Open access Journal International Journal of Emerging Trends in Science and Technology

Collaborative Location Privacy through Buffering

Authors

S. Jayasree[1], S. Keerthana[2], R. Manju[3], Dr. K. Valarmathi (M.E., Ph.D)[4]

Panimalar Engineering College, Chennai, Tamilnadu

Email: [1]*jaisrisekar1501@gmail.com*, [2]*keerthuvedha@gmail.com*, [3]*manjuradhakrishnan94@gmail.com*

[4]*valarmathi_1970@yahoo.co.in*

ABSTRACT

Location based services available in the smart phones are used to gain information about the surroundings. Users query the location based server by passing their position information thereby losing their privacy. A user collaborative approach to preserve the location privacy was introduced, where the users are hidden from the server when the information is already available among any peer device. This approach cannot be used when the users are not ready to cooperate or the informed users are outside the range of communication of user seeking the information. So in this system a common authentication server is used to store the response from the location based server when any user accesses context information for the first time. This information in authentication server can now be used by other users who require the same information without contacting the server even when the informed users are not nearby. Thus the privacy of the users is found to increase in a considerable manner.

Keywords: *Location Based Service, Location Privacy, Authentication Server*

1. INTRODUCTION

The introduction different technologies such as wireless networks, Geographical information systems (GIS), Internet and Global Positioning Systems (GPS), have led to the development new type of information technology called Location Based Service (LBS).Location Based Services are applications available within the mobile phone with the ability to locate a mobile user geographically and provide services to the user based on the users location. These services are used by the people to learn about their surroundings on the go. It can be used to provide many useful services. For example, LBS can provide traffic information, routes, weather reports, information about location of hospitals, police stations, restaurants, ATMs, tourist places etc.

The main problem in using location based services is the exposure of highly private information. Whenever a consumer uses a location based service their current location is submitted to the server. This information collected and held by LBS can reveal highly personal information such as where the customers go, whom they are acquainted with and what they do. Failure in protecting this information not only violates the customers' right to privacy but also threatens the customers' freedom of expression and association. The threat is already being realized. If privacy protections for the information collected by LBS is not established the growth of LBS will go to an end.

The solutions to enhance the privacy of users fall into the following two categories: centralized and user-centric approaches. In centralized approach third party servers are introduced whose prime work is to protect the user's information. In user-centric approaches the users themselves take the responsibility to protect their location information.

The centralized approach to protect the user's privacy can be done in the following ways. Third party server acts as an intermediary between the user and the location based service server. These third party servers could anonymize the user query i.e., the users details can be removed from the query or it could merge the user's queries [1] with that of other users so that the LBS server only sees a group of queries. These approaches transfer the problem from the LBS server to the introduced third party server. These third party servers can also be hacked by the attackers requiring user's private information. The technique named MobiCrowd depends on users collaborating among themselves. Our system aims to improve the privacy of users than in MobiCrowd with the help of a common authentication server.

2. RELATED WORK

The problem of location privacy with location based services is of importance because it concerns the sensitive information about common users. The privacy protection approaches under discussion are usually under two categories user-centric and centralized approaches. This survey document deals with various techniques proposed to provide privacy protection to users and the ways the existing privacy approaches are defeated. Numerous techniques are available to preserve the privacy of the users. A technique named mixzone [2] was introduced to prevent tracking of long term user movements. User has one or more unregistered geographical regions where no application can trace user movements then this area is said to be Mix Zone. However, as users must remain silent inside the mix zones. The adversary's success is relatively high, even if the mix zones are optimally placed.

A technique to prevent the identification of users from anonymous spatial queries [3] was introduced in the year 2007. This framework prevents location based identity inference of users issuing spatial queries to location based services. . This model is applicable for real time scenarios, but challenging problem is to preserving anonymity in issuing continuous spatial query.

Space Twist [4] technique handles the problem of location privacy, query performance and query accuracy. This approach uses kNN queries (k-nearest neighbor). The query gets forwarded to the users incrementally until the exact response is retrieved by the queried mobile terminal. This technique assumes uniform data which is actually different from real world data.

Context-Aware Privacy Protection system [5] deals with two challenging issues in privacy-preserving LBS namely protection of user location privacy from both location data and network communication perspectives. It involves dimension-reducing projection of two-dimensional geographical points in one-dimensional space. CAP lays the foundation for upcoming studies of privacy-preserving LBS.

The approach named Geo-in distinguish ability [6] addresses the problem of privacy of users in location based services. A generalized version of differential privacy is used in this technique. In this approach user's location within a radius r is protected with a level of privacy that is dependent on r. The users submit approximate locations to the server instead of their original location. This method should be modified in order to make it applicable for complex applications.

R. Shokri. Et al., in the year 2014 introduced a new solution for location privacy. This technique named MobiCrowd [7] allowed the users to share the information among them in order to preserve their privacy. In this technique the users who are in need of location context information first broadcast requests to other nearby users in an adhoc manner. If the other users have the requested information the seeker can instantly receive it from them. The main disadvantage with this technique is that the new user can obtain the information from the informed user only when they are within the contact range of the new user and are ready to share the information.

3. PROPOSED WORK

The problems with the Mobi Crowd technique can be overcome by introducing a common storage area which is accessible to every user with devices having the ability to connect to the internet. Authentication server has been used as the common storage area to store the location-context information. The authentication server initially does not have any information. When a user first accesses the service the device has to check the availability of information in the authentication server. If the information is available in the authentication server the user can directly access the information from it. Otherwise the device sends a request to the location based service server. The device will receive the location context information from the server in response. Once the response is received the device will place the response received from the server in the authentication server. Now when the same query is posed by some other user they can retrieve the information directly from the common authentication server.

This method is collaborative in that the user receiving the information from the server first helps other users to hide from the server by placing the information in the common authentication server storage. Moreover this technique can increase the number of times the users have to contact the server by having the context information within the authentication server instead of depending on the nearby users alone to hide from the server. The information will be available in the authentication server even when the users who have first received the information from the authentication server move outside the contact limit of the new user. With this technique the users need not unnecessarily deplete their battery power by allowing other devices communicating with it continuously to receive the location context information from it.

The architecture diagram in Figure 1 clearly specifies the structure of proposed system. The users initially send a request to the authentication server to check the availability of the needed context information. If available the Authentication server passes the information to the querying device. Otherwise, the user passes the request to LBS and retrieves the needed information. Finally the users store the context information in the authentication server which is available to other users.

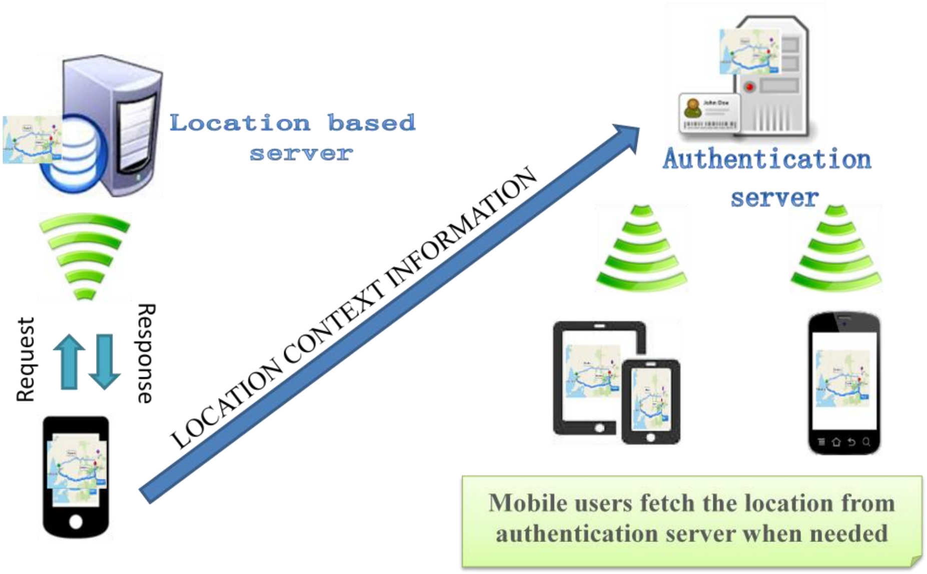

Location based server
Authentication server
Request
Response
LOCATION CONTEXT INFORMATION
Mobile users fetch the location from authentication server when needed

Figure 1: Architectural design of location information system using buffering mechanism

4. OUTPUT

The implementation of the proposed system is presented as follows. An application named Finder is developed and installed on an android mobile and the following screen shots are obtained. The Google map server is used as the location based server in developing this application. The screen given below presents the user a search field to enter the query.

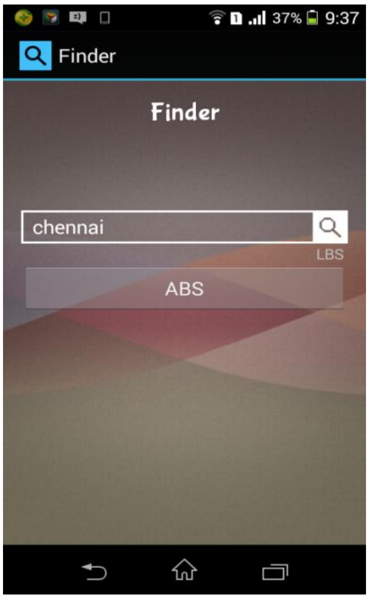
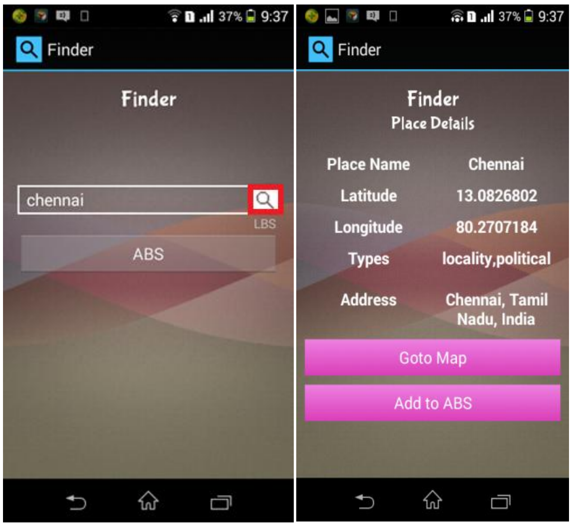


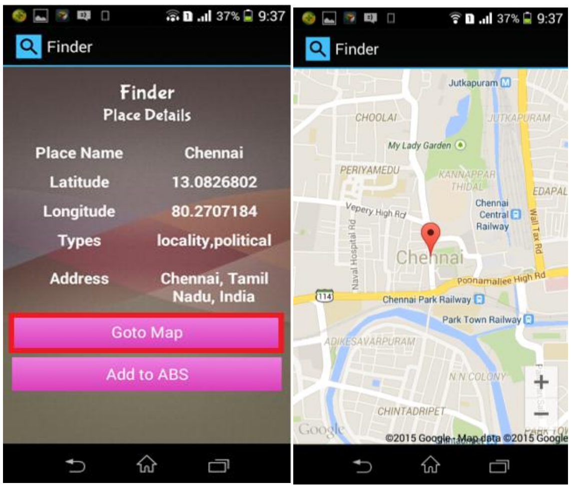
Figure 2: Search Screen

SEARCHING IN THE LOCATION BASED SERVER



Place Name Chennai
Latitude 13.0826802
Longitude 80.2707184
Types locality,political
Address Chennai, Tamil Nadu, India

Figure 3: Displayed context information on LBS search



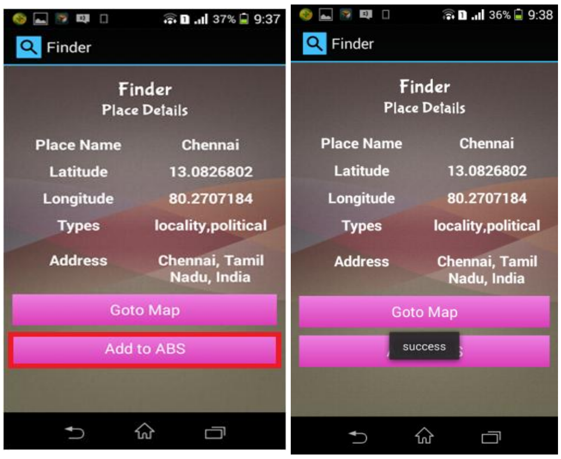
Place Name Chennai
Latitude 13.0826802
Longitude 80.2707184
Types locality,political
Address Chennai, Tamil Nadu, India

Figure 4: Map retrieved from LBS server

The above screen shows the location details that are retrieved from LBS and its location in the map.

STORING CONTEXT INFORMATION IN AUTHENTICATION SERVER

The next step is to place the context information obtained from the location based server in the authentication server. The collaborative action is carried out in this step by storing the information Authentication server to help the other users.

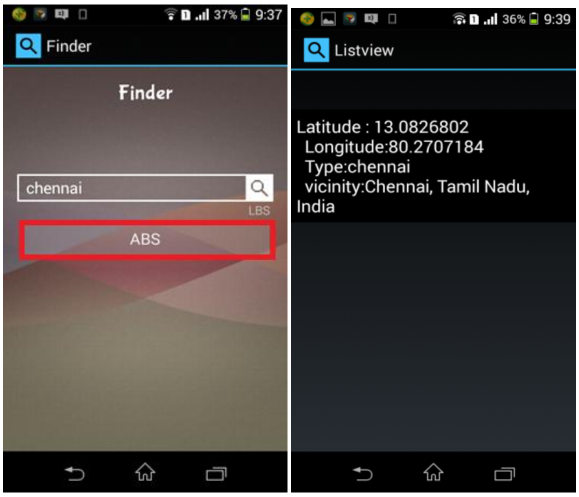


Place Name Chennai
Latitude 13.0826802
Longitude 80.2707184
Types locality,political
Address Chennai, Tamil Nadu, India

Figure 5: Storing the context information in Authentication server

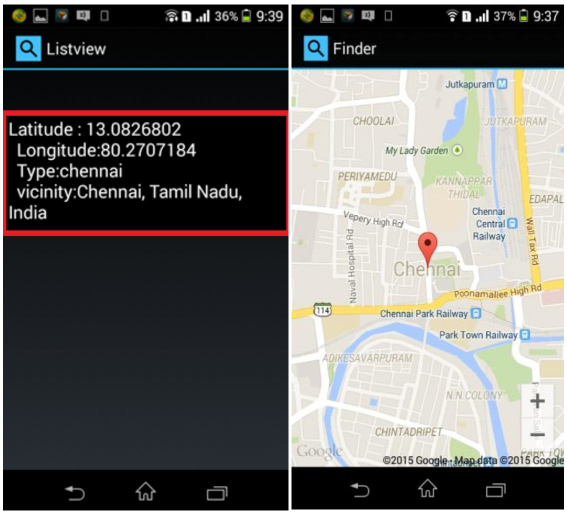
SEARCHING IN AUTHENTICATION SERVER

Once the location is available in the authentication server the context information can be directly obtained from it. This allows the users to hide from the location based server thereby improving the user’s privacy.



Latitude : 13.0826802
Longitude:80.2707184
Type:chennai
vicinity:Chennai, Tamil Nadu, India

Figure 6: Searching details in Authentication server



Latitude : 13.0826802
Longitude:80.2707184
Type:chennai
vicinity:Chennai, Tamil Nadu, India

Figure 7: Map retrieved from Authentication Server

5. CONCLUSION

This paper is concerned with the problem of location privacy in location based services. Authentication server is used to store the responses retrieved by users. This approach improves the privacy of users by allowing them to hide from the server when information is available with the Authentication server. This approach provides better privacy to users than the MobiCrowd technique.

REFERENCES

1. J. Meyerowitz and R.R. Choudhury, “Hiding Stars With Fireworks: Location Privacy through Camouflage,” Proc. MobiCom’09, 2009.
2. A.R. Beresford and F. Stajano, “Mix Zones: User Privacy in Location-Aware Services,” Proc. Second IEEE Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW ’04), p. 127, 2004.
3. Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis and Dimitris Papadias, “Preventing Location-Based Identity Inference in Anonymous Spatial Queries”, Proc. IEEE Trans. on Knowledge and Data Engineering, Vol. 19 , Issue: 12 ,p. 1719 – 1733
4. Man Lung Yiu , Christian S. Jensen, Xuegang Huang and Hua Lu, “SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services”, Proc. IEEE 24 th international conference on Data Engineering, 2008, p. 366 – 375.
5. Pingley, A. Wei Yu ; Nan Zhang ; Xinwen Fu ; Wei Zhao , “CAP: A *C*ontext-*A*ware *P*rivacy Protection System for Location-Based Services”, Proc. 29th IEEE international conference on Distributed Computing Systems, 2009. ICDCS '09, p. 49 – 57
6. M.E. Andr_es, N.E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi,“ Geo-Indistinguish ability: Differential Privacy for Location-Based Systems,” Proc. ACM SIGSAC Conf. Computer and Comm. Security, 2013.
7. Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, and Jean-Pierre Hubaux, “Hiding in the Mobile Crowd: Location Privacy through Collaboration”, IEEE Trans. on Dependable and Secure Computing, vol. 11, No.3, p. 266 - 279