International Journal of Advanced Engineering & Innovative Technology (IJAEIT)
Volume 1, Issue 4, October -2014
ISRA IMPACT FACTOR: 0.42

Location Privacy Preservation Using grid and Dummy Generation

Dhananjay Bhave, Arjun Chorghe, Akshay Jagtap, Deepak Jivanavar

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.

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

1 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 issue 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.

- *Dhananjay Bhave, Arjun Chorghe, Akshay Jagtap, Deepak Jivanavar, Research Scholar at Department of Computer Engineering ,Navsahyadri Education Society's Group of Institutions, University of Pune, Naigaon, Pune 412213 India*

2 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. [1-4] 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.[5]

3 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.[6]

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.

4 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.

(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. [7-8]

5 SYSTEM MODEL

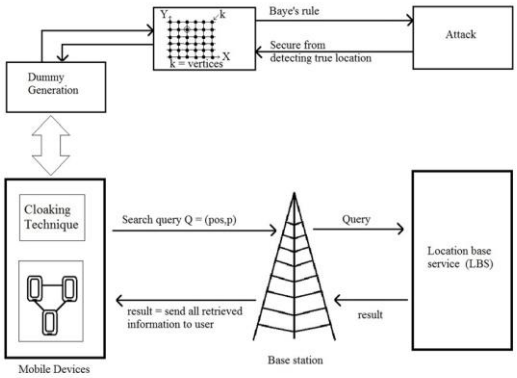

Fig No 1 System Model

In this paper LBS service has two main component

1) Mobile devices

2) LBS database server
Cloaking technique is implemented in mobile device, dummy generation technique is used to generate fake locations, 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.

6 ALGORITHM

1. Mobile device register to web server for authentication.
2. Use cloaking technique.
3. Use Grid Based Algorithm
   3.1.'k' are the vertices of square grid created , it calculates the number of vertices in directions(x-axis and y-axis)
   3.2. Attaching user pos to one of the k vertices, by generating the corresponding x and y indices at random.
   3.3. Based on the value of s and c and n, we set the side length g of each grid cell.
   3.4. Generate dummy repeatedly.
   3.5. Calculates the position of each grid vertex in row-major order and enters all position into array K in the flow.
   3.6. Finally returns both the position array K and the index of the user position pos in K.
   3.7. Attaching user position to one of the vertices.
   3.8. Generating grid cell.
   3.9. Generate Dummies repeatedly.
4. Check for the Bayesian attack if yes goto 5 else goto 6

5. Using bayes rule for prevention.
6. Send Query to LBS : Query Q=(pos , p) .
7. LBS evaluates the query of user.
8.LBS returns result(all retrieved information to user) to user.
9.End

7 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.

8 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

9 REFERENCES

[1] Yanzhe Che, Qiang Yang, Xiaoyan Hong. A Dual-active Spatial Cloaking Algorithm for Location Privacy Preserving in mobile Peer-to-Peer Networks, IEEE Wireless Communications and Networking Conference 'Mobile and Wireless Networks.2012.

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

[3]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, IEEE, ICDCS 2005.

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

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

[6] 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.