ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Location Privacy Context Information Effects Using Bayesian Inference Framework

B.Ram Kumar, S. Kripa Sankar, Prof.K.Ravikumar

Post Graduate Student, Department of CSE, Rrase College of Engineering, Chennai, India

Assistant Professor, Dept of C.S.E Rrase College of Engineering Chennai, India

Professor, Department of CSE, Rrase College of Engineering, Chennai, India

ABSTRACT -. Smartphones, among other increasingly powerful mobile computing devices, offer various methods of localization. Integrated GPS receivers, or positioning services based on nearby communication infrastructure (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. Even worse, the habits, personal and private preferences, religious beliefs, and political affiliations, for example, can be inferred from a user's whereabouts. This could make her the target of blackmail or harassment. Finally, real-time location disclosure leaves a person vulnerable to absence disclosure attacks: learning that someone is away from home could enable someone to break into her house or blackmail her [1]. An stalker can also exploit the location information.

KEYWORDS: Mobile Networks, Epidemic Models, Location Privacy, Location based services, Mobile networks

I. INTRODUCTION

Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers. Initially developed by Android, Inc., which Google backed financially and later bought in 2005, Android was unveiled in 2007 along with the founding of the Open Handset Alliance: a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. The first Android-powered phone was sold in October 2008. Android is open source and Google releases the code under the Apache License. This open source code and permissive licensing allows the software to be freely modified and distributed by device manufacturers, wireless carriers and enthusiast developers. Additionally, Android has a large community of developers writing applications ("apps") that extend the functionality of devices, written primarily in a customized version of the Java programming language. In October 2012, there were approximately 700,000 apps available for Android, and the estimated number of applications downloaded from Google Play, Android's primary app store, was 25 billion.

These factors have allowed Android to become the world's most widely used smart phone platform, overtaking Symbian in the fourth quarter of 2010, and the software of choice for technology companies who require a low-cost, customizable, lightweight operating system for high tech devices without developing one from scratch. As a result, despite being primarily designed for phones and tablets, it has seen additional applications on televisions, games consoles, digital cameras and other electronics. Android's open nature has further encouraged a large community of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

developers and enthusiasts to use the open source code as a foundation for community-driven projects, which add new features for advanced users or bring Android to devices which were officially released running other operating systems.

Android had a worldwide smart phone market share of 75% during the third quarter of 2012, with 500 million devices activated in total and 1.3 million activations per day. The operating system's success has made it a target for patent litigation as part of the so-called "smart phone wars" between technology companies.

II. RELATED WORK

To enhance privacy for LBS users two methods are used in existing centralized and user-centric.

Centralized approaches introduce a third party in the system, which protects users' privacy by operating between the user and the LBS. Such an intermediary proxy server could anonymize (and obfuscate) queries by removing any information that identifies the user or her device. Alternatively, it could blend a user's query with those of other users, so that the LBS server always sees a group of queries.M However, such approaches only shift the problem: the threat of an untrustworthy LBS server is addressed by the introduction of a new third-party server. Additionally, new proxy servers become as attractive for attackers as centralized LBSs.

User-centric approaches operate on the device. Typically they aim to blur the location information by, for example, having the user's smartphone submit inaccurate, noisy GPS coordinates to the LBS server. However, obfuscation approaches that protect user location-privacy can degrade the user experience if users need high privacy, e.g., LBS responses would be inaccurate or untimely. Obfuscation also is not effective against absence disclosure.

III. PROPOSED ALGORITHM

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.

1.Android mobile user registration: In the Location base query system we have to register the user for his future query search. Without registering a user can't access the clocking agent. For registering the user should give his details such as his name, address, age, sex, ext., Once a user register his details he can get useful information from the clocking server. Each user will identify by a unique username and password. If the Registrar decides to seek advice from a Registration Panel on your application we may need you to send us further information and documents (for example, references from your employing authorities and/or supervising consultants). We will write to you to let you know if this is the case. If you register, do not forget your password or your user name. If you are prone to forgetting these, make sure you enter your email address as part of signing up, so you can have a new password sent to you if you forget your current one. You won't be able to (easily) change your username once you choose it, so reading the username policy before creating a username is highly recommended.

2.User authentication and query process:

If a client want to arise a query first he should be authenticated by the server for this he have to login by his user name and password after he got sign-in he can arise query to the server. This query will go the clocking agent and the clocking agent will send the query to the Cloud server. Most applications need to know the identity of a user. Knowing a user's identity allows an app to provide a customized experience and grant them permissions to access their data. The process of proving a user's identity is called authentication. Once a user authenticates to your app, Gps manages their session, ensuring that the user is remembered across page refreshes and app restarts. query processing is to find information in one or more databases and deliver it to the user quickly and efficiently. Traditional techniques work well for databases with standard, single-site relational structures, but databases containing more complex and diverse types of data demand new query processing and optimization techniques.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

3.User location Identification:

The clocking agent will get user location and then it will find the user is moving towards the location or moving outwards the location. The current location is obtained using GPS from the mobile user. The mobile user will carry with the GPS for getting the longitude & latitude values. These values are obtained via satellite communication. So once the user sends the query to the Cloaking Agent, the Cloaking agent will get the exact location of the user via GPS values of the user. we inferring the home location of Gps users at different granularities, including city, state, time zone or geographic region, using the content of users location and their behavior. Mobile phone tracking refers to the ascertaining of the current position of a mobile phone, stationary or moving. Localization may occur either via multilateration of radio signals between (several) radio towers of the network and the phone, or simply via GPS. To locate the phone using multilateration of radio signals, it must emit at least the roaming signal to contact the next nearby antenna tower, but the process does not require an active call. GSM is based on the signal strength to nearby antenna masts.

4.Safe region Manipulation:

Whenever a clocking agent receives a query from the client it will check the query and find the safe region for the client. Safe region is calculated from the exact user location. First we have to fetch the direction of the user. If the direction of the user is towards forward then the cloaking agent will calculate the safe region with respect to the main location. For example user sends a request from Habibullah Road, user is moving towards T.Nagar, then the Safe region T.Nagar, if the user is moving in the opposite direction then the cloaking agent will specify the safe region as Nungambakkam.. After find safe region the clocking agent will send the request to the Cloud server. The Cloud server will send the result for the safe region the clocking agent receives the result from the Cloud server and then it find the nearest Location from the result and send the location to the client.

5.Query Request to the Cloud server:

The Clocking agent Manipulate the Safe region for the client and the send the query to the Cloud server. The Cloud server checks the Query and Retrieve the results according to the safe region and then send the result to the clocking agent. If the user is requested for ATM Bank from Habibullah Road, first the query is sent to the Cloaking Agent. Cloaking agent will manipulate the safe region as T.Nagar, then the query is forwarded to the Cloud Server. Query strings are also generated by sending a form or by a user typing a query into the ipaddress of the Location monitoring device. A query string is the part of a uniform resource locator (URL) containing data that does not fit conveniently into a hierarchical path structure. The query string commonly includes fields added to a base URI by a Web browser or other client application, for example as part of an HTML form.

6.Retrieve of results in according to safe region and ontology:

Clocking agent will send the query to the Cloud server. The Cloud server manipulates the user query and it will send the results to the clocking server based on the Area and Ontology. The main Cloud will retrieve the results with respect to the nearest place of the user as well as the Ontology Process. Ontology is the study of relativities. Using Ontology Cloud Server can get relevant information's and that information is also retrieved back to the user. If the query for Bank from the T,nagar as safe Region, then the Cloud Server will find the nearest bank as well as the relative ATM with respect to T.nagar.

7.Find the Nearest Location:

After getting the query result from the Cloud server, the clocking server will filter the results in accordance to the user exact location. The Cloud server will retrieve the bank information or ATM whichever is nearest to the user in accordance to T. Nagar to the cloaking agent. But the cloaking agent knows user is in Habibullah Road. So the cloaking agent will apply KNN Query Algorithm to fetch the nearest ATM or bank in accordance to Habibullah Road. So user will be receiving the exact information, as requested but then the user's Location Privacy is still maintained, because the Cloud server will update in its table as the query is from T.Nagar not from Habibullah Road. By this way we ensure Privacy in the user's location.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

K-means Clustering & M-Privacy

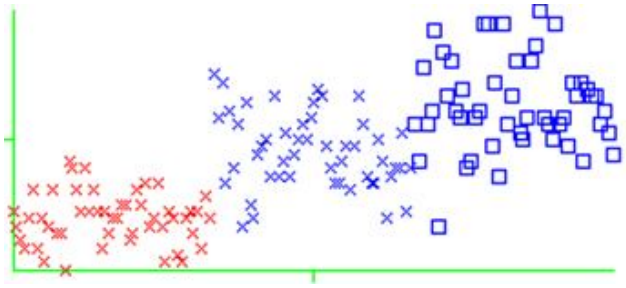

Fig 3.K-means Clustering

K-means algorithm is regarded as a staple of clustering methods due to its ease of implementation. It works well for many practical problems, particularly when the resulting clusters are compact and hyperspherical in shape. Here, this algorithm clusters the data record based on the attribute disease. For an example, the heart specialist doctor can access the patient record that is suffered by heart diseases and need not to view all other records which is a time consuming process. Hence the clustering process reduces the response time. So, K-means is a good selection for clustering largescale data sets. Moreover, several methods have been proposed to speed up K – means clustering.

IV. PSEUDO CODE

$$\lambda i = \sum u, j \neq i \pi u(ri) pu(rj|ri)$$

$$\sum u\ \pi u(ri)$$

Where λ= Probablity of exiting the region within a time unit.
∑= average collobaration probability.

Let λi be the entering and exiting the region ri respectively. They correspond to the expected number of users who are inside and outside of ri, normalized by the expected number of users who are inside and outside of ri.

The Contact rate βi used between users in the regions ri corresponds to the expected number of a device within its communication range.

Once they have it, they move into the Informed state. As long as a seeker user stays in the region that she seeks information about, she is called an insider seeker. These users can receive information from other Informed users in the region, or from the server, the ultimate source of information. A seeker who leaves the region after requesting information about that region is called an outsider seeker. An Outsider Seeker can only receive information from the server, as users need to be in the same region in order to be able to propagate information to each other.

V. SIMULATION RESULTS

The simulation studies involve user has to give the query for the further propose and to obtain the optimized query. Here we consider the static tables and data's. The table names and attributes are emp, dept, acnt, bank and the attributes of emp is name, age , sal, dno then dept table attributes are dno, dname, floor, budget, mgr, ano then acnt tables contains the following attributes are ano, type, balance, bno then bank table contains the following attributes are bno, bname, address. In this module, have to rewrite the user given query into the representation format based on the selection, project and joint. Based on this rewrites query only have to prepare the execution plans.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Based on the query request given from the mobile phone it searches from the nearest location and filters the result based on the location based services and provides the data to the user in an efficient manner.

VI. CONCLUSION AND FUTURE WORK

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. 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. Our extensive joint epidemic/ Bayesian analysis shows a significant improvement thanks to MobiCrowd, across both the individual and the average mobility prior knowledge scenarios for the adversary. We have demonstrated the resource efficiency of MobiCrowd by implementing it in portable devices.

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. Anderson and T. Moore, "Information Security Economics— and Beyond," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology, 2007.
[6] 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.
[7] 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.
[8] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying Location Privacy," Proc. IEEE Symp. Security and Privacy, 2011.
[9] J. Krumm, "A Survey of Computational Location Privacy," Personal Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.
[10] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A Unified Framework for Location Privacy," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (HotPETs), 2010.

BIOGRAPHY

Ramkumar is a post graduate student in the department of computer science engineering, Rrase College of Engineering, Anna University. He received Bachelor of Engineering degree (B.E) in 2011 from Anna University, Chennai, India. His research interests are Andriod Technology using Java, Algorithms, Database Management System, etc.