International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Hiding User Privacy in Location Based Services Through Clustering

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

[1, 2] Savitribai Phule Pune University, RMD Sinhgad School of Engineering, Warje, Pune, India

Abstract: ***Current age is a smartphone age, and so it use for surfing and browsing over internet is increasing and becoming popular. But most of the mobile users search some location specific queries which needs user location as input along with user query. All the smartphones these days are having an inbuilt location aware system known as Global positioning System. So in order to user any gps service, GPS user have to compromise all private information to the LBS server related to his information . While firing the location specific query to the serve,. It also sends some privacy information along with that query. LBS server stores this privacy information in database at and can make use of this user information as a money making business. But this is not a confidential way to share our private information at sever. Malicious servers may collaborate with third party users and thus compromise user information to malicious users. So the proposed system makes use of a clustering technique to hide all users location from LBS and still get the benefit of LBS service. This clustering method hide user location from LBS server and avoid sharing of privacy information with server. A user shares the information to the ip address or another user who has already compromised his/her location to the server and so other users at same location may get the benefit of it as there is no need of sending each and every uses' location to LBS directly .Here we have changed the architecture of LBS server Module.***

Keywords: Component; Mobile networks, location-based services, location privacy, Bayesian inference attacks, epidemic models..

1. Introduction

All over the world, people use smartphones for internet and location services. Smartphones are facilitated with a location tracking technology known as GPS (Global Positioning System) technology, is capable of providing location aware positioning services. GPS tracks user's current location in terms of latitude and longitude and sends it to LBS server. LBS server, then, provides services requested by user in relation to users query and users location. Smartphones are also Internet services with Wi-Fi system which establishes near field communication in small area network. GPS system is working on the basis of Wi-Fi and other Data facilities. Location aware devices are those devices which are capable of tracking location in static or active manner. Now navigation system are also provided along with positioning which are very helpful while driving. For surveying of location it communicate with local wireless devices. Major problem arises whenever user fires any location specific queries to the LBS server. These queries are directly sent to LBS server using the network. At server side, query possesses some location information of user, as Server does not allow any user to experience the services until user get registered at server for sharing his/her location. After registration server can able access all information about user. Server may access user's private information. One can misuse our private information to blackmail us. For example Lisa is using GPS services and she is on picnic right now. One can use this information and can try to robbery at her living place. Misuse of this information may arise the diversion on religion, public beliefs and political affair. This may be panic or harmful to the users.

Owner of LBS server can sell out or compromise the information out for daily soap advertisements. So we cannot be as trusty about LBS server for this information. Privacy of user may be access by third party. Therefore it is important to avoid sharing of private information from LBS server

2. Existing System

Below Figure 1, shows working of Existing system. In which all users are sharing their location to a centralized LBS server for Location based services which has no assurance of preserving user location and preventing it from getting compromised . Following are some existing systems.

A. Green GPS System

Green GPS is an approximation based method used for giving guidance to driver or traveler about fuel consumption along with navigation and requirements along with distance measurement. Green GPS has two databases. One is OSM database, which monitors the navigation data and respective street location points in XML type. Another on is the car\driver information recorder database. It provide GUI at front end to user where all information is being displayed. Induction are provided by user depending on that routes are displayed. Geo decoder converts these routes into longitude and latitude. This method is very useful to guess easily fuel consumption along with navigation distance.

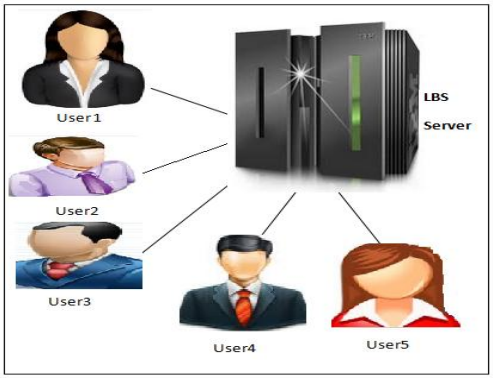


Figure 1. Architecture of existing system

Licensed Under Creative Commons Attribution CC BY

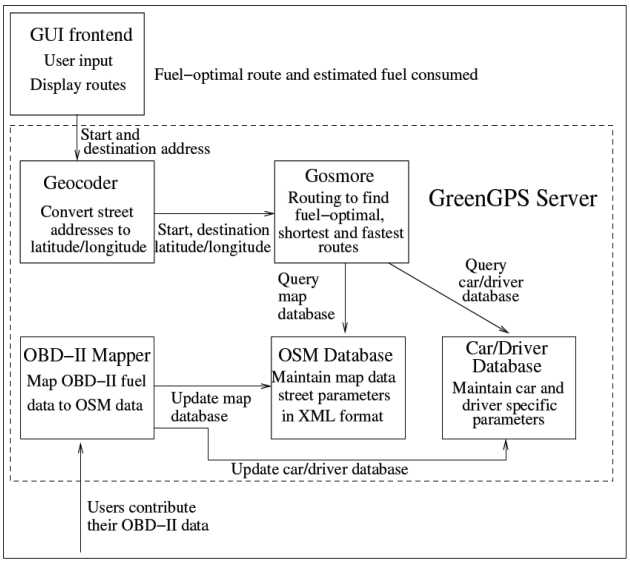


Figure 2: Green GPS architecture

B. Traditional LBS Approach

In traditional approach user sends request to server as shown in figure 3. For that user must connect to range antenna first. Then user query is get submitted to Server using data packet of internet. Query fired by user carries location of user. Server stores all information of user. It is not confidential to share all information to server. This information is less secure at server. And user has no option to avoid this.

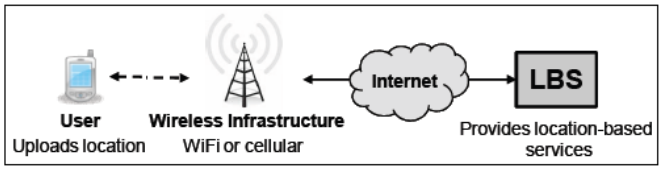


Figure 3: Traditional LBS approach

C. Deanonymizing the Mobility Traces

This uses de-anonymised methods to easily defeat user location traces. It is a better way because it generates social network graph of user location.

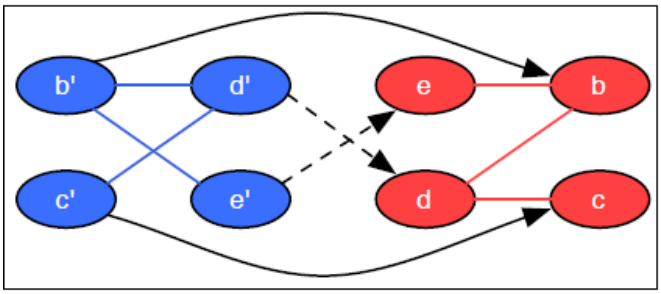


Figure 4: Mobility Traces

It also generate contact graph by identifying meetings of structural user and anonymised user. A user may be identified by meets graph and social network graph.

3. Proposed System

Our proposed systems objective is to hide location and private information of user from LBS server without compromising the services from LBS.The proposed system assumes that there are multiple user accessing the LBS services rom same location. So It can be termed of cluster of users. In a cluster C of users U, one of the user u_i will initially compromise its location to the LBS server. Once one of the user has connected to LBS, other users in a nearby vicinity can access the information from the first user which fires the query to LBS server on behalf of the other users. This leads to privacy preservation from LBS server.

As shown in below Figure 5, Other users will receive services from user 1. And user 1 will be act like LBS server to other users. There will be local communication in between server 1 and server 2 without sharing of private information.

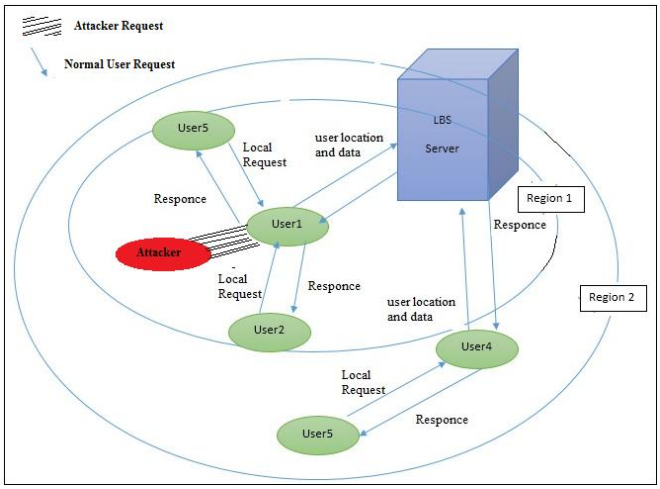


Figure 5: Proposed System Architecture

3.1 LBS Server Module

LBS server is a normal server that processes user queries in relation to user location and thereby provided location specific information for users queries. LBS provides location based information to the registered user which is present in particular region. For any user to fetch the information from the LBS, he needs to expose his location and device related private information so as to access services with full fedge. This can be benefitted by LBS server by compromising these information to third party for other malicious purposes. Also LBS servers are prone to Attacks such as DOS attack. If some users are continuously firing the queries and accessing LBS services , LBS server will have to serve the client and hence other user requests are denied from responding as LBS has already responding to other user or attacker.

3.2 User 1 Module

User 1 is considered to be the first user to share his private information and location details to LBS which on behalf of other users will send the information to LBS and act as middleware between other users and LBS. Very first user in system must share his private information to the LBS server. It will firstly select the region at which user wants to search

Licensed Under Creative Commons Attribution CC BY

the location, after that he will request server by sending a location based query. After connection with LBS server this User will Act as a server for upcoming users in same region. The User 1 in spite of acting as an LBS server to other users, attackers may attack such users too, so as to deny other users from getting the service.

3.3 User 2 Module

The second upcoming user will request for a location by fetching location based query along with the region. Then he will directly get connected to the first user instead of getting connected with LBS Server. The user1 and user2 will form a local request reply network. There is no need to share private information about user 2 to user 1. Hence here privacy of all upcoming users will get preserved.

3.4 DOS Attack Detection Module

As LBS may get compromised with malicious third parties, some malicious user may even try to attack LBS or the User 1 itself, So, the Denial of service attack is the major concern in the proposed system which is eradicated as follows:

a. User 1 has registered to the LBS as is serving other requests in the same region on behalf of LBS.
b. Malicious user may try to continuously get the service from User 1 and keep it busy for longer time and thereby compel other users to compromise their location to LBS and get the services as User 1 cannot respond to other users queries at same time.
c. If the User 1 detects that within a threshold value time or for x count of requests, user x has exceeded the count of request sin some particular threshold time, User 1 will not process the User x requests from that same Ip for the current session, so there user 1 becomes free to serve the other clients too.

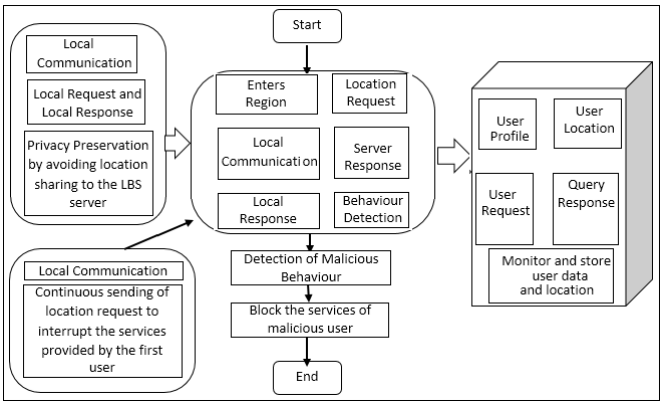


Figure 6: Block diagram of proposed framework

4. Mathematical Model

In a cluster *C* of users *U={u1,u2,u3,....un},* one of the user u_i will initially compromise its location to the LBS server. Once one of the user has connected to LBS, other users in a nearby vicinity can access the information from the first user which fires the query to LBS server on behalf of the other users.

For the proposed system, we assume that at a time single user will be served by $User_i$ for Location based service.

So mathematical representation of $User_1$ Service module is as follows:

If($User_j$.getSource().getIP().requestCount()<= threshold)
{
$User_i.query=User_j.getLocation().getQuery();$
$User_i.response=LBS.response(User_i.query)$
}
Else
{
$User_j$.getSource().getIP().Blocked; for current session
}

Where ,
Userj is the other user apart from one registered to LBS,
Useri is the user who has compromised location to LBS,
getSource().getIP() gives the Ip address of the requesting user.
Useri.query is the query that will be passed by useri to LBS.

5. Working of Proposed System

Steps:
1. User 1 registers itself to the LBS server.
2. LBS server stores the personal information of User 1.
3. User1 sends Region Information to LBS server.
4. User 1 request for a location.
5. Server processes user 1 location query and returns results.
6. User 2come into same region as that of user 1.
7. User 1 sends location request.
8. User 1 receives user2 request.
9. Local communication is establish between user1 and user 2.
10. User 1 sends request of user2 towards LBS server.
11. LBS server send reply to user1.
12. User1 sends result to User2.
13. Same process followed by all users in same region.
14. Malicious user send request to User1 in continuous manner and tries to interrupt the services of user 1.
15. User1 detects malicious user and block the services for that user.

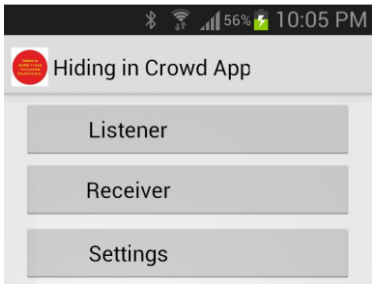
6. Experiment and Results

The proposes system is location based query processing system and thus whose efficiency is computed by avoiding location compromising to the LBS by all the users.

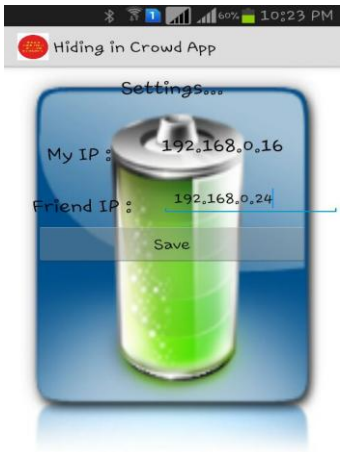
6.1 Settings Menu

User 1 stores the ip of the requesting user and requesting user stores the ip of the User1

Licensed Under Creative Commons Attribution CC BY



a)

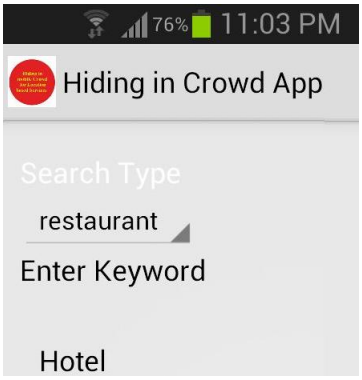


b)

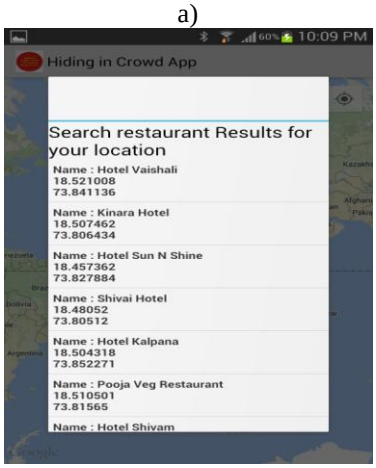
Figure 7: a) Home Screen , b)Setting Menu

6.2 Receiver Menu

Requesting user sends query by selecting query type and typing keyword related to query and receives the search results related to that keyword and access the data received from User1.



a)



b)



c)

Figure 8: a) Requested user sends query, b) Get search results related to query, c) location map related to query

6.3 Listener Menu

User 1 acts as Listener ; When requested user sends query then User1 send it to LBS and get the search results and provides search results to requested user.

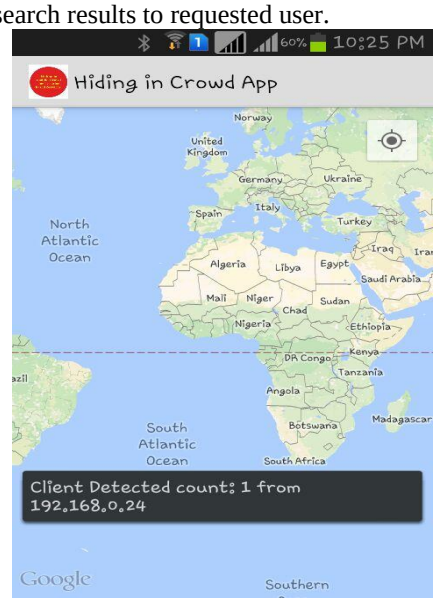


Figure 9: User1 receives query request

6.4 Detecting and Blocking Malicious User

If requesting user is malicious user then it will cross the threshold value and get detected by User1.User1 then blocks the services for that malicious requested user.

Licensed Under Creative Commons Attribution CC BY



Figure 10: User1 detects and block services for requested user

7. 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] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A Distortion- Based Metric for Location Privacy," Proc. Eighth ACM Workshop on Privacy in the Electronic Society (WPES '09), pp. 21-30, 2009.
[6] 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.
[7] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying Location Privacy," Proc. IEEE Symp. Security and Privacy, 2011.
[8] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A Unified Framework for Location Privacy," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (HotPETs), 2010.
[9] 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.
[10] "NIC": Nokia Instant Community," http://conversations.nokia. com/2010/05/25/nokia-instant-community-gets-you-social/.
[11] "Wi-Fi Direct," http://www.wi-fi.org/wi-fi_direct.php, 2013.
[12] R.K. Ganti, N. Pham, H. Ahmadi, S. Nangia, and T.F. Abdelzaher, "GreenGPS: A Participatory Sensing Fuel-Efficient Maps Application," Proc. ACM Eighth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '10), 2010.
[13] Y. Liu, A. Rahmati, Y. Huang, H. Jang, L. Zhong, Y. Zhang, and S. Zhang, "xShare: Supporting Impromptu Sharing of Mobile Phones," Proc. Seventh Int'l Conf. Mobile Systems, Applications, and Services, 2009.
[14] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the Privacy Risk of Location-Based Services," Proc. Fifth Int'l Conf. Financial Cryptography and Data Security (FC '11), pp. 31-46, 2012.
[15] M. Srivatsa and M. Hicks, "Deanonymizing Mobility Traces: Using Social Network as a Side-Channel," Proc. ACM Conf. Computer and Comm. Security, pp. 628-637, 2012.
[16] N. Vratonjic, K. Huguenin, V. Bindschaedler, and J.-P. Hubaux, "How Others Compromise Your Location Privacy: The Case of Shared Public IPs at Hotspots," Proc. 13th Privacy Enhancing Technologies Symp. (PETS), 2013.
[17] B. Hoh and M. Gruteser, "Protecting Location Privacy through Path Confusion," Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks, 2005.
[18] 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.
[19] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the Optimal Placement of Mix Zones," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (PETS '09:), pp. 216-234, 2009.
[20] 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.
[21] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an Old Cloak: K-Anonymity for Location Privacy," Proc. Ninth Ann. ACM Workshop on Privacy in the Electronic Soc., 2010.
[22] M.E. Andr_es, N.E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-Indistinguishability: Differential Privacy for Location- Based Systems," Proc. ACM SIGSAC Conf. Computer and Comm. Security, 2013.
[23] R. Chow and P. Golle, "Faking Contextual Data for Fun, Profit, and Privacy," Proc. Eighth ACM Workshop on Privacy in the Electronic Soc. (WPES '09), pp. 105-108, 2009.
[24] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting Location

Licensed Under Creative Commons Attribution CC BY

Privacy: Optimal Strategy against Localization Attacks," Proc. ACM Conf. Computer and Comm. Security, 2012.
[25] F. Santos, M. Humbert, R. Shokri, and J.-P. Hubaux,"Collaborative Location Privacy with Rational Users," Proc. Decision and Game Theory for Security, pp. 163-181, 2011.
[26] R. Shokri, G. Theodorakopoulos, G. Danezis, J.-P. Hubaux, and J.- Y. Le Boudec, "Quantifying Location Privacy: The Case of Sporadic Location Exposure," Proc. 11th Int'l Conf. Privacy Enhancing Technologies, 2011.
[27] T. Jiang, H.J. Wang, and Y.-C. Hu, "Preserving Location Privacy in Wireless LANs," Proc. Fifth Int'l Conf. Mobile Systems, Applications and Services (MobiSys), pp. 246-257, 2007.
[28] 3rd Generation Partnership Project, "3GPP GSM R99," Technical Specification Group Services and System Aspects, 1999.
[29] G. Theodorakopoulos, J.-Y. Le Boudec, and J.S. Baras, "Selfish Response to Epidemic Propagation," IEEE Trans. Automatic Control, vol. 58, no. 2, pp. 363-376, Feb. 2013.
[30] J. Krumm, "Inference Attacks on Location Tracks," Proc. Fifth Int'l Conf. Pervasive Computing (Pervasive '07), 2007.
[31] R. Shokri, "Quantifying and Protecting Location Privacy," PhD dissertation cole polytechnique f_ed_erale de Lausanne, 2013.
[32] M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "CRAWDAD Data Set Epfl/Mobility (v. 2009-02-24)," 2009.

Author Profile



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.



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

Licensed Under Creative Commons Attribution CC BY