A SURVEY ON HIDING USER PRIVACY IN LOCATION BASED SERVICES THROUGH CLUSTERING

Nilam V. Khandade[1], **Snehal Nargundi**[2]

[1]M.E Student, Dept of Information Technology, R. M. D. Sinhgad School of Engineering, Maharashtra, India
[2]Asst.Professor, Dept of Information Technology, R. M. D. Sinhgad School of Engineering, Maharashtra, India

Abstract

Smartphone's are being more and more popular as the technology being evolve. The Smartphone's are capable of providing the location aware services like GPS. They share all the location information with the central location server. When user submit any query then these query also carries some personal information of the user. This query and information is then submitted to the LGS server. At the LBS server this information is not much confidential. Someone can use this information to make user panic. To overcome this we are proposing the new collaborative approach to hide user's personal data from the LBS server. Our approach does not lead to make changes in the architecture of the LBS server. And we are also not going to use the third party server. Here we are going to use the other user's device to search other users query so that other user can be get hide from the LBS server.

Keywords: *Mobile networks, location-based services, location privacy, Bayesian inference attacks, epidemic models*

---***---

1. INTRODUCTION

Many smart phone user the GPS as a location aware system. The Smartphone's are generally works on the Wi-Fi network. Which can capable of doing the connection in between two or more devices and making the use of mobile data on the mobile devices. The Wi-Fi allows the Smartphone's to use the location aware services. Location consciousness refers to devices that determine their location actively or passively. The location coordinates are taken from Navigational instruments for vehicles. The surveying equipment finds location by a well-known device named location wireless communications. Network location awareness (NLA) traces the location of node in the network. But when we are using the location aware services this connects us to the LBS server. When we fire any query then this query also sends our personal location data. By using this data one can make misuse of that data. For example one can blackmail or harm us by using our location information. User's personal information may lead to the religious war, personal or public beliefs and may lead to political affair. This may cause harassment to the user. If sometime the user goes out of home then one can break into user's house and can blackmail him. The LBS sever consist of all this information so one can make a trade of it. For example one can sell it for advertise or other public activities. That's why keeping the trust on the LBS server is not a much confidential way. The private information can be fall into the non-trusted party. So there is a great need to prevent the user's private data to be shared from the LBS server.

2. LITERATURE SURVEY

In the existing system the all the users are get connected to the LBS server for requesting their queries. These all queries also content the user's personal information. Some of the existing methods are stated as follow.

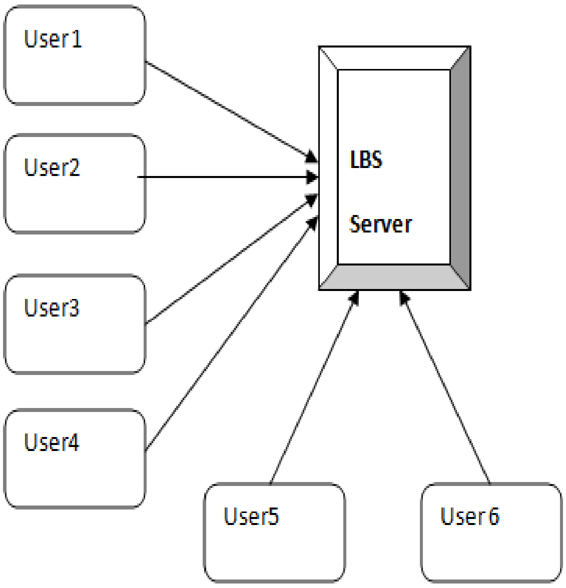

Fig -1: Architecture of the existing system

2.1 Green GPS System

The Green GPS is the navigation based technology which gives assumption to the car driver about the travel distance and the respective fuel require. It maintains two databases. First one is OSM database. This maintains the map data and corresponding street parameters in XML format. Second, one is car\driver database. This maintains the car and driver specific parameters. The user gives his input to the front end GUI which displays the routs. Then these routes are get converted into the latitude and longitude by the geocoder. Then system uses the Gosmore routing to find fuel optimal shortest and fastest routes.

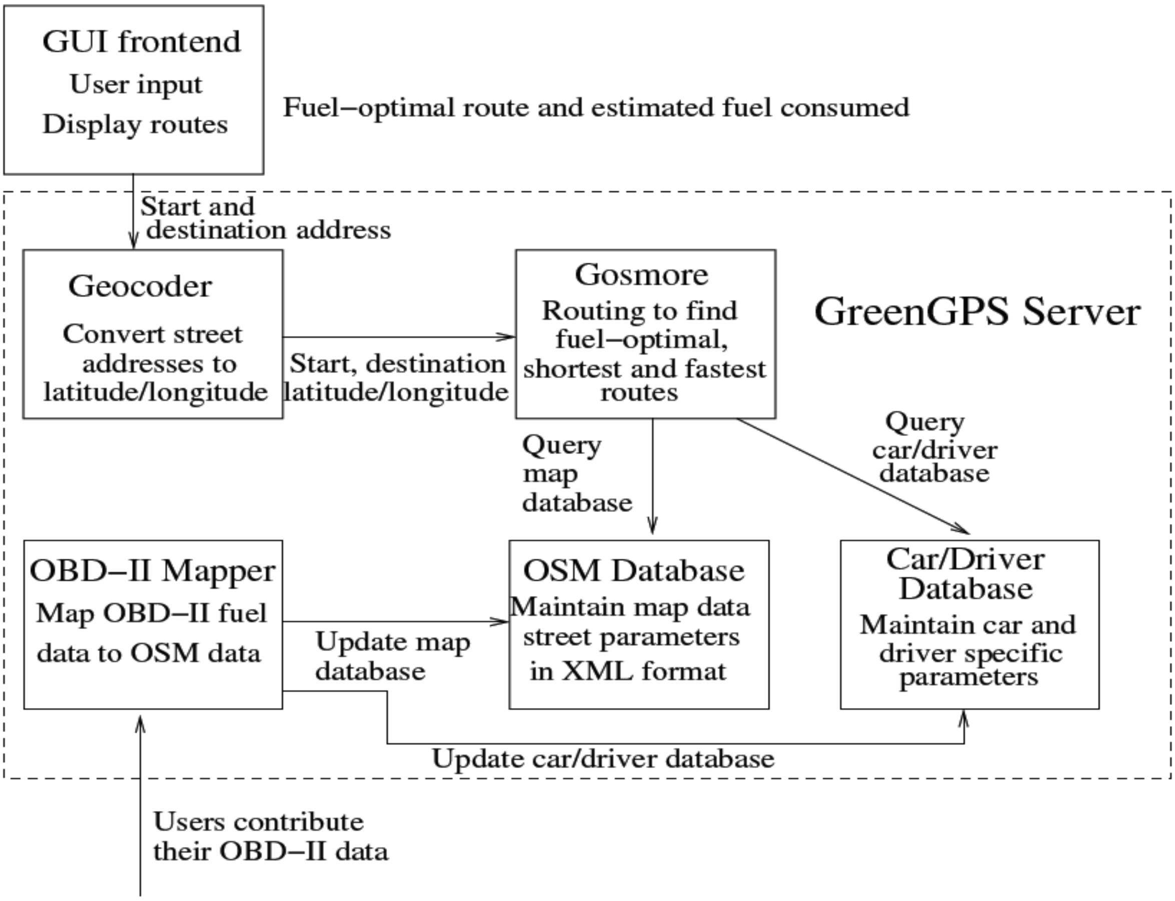
GUI frontend
User input
Display routes
Fuel−optimal route and estimated fuel consumed
Start and destination address
Geocoder
Convert street addresses to latitude/longitude
Start, destination latitude/longitude
Gosmore
Routing to find fuel−optimal, shortest and fastest routes
GreenGPS Server
Query map database
Query car/driver database
OBD−II Mapper
Map OBD−II fuel data to OSM data
Update map database
OSM Database
Maintain map data street parameters in XML format
Car/Driver Database
Maintain car and driver specific parameters
Update car/driver database
Users contribute their OBD−II data

Fig -2: Green GPS Architecture

2.2 Traditional LBS Approach

The following figure shows the traditional approach of the LBS server. Here we can see that user is requesting to the LGS server for location. User is firstly getting connected to the wireless antenna. The by using the internet the user query is get submitted at the server. This query consists of the user location as shown in the figure. Here privacy is the main problem. Without any privacy preserving mechanism the server can find out list of all mobile users and may misuse this information. The server consists of large amount of the information.

If the information on the server is not being secure then the third party person can use that private information to blackmail or make harassment to the user.

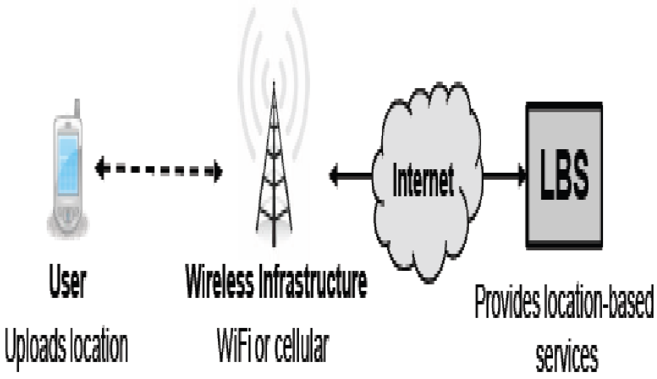

Fig -3: Architecture of Traditional GPS

2.3 Deanonymizing the mobility traces.

This consists of methods which can overcome: We can deanonymize the location traces which are easily picked from social network graph. The main idea behind this approach is that identity of user is traced by those meets: we are identifying anonymized users because a set of traces in contact graph which identify anaoymized users and they are structurally correlated with social network graph.

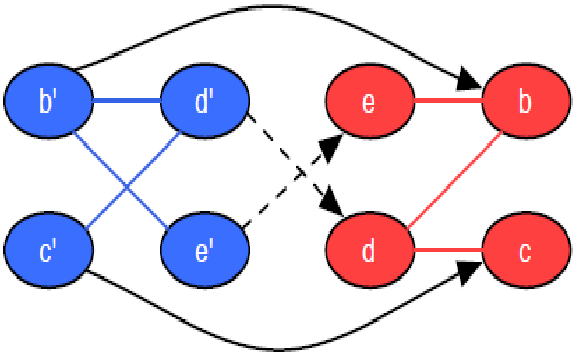

Fig -4: Mobility traces.

3. PROPOSED SYSTEM

In our proposed system we are going to hide the particular user from the LBS server. The user will able to get all the require information without being connected to the LBS server. The below figure shows the architecture of the proposed system.

Very first user in the particular region will place request to the LBS server. Along with his request his personal data will also get stored at server side. The server will provide the all require services to the user 1.

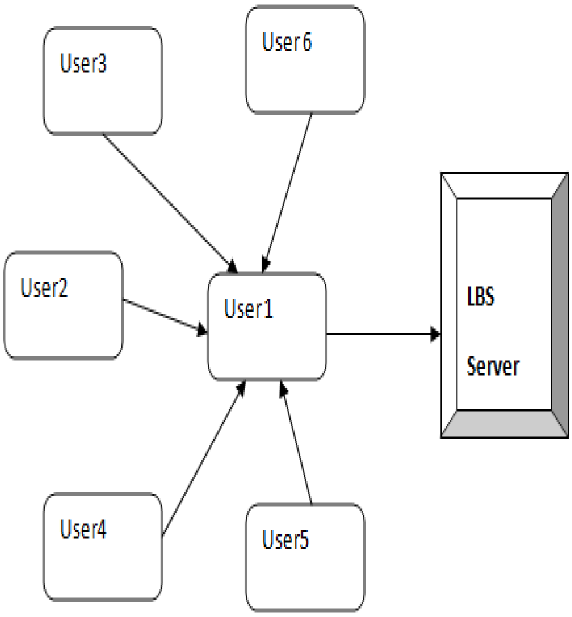

Fig 5-: Architecture of proposed system.

When another user try to request to the server in the same region then that user will not directly get connected to the LBS server. It will get connected to the previously connected users that is here it user 1. Then the user 1 will act as an LBS server to the all upcoming users in the same region.

4. CONCLUSION

Here we come to conclude that traditional way to use the location aware system is not secure and it can be very harmful to the user's privacy. To overcome this we proposed the new framework in which we do not change the architecture of the LBS server. Then also we are hiding the user specific data from the server by using the mobile crowd.

REFERENCES

[1]. "Pleaserobme," http://www.pleaserobme.com, 2014.
[2]. J. Meyerowitz and R.R. Choudhury, "Hiding Stars With Fireworks: Location Privacy through Camouflage," Proc. MobiCom '09, 2009.
[3]. F. Olumofin, P.K. Tysowski, I. Goldberg, and U. Hengartner "Achieving Efficient Query Privacy for Location Based Services," Proc. 10th Int'l Conf. Privacy Enhancing Technologies, 2010.
[4]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2008.
[5]. M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "A Parsimonious Model of Mobile Partitioned Networks with Clustering," Proc. First Int'l Conf. Comm. Systems and Networks, 2009.
[6]. R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying Location Privacy," Proc. IEEE Symp. Security and Privacy, 2011..
[7]. R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, "Collaborative Location Privacy," Proc. IEEE Eighth Int'l Conf. Mobile Ad-Hoc and Sensor Systems, Oct. 2011.
[8]. R. Shokri, P. Papadimitratos, and J.-P. Hubaux, "Mobicrowd: A Collaborative Location Privacy Preserving LBS Mobile Proxy (Demonstration)," Proc. Eighth ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2010.
[9]. "NIC": Nokia Instant Community," http://conversations.nokia. com/2010/05/25/nokia-instant-community-gets-you-social/.
[10]. "Wi-Fi Direct," http://www.wi-fi.org/wi-fi_direct.php, 2013.
[11]. A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Loction- Aware Services," Proc. Second IEEE Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW '04), p. 127, 2004.
[12]. C.-Y. Chow, M.F. Mokbel, and X. Liu, "A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-Based Service," Proc. 14th Ann. ACM Int'l Symp. Advances in Geographic Information Systems (GIS '06), 2006.

BIOGRAPHIES

Nilam V. Khandade has completed bachelor degree from Savitribai Phule Pune University and now ME student at RMD Sinhgad School Of Engineering from Savitribai Phule Pune University Maharashtra, India.

Snehal Nargundi Working at RMD Sinhgad School Of Engg. from Savitribai Phule Pune University Maharashtra, India