ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Preserving Location Privacy of User Participating in LBSs Through Collabaration



Sk.Shameen Taz
PG Scholar,
Department of CSE,
QUBA College of Engineering & Technology, Nellore, AP, India.

Syed Abdul Haq
Associate Professor & HOD,
Department of CSE,
QUBA College of Engineering & Technology, Nellore, AP, India.

Panidipati Babu
HOD & Dept of MCA,
Department of CSE,
QUBA College of Engineering & Technology, Nellore, AP, India.

Abstract:

Location-aware smart phones support various location-based services (LBSs): users query the LBS server and learn on the fly about their surroundings. However, such queries give away private information, enabling the LBS to track users. We address this problem by proposing a user-collaborative privacy-preserving approach for LBSs. Our solution does not require changing the LBS server architecture and does not assume third party servers; yet, it significantly improves users' location privacy. The gain stems from the collaboration of mobile devices: they keep their context information in a buffer and pass it to others seeking such information. Thus, a user remains hidden from the server, unless all the collaborative peers in the vicinity lack the sought information. We evaluate our scheme against the Bayesian localization attacks that allow for strong adversaries who can incorporate prior knowledge in their attacks. We develop a novel epidemic model to capture the, possibly time-dependent, dynamics of information propagation among users. Used in the Bayesian inference framework, this model helps analyze the effects of various parameters, such as users' querying rates and the lifetime of context information, on users' location privacy.

Keywords:

Mobile Networks, Location-based Services, Location Privacy, Bayesian Inference Attacks.

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. EXISTING SYSTEM :

Among other increasingly powerful mobile computing devices, offer various methods of localization. Integrated GPS receivers, or positioning services based on near by communication infrastructure.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

(Wi-Fi access points or base stations of cellular networks), enable users to position themselves fairly accurately, which has led to a wide offering of Location-based Services (LBSs). Such services can be queried by users to provide real-time information related to the current position and surroundings of the device, e.g., contextual data about points of interest such as petrol stations, or more dynamic information such as traffic conditions. The value of LBSs is in their ability to obtain on the fly up-to-date information. Although LBSs are convenient, disclosing location information can be dangerous. Each time an LBS query is submitted, private information is revealed. Users can be linked to their locations, and multiple pieces of such information can be linked together. They can then be profiled, which leads to unsolicited targeted advertisements or price discrimination.

2.1 ARCHITECTURE OF EXISTING SYSTEM:

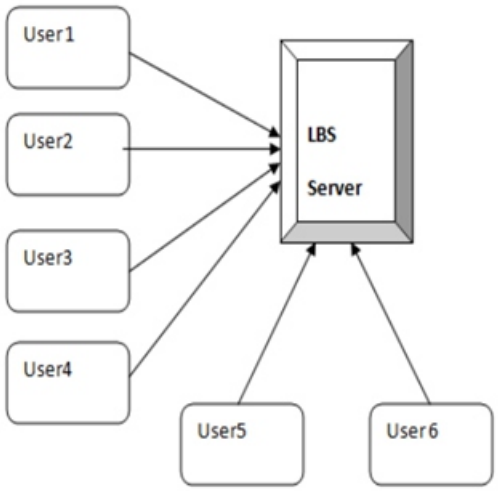

Fig -1: Architecture of the existing system

DISADVANTAGES OF EXISTING SYSTEM:

•Can be inferred from a user's whereabouts. This could make user the target of blackmail or harassment.

•A stalker can also exploit the location information.

•Misuse their rich data by, e.g., selling it to advertisers or to private investigators.

3. PROPOSED SYSTEM:

We propose a novel location-privacy preserving mechanism for LBSs. To take advantage of the high effectiveness of hiding user queries from the server, which minimizes the exposed information about the users' location to the server, we propose a mechanism in which a user can hide in the mobile crowd while using the service. The rationale behind our scheme is that users who already have some location-specific information (originally given by the service provider) can pass it to other users who are seeking such information. They can do so in a wireless peer-to-peer manner. Simply put, information about a location can "remain" around the location it relates to and change hands several times before it expires. Our proposed collaborative scheme enables many users to get such location-specific information from each other without contacting the server, hence minimizing the disclosure of their location information to the adversary.

3.1.PROPOSED SYSTEM ARCHITECTURE:

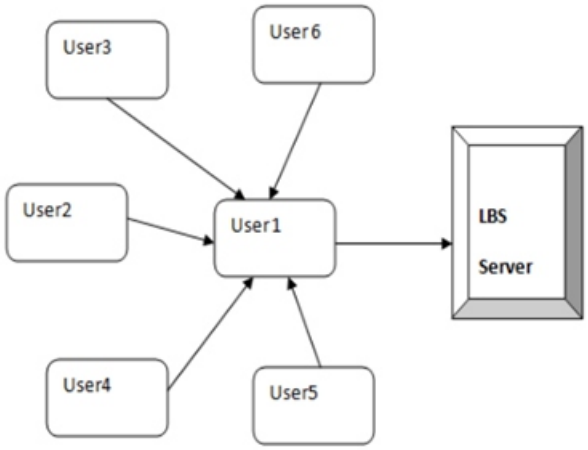

Fig-2: Architecture of Proposed system

ADVANTAGES OF PROPOSED SYSTEM:

•The System is attached to the information and protected with the digital signature.

•Malicious users cannot mislead others into receiving fake information, because messages are digitally signed by the LBS.

•A user's query becomes hidden from the server due to MobiCrowd protocol.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4. IMPLEMENTATION OF PROPOSED SYSTEM:

The framework of our proposed system has the accompanying modules alongside the following prerequisites.

» Mobile Users

» Location Based Server (LBS)

» User Query

» Check authenticity

» User privacy

MOBILE USERS:

Consider N users who move in an area split into M discrete regions/locations. The mobility of each user u is a discrete-time Markov chain on the set of regions: The probability that user u, currently in region ri, will next visit region rj is denoted by pu(rj |ri). Let πu(ri) be the probability that user u is in region ri. Each user possesses a location-aware wireless device, capable of ad hoc device-to-device communication and of connecting to the wireless infrastructure (e.g., cellular and Wi-Fi networks).

LOCATION BASED SERVER (LBS):

As users move between regions, they leverage the infrastructure to submit local-search queries to LBS. The information that the LBS provides expires periodically, in the sense that it is no longer valid. Note that information expiration is not equivalent to the user accessing the LBS: A user accesses the LBS when her information has expired and she wishes to receive the most up-to-date version of it.

USER QUERY:

A seeker, essentially a user who does not have the sought information in her buffer, first broadcasts her query to her neighbors through the wireless ad hoc interface of the device. This a local query. Each user with valid information about a region is termed informed user for that region. Users interested in getting location-specific information about a region are called information seekers of that region.

CHECK AUTHENTICITY:

The information the LBS provides is self-verifiable, i.e., users can verify the integrity and authenticity of the server responses. This can be done in different ways; in our system, the user device verifies a digital signature of the LBS on each reply by using the LBS provider's public key As a result, a compromised access point or mobile device cannot degrade the experience of users by altering replies or disseminating expired information.

USER PRIVACY:

In essence, a subset of users in every region has to contact the LBS to get the updated information, and the rest of the users benefit from the peer-to-peer collaboration. Intuitively, the higher the proportion of hidden user queries, the higher her location privacy.

5. 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 Mobi Crowd, 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. Mobi Crowd 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. Our epidemic model captures the hiding probability for user locations, i.e., the fraction of times when, due to MobiCrowd, the adversary does not observe user queries. By relying on this model, our Bayesian inference attack estimates the location of users when they hide.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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 LBSMobile 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.