International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1	**VOL**	02
Website	icssccet.org	**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016	**Accepted**	10 - March – 2016
Article ID	ICSSCCET029	**eAID**	ICSSCCET.2016.029

Traffic Reduction on the Server Sides using Hilbert Curve in the Mobile Crowd Sensing

S Umadevi[1] and K Kalaiselvi[2]
[1,2]Assistant Professor, Department of CSE, Karpagam Institute of Technology, Coimbatore

Abstract-*Location based service help the user to know about their surroundings when the user queries the required location to the LBS server. In user-collaborative privacy-preserving they keep the context information in the use mobile buffer and pass it to other user seeking that information. However such request gives away the private information of one user to the other user. In the proposed method users security and network traffic can be reduced by, using Cachecloak and Hilbert Curve Algorithm. Cachecloak for temporary storage of the entire predicted path to avoid frequent request by the user to the server so that network traffic on the server side can be reduced. Hilbert Curve Algorithm to find the Nearest Neighbor: gathering a group of requesting user in the nearest location and sending it to the server when there is no requested data on the cache. Through the above methods, the security is highly provided to the users and the processing time on the server side also gets reduced.*

Index Terms—*Mobile networks, location-based services, location privacy, cachecloak, Hilbert curve*

I. INTRODUCTION

SMARTPHONES, is a powerful computing mobile device, offers various methods of localization..Among other increasingly powerful mobile computing devices, offer various methods of localization. Integrated GPS receivers, Wi-Fi access point, helps the user to position themselves accurately, which led to the offering of Location-based Service (LBSs). These services provide the information which is needed by the user. First each data in a particular location has to be uploaded in the server. The service needed for the user has to be queried by them and has to be send to the server. The server in turn matches the data which has been received from the user with the data stored in the database on the server side. If the requested query matches with the data of the database, then the server send the data to the user. By this way the user can know the current position and their surroundings, e.g., contextual data about point of interest such as colleges, hospitals or more dynamic information such as traffic condition.

Even though LBSs are convenient to trace out the information about a particular location, it is very dangerous since it traces out the location of the user and can hack the user privacy. Each time when the user submits the query to the server to know the up-to-date information, private information of the user is revealed.

Even worse, the user's personal data, their habit, religious beliefs, and political affiliation, can be known by the server. Finally, real-time location reveals a person vulnerable to absence of disclosure attack: knowing that someone is away from home could allow someone to break into their home and can blackmail them.

This information will be collected by the LBS operator. Finally user-sensitive data will fall into the hands of untrusted parties. To avoid these problems, two main categories such as centralized and user-centric approach have been used in the early proposal of the project.

Cite this article as: S Umadevi, K Kalaiselvi. "Traffic Reduction on the Server Sides using Hilbert Curve in the Mobile Crowd Sensing". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 149-153. Print.

A. Centralized and User-Centric

In centralized approach they have introduced a third party, which protect the users by operating between the user and the LBS. This approach had a problem whether the trusted third party will be secure. Another centralized approach has been used, such as encryption using PIR, which stored the user data in different format. User-centric approach operates on device. The aim of this approach is to blur the location information, allowing the users Smartphone inaccurate, noisy GPS coordinates to the LBS server. The problem in this approach is that LBS response would be inaccurate or untimely. Obfuscation is also a problem when there is an inaccuracy of data [6].

In this approach we avoid the problem of hacking of one user's private information to the other user when the seeker sends the request to the user who is having the requested data.

The key idea in the paper, called mobile crowd is that a separate cache cloak is used which is used to store the previous data which has been already requested by the user for the particular information to the server side will be stored temporarily in the cache cloak for a particular period of time. Hence cache cloak is used as a temporary storage. Hence the network traffic on the server side can be reduced i.e when many user send the same request for the same particular location to the server the same message will be send to all the user who are requested for the same location. The problem is that network traffic on the server side will be increased. To overcome this problem cache cloak has been introduced. By this approach the data will be stored on the cache cloak whenever the data is retrieved from the server.

If there is no data on the cache cloak then there is no chance, the user has to send the query to the server to get the details of a particular location. At this point the server has the chance to track the privacy of the user. in order to avoid this problem Hilbert curve algorithm is used. By this approach the nearest neighbor around the user for a particular location will be searched. All the queries of the entire user will be gathered together and will be send to the server. By this way the server cannot track the particular user and hence the privacy of the user can be protected.

II Related Works

There are many related schemes for mobile network. Queries can be submitted in different query form from actual user queries, possibly by encryption technique using private information retrieval PIR[3], or data can be stored differently(eg., encryption or encoded technique to allow private access[4].

Mobile users, for example, allow users to find the most nearest route between two points for fuel efficient [7]. Various threats while sharing location information have been identified for example users can be identified easily if they share their location periodically to the server [8].Knowing the social relations between anonymized users in a set of traces will leads to trace the location of each user[10].

Finally, location sharing between the users not only diminishes her own privacy, but also the privacy of others [9]. Many techniques have been proposed to protect the privacy of each user in the location based service. Technique like anonymization can be used to protect the user (user's identities can be removed), pseudonym user's real name can be replaced by temporal false name), obfuscation (perturbing some spatiotemporal information with user's query).

Finally camouflaging method can be used in which some dummy queries can be added, or be eliminated completely and can be hidden from the LBS [11].Perturbation algorithm is applied in cross paths areas where at least two users will meet together. This increases the confuse in paths of different users[2].Changing pseudonyms of each user while passing through pre-defined spots known as mixed zones[1] ,becomes difficult for tracking the user along their trajectory path.

However silent must be made by the user along this mixed zone, which means that LBS cannot be used by the user. In order to overcome this problem, the mixed zone size has to be kept small, which in turn the user's query cannot achieve the highest limit by the LBS server. Even when the mixed zones are optically placed, the success of adversary is relatively high [3].

Spatial cloaking algorithm is used where peer-to-peer (P2P) service is provided in which mobile and stationary user form a group and share their data[4], which in turn the privacy of each user can be known by the other user. Centralized anonymity server is placed between the user and the server and the identity i of the user is removed by this method and only the location and query is submitted to the sever by this method [5], which in turn accuracy data will not be provided.

The user's queries can add the dummy queries for eg., noise can be added to confuse the adversary about user's real location. But when dummy queries are generated it diverts the actual location of the user [7], as they need to look actual queries over time and space.

Cite this article as: S Umadevi, K Kalaiselvi. "Traffic Reduction on the Server Sides using Hilbert Curve in the Mobile Crowd Sensing". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 149-153. Print.

When we do not address the local observer who is trying to interfere in other's user private information, by changing MAC addresses for Wi-Fi network by frequently changing device identifiers [11] similarly changing the TMSI for GSM networks [2].

III Problem Statement 3.1mobile Users and LBS

When N number of users is considered, who moves in an area is split into M discrete. We consider N users who move in an area split into M discrete region/location. Each user having location based wireless-device capable of having device-to-device ad-hoc network and are connected to wireless network (e.g., cellular and Wi-Fi network). As the user moves around the region, they submit the query of their particular location to the LBS. The frequency at which the user query the LBS will be changing based on location as they moves and the request given by the user.

The information provided by the LBS can be stored in the user's mobile buffer. This information can be view by the user for future reference. At the same time to avoid the tracking of user by the server these data can be send to the other user who are seeking the information. But the problem arises during transfer of data from one's user mobile to the other user through Wi-Fi is that not only the requested data will be transferred but the user's private information will also be transferred. Hence the privacy of the user data is not protected. Thus the trusted third-party (TTY) is a major problem while transferring the data between the users. Even though the users are protected from the server they are hacked by the other users. Hence privacy mechanism has been failed.

IV Design Objectives

When the user sends the query to the server to gather the information for a particular location the server will get the requested information from the database of the location based service. Then the servers will response to the user by sending the data's of the requested information. At the same time these data will be stored in the cache for the other user who needs the same data for the next time. When the second user sends the request for the same location it first searches for the data in the cachecloak.

If the requested data is found on the cache cloak the data will be sending to the corresponding user from the cache. Hence the traffic on the server side can be reduced. If the requested data is not found on the cache cloak then there is no choice, the request has to be send to the server side and the data will be gathered and will be send to the respected user. Hilbert curve algorithm for gathering a group of users who are requesting the information for the particular location and sending the entire request together to the server .

A. Path Confusion

Another problem is that mix zone will occur that is when two users are at the same location at the same time. For instance when the two users are at the same intersection point of a road their path becomes indistinguishable. At this point when the two user sends request for two different direction of location the server gets the data from location based service but the server gets confused for which user the particular data has to be send. Since both the user are at the same location the server gets confused to deliver the correct data to both the user and there is a chance to deliver data incorrectly to both the user. This is the main problem in the delivery of data by the server.

B. Predicted Privacy

To overcome the problem of path confusion predictive privacy method is used. By this method when the user sends the query for a particular location to the server, the server in turn gather all the nearby location from the location based service. This information will be stored in the cachecloak. When the user request the other information for the same location there is no need to contact the server. In turn these data can be retrieved from the cache which has been already stored in it. Hence the network traffic on the server side can be reduced and also the privacy of the user can be increased since there is no need to access the data many times for the same location. If user does not access the server many times then the server cannot track the user wherever he goes. Hence the privacy of the user can be protected.

V Our Schemes

Based on the design objective stated above, location privacy preserving mechanism for LBSs server has been employed. High effectiveness can be brought by hiding user queries from the server, we have proposed a mechanism in which user queries can hidden by using the cachecloak which minimizes the exposed information about user's location to the server.

The main objective behind our scheme is that once the information is retrieved from the server a copy of these data is stored in the cachecloak as a temporary storage.

Cite this article as: S Umadevi, K Kalaiselvi. "Traffic Reduction on the Server Sides using Hilbert Curve in the Mobile Crowd Sensing". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 149-153. Print.

Hilbert curve algorithm is done in order to avoid the user from attack by the server when they are accessing the data when there is no data on the cache.

VI Scheme Details

A. Location Base Searching

Mobile device are very useful to the user and also portable and flexible and can be anywhere at any time. With the help of the GPS which are available in the mobile the user can get the details of any location at any time. To get the details of a particular location for e.g., about college, hospitals, theater, hotels, etc, the user can enter the query and send the request to the server. The server in turn responses to user's by providing the information which is requested by the user.

B. CacheCloak

To reduce the network traffic on the server side while accessing the data frequently by the user cache cloak is created as a temporary storage. This temporary storage is created on the cloud. The data availability can be of any days based on the retrieval of data by the users. If the second user needs to retrieve the data first the request will be checked on the cachecloak whether the requested data is present on the temporary. If the data is present it is given to the corresponding user. Thus the user is protected from the attacks from the server side since the user has not visited to the server side. At the same time the network traffic on the server side can be reduced since most of the retrieved data will be stored as a temporary storage and these data can be retrieved by the other user who is requesting the data for the particular location without visiting the server.

C. Retrieving Data About Service

The user can retrieve data about the location which is needed for him from the cache if the data is already available in the temporary storage. Hence the user is protected from the attack of server. At the same time the network traffic on the server side can be reduced. The privacy is indicated to the user by indicating that the data has been retrieved from the cache. It can be viewed by the user and hence he can be satisfied with it.

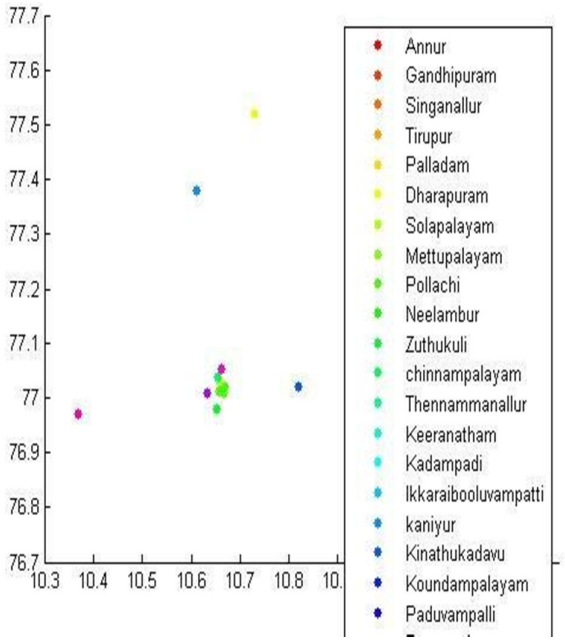

Figure 1: Privacy Preserving

The figure gives the various location and the dotted symbol represent the tower located at various location. The values in the x-axis and y-axis gives the latitude and longitude at various location. When the user sends the request the server tracks the position of the user with the help of this latitude and the longitude value.

Cite this article as: S Umadevi, K Kalaiselvi. "Traffic Reduction on the Server Sides using Hilbert Curve in the Mobile Crowd Sensing". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 149-153. Print.

D. Hilbert Curve Algorithm

In case if the data is not present on the cache then there is no choice the user has to contact to the server. At this time it has the chance to track the user by the server when submitting the query by the user. In order to avoid this problem a technique called Hilbert curve algorithm is used. In this technique first if the user sends the query for particular information this technique first searches the cache whether the data is available. If the data is available, it will be provided to the corresponding user. In case if the data is not available the Hilbert curve algorithm searches the nearby user whether they are accessing the network

All the user request are gather together and will be send to the server side. Server in turn response by providing the information to the above technique. These data will be given to the corresponding user.

E. Security Enhancement

Since all the user's query are submitted at the same time the server can't track the user sine the server cannot identify with query is submitted by which user. Hence the security of the user from the server side attack can be increase. The network traffic on the server side can also be decreased since all the queries are submitted at the same time with the help of Hilbert curve algorithm.

VII Conclusion

The privacy of the LBS user has been increased by hiding the user from the server. The temporary storage of data is useful in preserving the user's private data and the network traffic on the server side has also been reduced. In the future work the distance of the particular location from the user present location and the directed can be provide which will be useful for the user to identify the location easily.

References

1. 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.
2. 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
3. J. Freudiger, R. Shokri, and J.-P.Hubaux, "Evaluating the PrivacyRisk of Location-Based Services," Proc. Fifth Int'l Conf. Financial Cryptography and Data Security (FC '11), pp. 31-46, 2012
4. 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.
5. R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P.Hubaux, "Quantifying Location Privacy," Proc. IEEE Symp. Security and Privacy, 2011.
6. 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
7. 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
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

Cite this article as: S Umadevi, K Kalaiselvi. "Traffic Reduction on the Server Sides using Hilbert Curve in the Mobile Crowd Sensing". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 149-153. Print.