Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

Protecting and Quantifying Privacy in Mobile Crowd Through Collaboration

Shashikala N
Department of Computer Science and Engineering
Shree Devi Institute of Technology
Mangalore

Shrikanth N G
Asst. Prof. , Department of Computer Science and Engineering
Shree Devi Institute of Technology
Mangalore

Abstract— Security is the one of the most important issue that has attracted a lots of research and development effort in past few years. Location knows mobile phones helps different location based services (LBS). User sending a request to LBS server, while doing this type of request for information provides a private data by using data LBS can find a user. To overcome this drawback by proposing a user collaborative security protecting. We are not using a third party server. So by doing collaboration with Smartphone's we can protect user's information. This device stores a data in cache, if any one needs such a information so that time they can share it no need of sending a request to server. While doing like this we can protect users location information from servers. The result shows that, protecting a high fraction of location based information's. Finally, our main implementation on smart phones shows that lightweight and low cost.

Keywords— Smartphone Network, Location based services, Location Security.

INTRODUCTION

Now a day's mobile phones are increasing, all Smartphone's helps for different types of places. Mobile phones support the GPS so by using these services we can find person locations. Users can be linked to their locations, and multiple pieces of such information can be linked to together. So they can misuse this information's, using this data they can blackmail his / her [1]. The drawback is providing security for users. We need to increase the quality of security for LBS users and two categories: centralized and user centric. In the centralized, using a third party in between user and LBS server [4]. Servers every time finds a requested information in a group [2]. This LBS server can misuse the user data i.e. they can modify data or they can identify user device [5]. Another approach is user centric; in this one their aim is to blur the location information. So by doing this method server does not able to send the requested data to the users [6]. So to overcome these problems users collaborate with each other to improve their security, without using a third party. Mobile Crowd is users can contact the LBS server if they cannot find the requested information in their neighbors' [7]. Compare to existing system our system is providing more security to users. Our approach can be used in the upcoming technologies [8]'. So smart phones directly communicate with each other developing a smart phone social network.

LITERATURE SURVEY

In the year 2009 J. Meyerowitz and R. Roy Choudhaury proposed a paper titled "Hiding stars with fireworks: location privacy through camouflage," To provide a security for particular faces from the untrusted location based services. Proposed a CacheCloak, this is a system provides something real time unknowns location data. CacheCloak it is a server provides a mobility predictions from historical data and submit dividing predicted paths to the LBS. Every time the predicted path is to divide with others users paths, no particular user path can be able to be relied on a rough path over time. Smartphone users retrieve cached information responses for successive new location from the trusted server, triggering new prediction only when requested information is not present in the present location. Protect user of CacheCloak, providing a measure of location privacy over time.

In the year of 2008 G. Ghinita, P. Kalnis, A. Khoshgozaram, C.Shahabi, and K L Tan Proposed a paper titled " private queries in the location based services: anonymizer are not necessary," Now a days all mobile phones providing a location capabilities. To provide security for user location must not be disclosed. In the existing system they introduced third party in between user and server. This as more problems: (1) Every user as to trust a third party (2) A large no of cooperating (3) Security providing only for particular user. To overcome this problem proposed a framework to help a private location dependent query, based on private information retrieval (PIR). In the proposed system no need third party security will be providing through cryptographic techniques. Compare to existing system proposed system is providing more security and this will be useful for to find a nearest neighbor.

In the year 2009 R. Shokri, J. Freudiger, M Jadliwala and J P Hubauux Proposed a paper titled " A Distortion based metric for location privacy," framework for measuring and evaluating location privacy preserving mechanisms in mobile wireless networks. Within in this framework, first present a formal model of the system, which provides an efficient representation of the network users. This model generally expresses and analyzes a variety of location privacy metrics that were proposed earlier. Proposed model, we provide formal representations of four metrics among the most relevant categories of location privacy metrics. We also present a detailed comparative analysis of these metrics based on a set of criteria for location privacy measurement. Finally, we propose a novel and effective metric for measuring location privacy, called the distortion based metric.

In the Y. Liu, A. Rahmati, Y. Huang, H. Jang, L. Zhong, Y. Zhang, and S. Zhang Proposed a paper titled "XShare: Supporting Impromptu sharing of Mobile Phones," Mobile phone loaded with a personal data e.g. photos, contacts, and call history. Sometimes we have to share our mobile phone with others. When we giving our mobile phone to others, that time they can access any data from our mobile. So for this problem we present a xShare, a protection solution to

address this problem. xShare allows a phone owner to rapidly specify what they want to share and place them into a restricted mode in that place only we can share a data and applications can be accessed. We then present the design of xShare based on file level access control. We describe the implementation of xShare on windows mobile and report a comprehensive usability evaluation of the implementation, including measurements and user studies. The evaluation demonstrates that our xShare implementation has negligible overhead for interactive phone usage.

In the year 2012 Mudhakar Srinivas, IBM T.J Watson Research Center, Mike Hicks, and University of Maryland Proposed a paper titled "Deanonymizing Mobility Traces: Using Social Networks as a Side channel," Location based services which employ data from Smartphone, vehicles etc are growing in popularity. To reduce the threat that shard location data poses to user's privacy some services anonymizes or obfuscate this data. We show these methods can be effectively defeated: a set of location traces can be deanonymized given an easily obtained social network graph. The key idea of our approach is that a user may be identified by those she meets: a contact graph identifying meetings between anonymizer users in a set of traces can be structurally correlated with a social network graph, thereby identifying anonymizer users. We demonstrate the effectiveness of our approach using three real world datasets: University of St Andrews mobility trace and social network, small Blue contact trace and facebook social network

SYSTEM MODULES AND PROBLEM STATEMENTS

A. Problem Statement

The problem in the Mobile users and LBS, consider a No of users move in an area split into a locations or regions. Each user can communicate with other by using wireless device. LBS contains data, this information will be expired, LBS does not having a longer valid information. LBS providing information is a self verifiable, users can verifying a LBS response by using public key. LBS server concentrate only location information queries from the users, it is not concentrate on attackers. So that time untrusted service providers can attack and get the information for that one adversary is present to observe the untrusted service providers. A centralized LBS can be a default observe all the queries of a user.

B. System Modules

The System contains five modules

1. Mobile Users
2. Location Based Server (LBS)
3. User Query
4. Check Authenticity
5. User Privacy

a. Mobile Users

In the mobile crowd there will be a N no of users will be using a mobile phones. So in the mobile crowd the users will be move into an area split into regions / locations. Each user has its own time. Consider a user u, this user is currently in the region ri, he has to visit next region rj is denoted by pu (rj|ri). Each user communication will taking place ad hoc device-to-device communication.

b. Location Based Server (LBS)

User is sending a request to the LBS. If the requested information is present in buffer it is sending responses to user, if it not available then it is sending a request to server and server sending a responses to LBS. Sometimes the data not available longer valid time.

c. User Query

User is sending request information is not available in buffer so that time it will broadcast her query to neighbors through wireless ad interface of the device. A user has a correct information about a region is called informed user. User interested getting information about a region is called information seekers.

d. Check Authenticity

The data providing LBS is self verifiable. User can verify the server Reponses. This can be done in different ways. Each response from LBS can be verified by using public key from server provides.

e. User Privacy

A subset of users in every region has to contact the LBS to get updated data and arrest of the users can make use it from neighbors through collaboration.

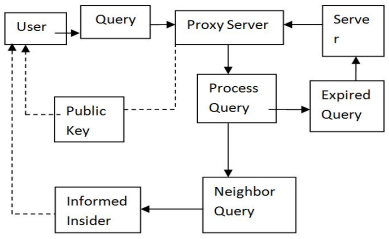

Fig 1: System Architecture

SYSTEM ARCHITECTURE

Compare to existing system the proposed system provides a good privacy for users. In the mobile crowd number of users will be present. Each user sending a query to proxy, the requested information present then it is sending responses to user, if it is not available then the request is sending to server. Server is sending responses to proxy and proxy sending a data to user. User can verify by using public key. Shows in fig1.

SYSTEM IMPLEMENTATION AND RESULT ANALYSIS

The system is implemented. Initially user is sending request to proxy, proxy the is checking with in his buffer. If the requested information is present sending data to a user. If it is not available proxy is sending a request to server and server sending a response to proxy and proxy is sending to user. The user will be checking with public key. The public key will be sent by LBS server. This much implantation is done. The result will be the main purpose here is to providing a privacy for the user and hiding user information from the server.

CONCLUSION

We have proposed a novel approach to enhance the privacy of LBS users, to be used against service providers who could extract information from their LBS queries and misuse it. We have developed and evaluated MobiCrowd, a scheme that enables LBS users to hide in the crowd and to reduce their exposure while they continue to receive the location context information they need. MobiCrowd achieves this by relying on the collaboration between users, who have the incentive and the capability to safeguard their privacy. We have proposed a novel analytical framework to quantify location privacy of our distributed protocol. We have demonstrated the resource efficiency of MobiCrowd by implementing it in portable devices.

REFERENCES

[1]. "Pleaserobme: http://www.pleaserobme.com."

[2]. J. Meyerowitz and R. Roy Choudhury, "Hiding stars with fireworks: location privacy through camouflage," in MobiCom '09: Proceedings of the 15th annual international conference on Mobile computing and networking, 2009.

[3]. F. Olumofin, P. K. Tysowski, I. Goldberg, and U. Hengartner, "Achieving efficient query privacy for location based services," in Privacy Enhancement Technologies (PETS), 2010.

[4]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in Proceedings of the ACM SIGMOD inter- national conference on Management of data, 2008.

[5]. R. Anderson and T. Moore, "Information Security Economics– and Beyond," Advances in Cryptology-CRYPTO, 2007.

[6]. R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A distortion-based metric for location privacy," in WPES '09: Proceedings of the 8th ACM workshop on Privacy in the electronic society. New York, NY, USA: ACM, 2009, pp. 21–30.

[7]. M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "A parsimonious model of mobile partitioned networks with clustering," in Proceedings of the First international conference on COMmunication Systems And NETworks, 2009.

[8]. R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2011.

