detecting the location. LBS provides a vital information for the mobile user by accessing the precious location of the user.LBS server are used to handle the services requested by the user in the form of query which contains user's location and query, which server respond to the user with the information of the query asked. LBS are been categorized into two from snapshot LBS and continuous LBS. In snapshot technique the mobile user need to report its location to the service provider for retrieving the information. And in continuous LBS the mobile user need to report the location to the service provider only after at some interval or on-demand manner for retrieving the information. Snapshot LBS are more secure than continuous LBS because in continuous technique unauthorized person may use the user's location grouped sample for finding the appropriate location with high degree of certainty

III. DUMMY GENERATION

Dummy Generation technique are use to create dummy location for creating confusion for attacker. Circle Based

Dummy Generation and Grid Based Dummy Generation technique are use to create fake location.
Grid Based Dummy Generation technique is use to overcome disadvantage of Circle Based Dummy Generation like grid based require less memory as compare to circle based.

Steps for Grid Based Dummy Generation technique:

1:'k' are the vertices of square grid created, it calculates the number of vertices in directions (x-axis and y-axis)
n ← square root(k).

2: Attaching user pos to one of the k vertices, by generating the corresponding x and y indices at random.
x←random(0,n-1) ;
y←random(0,n-1);

3: Based on the value of s and c and n , we set the side length g of each grid cell.
g←square_root(s)/(n-1).

4: Generate dummy repeatedly
For i form 0 to n-1 do
For j from 0 to n-1 do
xco←(i-x).g to pos.x
yco←(j-y).g + pos.y
K[j * c+ i] ←(xco,yco)
return K and yco*c+xco

5: Calculates the position of each grid vertex in row-major order and enters all position into array K in the flow.

6: Finally returns both the position array K and the index of the user position pos in K.

7: Attaching user position to one of the vertices.

8: Generating grid cell.

IV. SPATIAL CLOCKING

Cloaking technique is used to hide location of particular person where we are avoiding the LAS server. Following are some algorithm methods are used in cloaking technique: Basic Spatial cloaking algorithm and dual active mode design.

(1) Basic spatial cloaking : In this Basic spatial cloaking there are three main steps
a) In first step each mobile user gathers a list of candidate whose location is anonymized, or shared through his direct connected users.

b) Second step is Cloaking step, where user generate cloaked region according to the information of location.

c) In final step query is processed, here user initiates search query and receives the replay from LBS database server.

V. SYSTEM MODEL

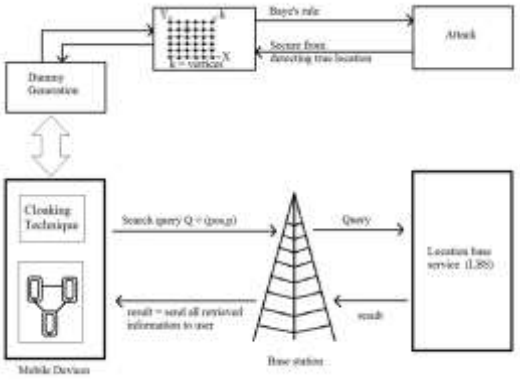

Fig No 1 : System Model

In this paper LBS service has two main components

1) Mobile devices

2) LBS database server
Cloaking technique is implemented in mobile device, dummy generation technique is used to generate fake locations, and those locations are not actually physically present there. In Dummy there is a fixed sized grid, size of grid is allocated through using k vertices when grid is formed, fake locations are created .Due to these fake locations the privacy of original user is maintained, due to this user gets protections from attacks. Baye's rule is used to prevent adversary attack, after location gets secured mobile device sends search query Q with parameter.
This search query is reached to LBS server, LBS server performs search operation and generates result, and then mobile user gets answer.

VI. ALGORITHM

Step 1: Peer Search Step

1. Initially set number of peers required k=4, Area(A)=Amin
2. Broadcast a request (containing ID of user U) to all neighboring peers.
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.

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)

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 one peer records.
   b. Show a region A previously defined before searching peer(to show that peer is within that region).
2. Else
   a. Set latest timestamp = ID of user U
   b. Add some constant value to U's latitude and longitude.
   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 fake location information and bounded area to Location-based server

VII. EXPERIMENTAL RESULT & ANALYSIS

We compare two algorithms:

Anonymizing success rate: it is calculated by dividing the number of users who successfully generate the cloaked region in a given time by the total user number

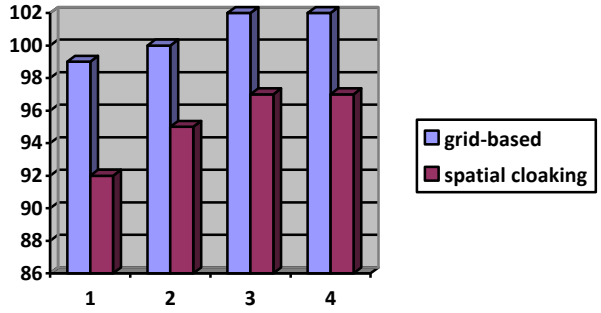

Fig (a): Anonymization success rate

Average communication overhead per query: it measures the total size of all the messages involved caused by a query's anonymization process

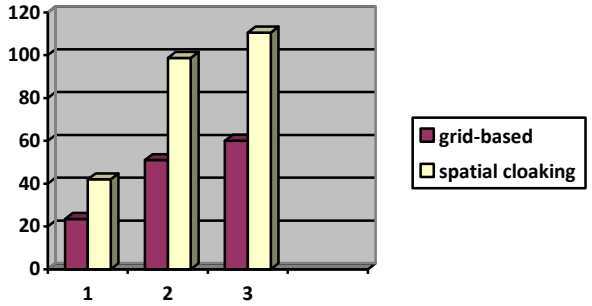

Fig (b): Average communication overhead

Figure a:
Present the anonymizer success rate in the scenario .It shows spatial cloaking and grid based having different success rate, grid based system shows higher success rate than spatial cloaking. The grid based has around 100 where spatial cloaking has around 95 in first scenario. Similarly it varies for further scenario but the success rate of grid base is quite higher than spatial cloaking.

Figure b:
Present avg communication overhead in the scenario .It shows spatial cloaking and grid based having different success rate, grid based system shows higher success rate than spatial cloaking. The grids based have around 100 where spatial cloaking has around 95 in first scenario.

Similarly it varies for further scenario but the success rate of grid base is quite higher than spatial cloaking.

VIII. CONCLUSION

In this paper we have proposed system which hides location of the user from LBS. As the implementation of the algorithm is done on the mobile device we can directly communicate with the LBS server without using trusted third party. We also do not make any architectural changes in the LBS server

IX. FUTURE SCOPE

If we implement this in service provider's server then we can give security to all devices.
We can also hide location on social media like face book.
we can increase speed of searching operation

REFRENCES

[1] Reza Shokri, Panos Papadimitratos, Ehsan Kazemi,George Theodorakopoulos,
Jean-Pierre Hubaux, "Hiding in the Mobile Crowd. Location Privacy through Collaboration" IEEE 2014

[2] Prof Dr. P. K. Deshmukh, Prof. Dr. A. B. Bagwan, Prof Suchita R.Shastry, Generating random regions in spatial cloaking algorithm for location privacy preservation ,Mar-Apr 2013

[3] Yanzhe Che, Qiang Yang, Xiaoyan Hong. A Dual-active Spatial Cloaking Algorithm for Location Privacy Preserving in mobile Peer-to-Peer Networks, IEEE 2012

[4] F. Olumofin, U. Hengartner, P.K. Tysowski, I. Goldberg, "Achieving Efficient Query Privacy for Location Based Services," Proc. 10th Int'l Conf. Privacy Enhancing Technologies, 2010.

[5] R.R. Choudhury, J. Meyerowitz, "Hiding Stars With Fireworks:Location Privacy through Camouflage"09, 2009.

[6] Yimin Lin, Kyriakos MOURATIDIS, Kar Way Tan 'Spatial Cloaking Revisited: Distinguishing Information Leakage from Anonymity' '07,2009'

[7] Christian S. Jensen, Hua Lu, Man Lung Yiu , Location Privacy Techniques in Client-Server Architectures,2009

[8] Man Lung Yiu, Christian S. Jensen, Hua Lu, Privacy-Area Aware,Dummy Based Location privacy in Mobile Services ,2008

[9] B. Gedik, L. Liu, "Location privacy in mobile systems: 'A personalized anonymization model' " in *Proc. of Int. Conf. on Distributed Computing Systems*, pp. 620 to 629

