Forecasting the Relevant user Future Location and Reduction of Searching Time by Unscented Kalman Filter

Sathya.S[1] Vinitha Subashini.B[2]
[1]M.E. Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Akshaya College of Engineering and Technology Coimbatore, India

Abstract— With the help of the GPS the user can Location based service helps the user to know about their surroundings when the user query the request for a particular location to the LBS server. Based on the user query rates per unit time and the lifetime of the context information the user are not observed by the server. But when the life time of the user request to the server side increases the users are easily tracked by the server. The user confidentiality can be increased by using Unscented Kalman Filter algorithm. By this algorithm the required data which is needed for the user will be displayed at the top. First the user has to send the required location as a query to the LBS server. The server in turn matches the user queries with the cloud database to verify whether the authorized user has entered the query. The Unscented Kalman Filter algorithm will display the required details which are provided to the user at the top. Hence the user can get the required details immediately. Thereby the frequent request by the user will be avoided.

Key words: Mobile networks, location-based services, location privacy, Kalman Filter

I. INTRODUCTION

In long-established cellular networks, users can share their location with the help of network operator in order to obtain accent and data services which are provided by the large data service on the network. With the appearance of data services, users can increasingly share their location with other user such as location-based Services (LBSs). Particularly, users first obtain their location by relying on the localization potential of their mobile device share it with LBSs and then obtain adapted services based on their location. Yet, unlike cellular operators, LBSs are mainly provided for free and produce proceeds with location-based classified ad. Hence, there is a mean difference between the production models of LBS providers and cellular operators: LBS providers aim at profiling their users in order to serve made to order advertisement. Subscribers of cellular networks know that their special data is contractually protected.

On the reverse, users of LBSs often be short of understanding of the privacy implications caused by the use of LBSs [8]. Some users shield their confidentiality by hiding at the rear of Pseudonyms (by giving the false information) that are mostly invariant over time. Fundamentally, these mechanisms rely on trusted third-party servers that anonymize requests to LBSs. On the other hand, such privacy-preserving mechanisms are not commonly obtainable and users keep on sharing their location information unprotected with the third-parties.

Yet, with most LBSs, users do not share their location frequently but as an substitute, connect to LBSs depending on their needs and thus reveal a few location samples of their entire course. For example, a generalized search on Google Maps [7] only reveals a location illustration by physically connecting to the service. Depending on the provided service, LBSs collect location samples concerning their users. For example, a typical service (such as Google Maps, Facebook, or Twitter) offers users to connect with their friends, to identify their surroundings or to optimize their mobility. Depending on their needs, users can access such LBSs at unusual times and from different locations, thus revealing several location samples. In specific, users of these services do not constantly share their locations with the other user. As an alternative, users have to physically decide when to share their location with the other mobile devices. We classify most all the rage LBSs into three broad categories and explain the information shared by users in each case.

A. Localization Search:

Many LBSs allows the user to search for local services around a detailed location (e.g., localization with the help of Google Search [7]). Localization searches offer mobile subscribers spontaneous access to close at hand services. Hence, a user location will acts as a spatial query to the LBS. For example, users can obtain the position of nearby businesses, products, hospital, restaurants, colleges movie theaters or other local information depending on the type of information provided by the LBS. Such localized searches help users find the way to unfamiliar regions and determine unknown places. Thus, users episodically connect to LBSs, informative samples of their mobility. LBSs obtain arithmetical information about the visited locations of mobile users and learn popular locations and can learn different user habits. Yet, LBSs do not learn the real movement of mobile users (e.g., the name of the visited restaurant, hospital, theater) as they do not know the resolution of the user about the provided information.

B. Street Directions:

Another popular use of the LBSs is in finding a route between two different locations. Typically, a user can share their location with LBS and request for the shortest route to a different location (e.g., Google Maps). Users of such services usually expose their current location and a possible destination. Hence, the users may reveal their home/work locations to LBSs in adding up to samples of their movement. This enables LBSs to obtain arithmetic information about the chosen origins and destinations of mobile users whereabouts.

C. Location Check-Ins:

A new type of location-based service offers users to check-in to particular places in return of the information related to the visited location [13]. For example, it can be used to check into college, restaurants or museums. It can allow the users to meet with the other users that can share similar

All rights reserved by *www.ijsrd.com*

interests and to discover new aspects of their city with the help of recommendations [9]. With that such services, users not only accurately reveal their location (GPS coordinates), but also their location and the need of the intention. Indeed, the LBS can learn the current movement of its users. Users can check-in to communal places, but also private homes.

The main problem on getting an on-site on demand high-class information is the loss of user's privacy: Each time when LBS query is submitted to the server by the user, private information of the user exposed. The user can be connected to their location with the help of the GPS, and several pieces of such information can be connected together with the help of the LBS. Thus the present location of users becomes possible to the server. When the user wants to obtain additional information as much as possible about the LBS, the server, which is mainly used for distribution the necessary information, the service provider will track the user using a variety of techniques over time.

Clearly, the user could receive the LBS benefits; e.g., the user could download a very huge amount of data capacity and then search nearby about specific framework information which is required for them. But this would be awkward and it would be ineffective when obtaining the information that change regularly over time. For example, if the service provider ask the users contact information, when the user is connected to the GPS.

However, even if the user does not give any details concerning them to the server or even if the server does not recognize the information of the user who are linked with the GPS for obtaining the details of the present location, the server will trace the user by tracing their IP address or their location[13], and then trace the user whereabouts. Certainly, the LBS operators mainly targeted to use incorrectly the secret information of the user and collect the details of the user, as contrasting to cellular operators (who have a agreement with their users), share the data with third party company that offer, the under assail advertisements, who smash into the LBS servers and obtain logs of user queries.

Moreover, whether the user is accepted or not, or introduction too much trust in the LBS source by the user which is redundant. Tracking the user over time and position, and then identifying the user, implies not only thrashing of confidentiality of data and information for the user but probably other desire consequences such as lack of disclosure: learning that the user is exterior and away from their home could allow the untrusted party to break the house or could blackmail them [3]. The outcome in all cases is the same: users secret and sensitive data will fall in the hands of untrusted parties.

One of the approaches to avoid the problem of tracking the user could be to blur the user present location information, e.g., by having the user's smart phone (or the privacy alternative) they can present incorrect samples to the LBS server. As a result, the need to improve privacy for LBS users has been understood and several solutions have to been recognized and should be planned. Moreover, obfuscation cannot be efficient against absence of correct data of the present location and confession [9]. However, obfuscation approaches (e.g., spatial/temporal cloaking introduced in [15]) which can shield the users up to date location-privacy, corrupt the user request data which is required for them to discover the location which is unfamiliar to them, if users need high privacy: e.g., LBS responses for the request which is reorganized by the user would be incorrect or untimely.

Another approach for protecting the privacy of the user in opposition to the untrusted party could be introducing a trusted third party in the system, acting as an intermediary linking the user and the LBS: its main role is to protect the users' confidentiality. Such an intermediary alternative server, between the user and the LBS, could anonymize and obfuscate queries by eliminating any information that identifies the users device [13], [14] that is the information which is reorganized by the user to the LBS server.

However, such approaches only change the problem: the threat of not to be trusted LBS server is by trusting or by the introduction of a new third-party server. Or it could mix together or group one's query information with those of other users query, so that the LBS server always sees a group of queries request at the same time and could response the user with that of incorrect or one user's information to other user leading the user's to be get confused [11].

Many other approaches has been considered necessary or essential to change the operation and the functioning of the LBS, for example camouflaging method can be used in which some dummy queries can be added (submitting the user query in dissimilar form than actual queries of the user),or that these user's query can be stored in a different way (e.g., encrypted or programmed, to allow private contact [10]). This increases the misunderstanding in paths of dissimilar users [2]. altering pseudonyms of each user while passing through pre-defined spots known as mixed zones[12], becomes complex for tracking the user next to their trajectory path.

Any such centralized intervention or any considerable changes to the LBS operation would be hard to implement, simply because the LBS providers would have little encouragement to essentially change their operation. Perturbation algorithm is functional in cross paths where at least two user will meet together. However quiet must be made by the user along this mixed zone, which means that LBS cannot be used by the user. In order to conquer this problem, the mixed zone dimension 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 zone are optically placed, the success of opposition is relatively high[13]. In addition, new proxy servers become as good-looking for attackers as a centralized LBSs when the query has been submitted. Skewed incentives have been recognized as the root cause of many safety measures problems in the mobile crowd[6]. In order to present and to improve the location privacy of LBS users without any of the above-mentioned boundaries, an suggest method has been in this method with a user-centric method. Hence, the deficient of incentives and guarantees for shielding the users' locality information, make these approaches infeasible in perform.

The solution to the above problem has been solved by introducing a new scheme, called unscented Kalman Filter algorithm for protecting the privacy of the user against the attack of the other untrusted party and also by the server. In order to preserve the privacy, mobile user are concerned

All rights reserved by *www.ijsrd.com*

with their location confidentiality which are indeed with the most motivated entities by engaged in shielding themselves. This approach does not involve any change in the LBS server architecture and its common operation; it makes no assumption on the trustworthiness of the LBS or any other third-party.

In the proposed work the safety measures to the user's private information has been provided. The server in turn finds the position of the user with the help of the latitude and the longitude value. In the unscented Kalman filter algorithm when the user enter the query for the new position with the help of the GPS in the mobile to the LBS server. All these data should be uploaded before in the server database. This latitude and the longitude value will be provided for each location. At the similar time the network traffic on the server side will been reduced with the help of this planned method since a lot of user will access the server at the same time. These data will be stored on the server and these data will be managed and be protected by particular server or organization. Only then the user's query request can be provided by the server.

II. RELATED WORK

There are a lot of related schemes for the mobile network. Queries can be submitted in dissimilar query form from real queries, probably by encryption technique using private information retrieval PIR[3], or data can be stored in a different way(eg., encryption or encoded method to allow private access[4]).

Many techniques has been proposed to shield location privacy in LBSs can be classify based on how they alter the users' queries before they enter at the LBS server. The server will ask the user contact details to provide the information but the unusual and full detail should not be provided. The user query can be *anonymized* (by eliminate user's identities) unique details of the user should not be submitted.

Another method is by providing the *pseudonym* (by replacing users' actual names with sequential identifiers called pseudonyms), or they can used by *obfuscation* (by generalizing or perturbing the spatial secular information connected to the queries). The user queries can be anonymized (by removing user's identities) unique details of the user should not be submitted. Combinations of these methods have been engaged in the presented (centralized or distributed) mechanisms. The user queries can be anonymized (by eliminating user's identities) unique details of the user should not be submitted. While changing the user pseudonyms while the users are passing through pre-defined spots, called mix zones [7], makes it complex to track the users along their trajectories.

The mere anonymization of (especially the permanent queries from the user side) queries does not shield users' location privacy: the queries of a user are connected in time and location, hence, the opponent can successfully link them by using target tracking algorithms [7] or identify the real names of the users [13], [11]. Thus, the unlinkability of users' queries is limited and the adversary's success is relatively high, even if the mix zones are optimally placed [12]. Perturbing the query's with spatial temporal information, in adding to anonymization by the trusted third party (fundamental anonymity server), is proposed for obtaining a superior level of privacy [13], [14]. However, such users must remain quiet inside the mix zones, so that they cannot use the LBS server, but the size of the mix zones should be kept small in order to let users promote from the LBS.

The main drawback on a centralized third party that limits the practicality. For example, the queries sent to the anonymity server [13] have to be waited until sufficient anonymization has been achieved for a cluster of users. Finally, most of the obfuscation based techniques shown insufficient to protect location privacy [11], [14] which are based on k-anonymity. Similarly in [8], the need for constructing the cloaking regions and also to accept the responses from the server through other users can significantly will disgrace the service.

But while generating valuable replica queries for diverting the adversary is a tricky task [9], since they need to look like actual queries over time and location. Adding tailor's dummy queries to the user real queries might help to confound the adversary of the server about the definite user location. In all the above-mentioned mechanisms, there is always a exchange between user's confidential information and the superiority of service which they experience. However, such users must remain quiet inside the mix zones, so that they cannot use the LBS server, but the size of the mix zones should be kept small in order to let users promote from the LBS.

The stress gets maximized when hiding queries from the LBS server. Hiding the user query from the LBS server minimizes the exposed user information, hence, maximizes user privacy with respect to that of query.

III. PROBLEM STATEMENT

While considering location-aware wireless network devices, which is capable of ad hoc device-to-device communication and by connecting to the wireless infrastructure (e.g., cellular and Wi-Fi networks). The server in turn replies to the equivalent user, on condition that the latest requested context information around the submitted location. Users in attendance *queries* for their contemporary location, and the type of information which is required for them (context, point of interest, etc) they are interested in. Depending on the type of requested information the occurrence of the users LBS queries varies, the dynamics of information updated in the LBS database, or the environmental region.

Based on the observed queries the Inference attacks are classified into two

The two Categories are

1) Tracking
2) Identification attacks

In tracking mechanism the user are easily identified by the untrusted party when the user send the query to the server. The tracking will be done with the help of the IP address which is provided to each mobile number.

In the identification mechanism the user are easily know by the unknown user when they share the data to the others with help of Bluetooth and other application device which is available in the mobile. Hence all the information and the private data will be tracked and can misuse the data.

Two types of location-privacy are

- Presence of disclosure of attack
- Absence of disclosure of attack

All rights reserved by *www.ijsrd.com*

The extra queries provided by the user to the server the opponent observe, the superior its location inference attack success will be. Smaller amount information about the user current locations makes it difficult for the adversary to track the actual trajectories of the user and to identify their real names. This is why protection mechanisms try to reduce the adversary's information.

A. Design Objective:

Hence with the help of Unscented Kalman Filter the required data from the given server details can be displayed at the top which is needed for the user. Therefore the user can view the result immediately and can go to the required location.

IV. ACKNOWLEDGEMENT

The success of a work depends on the team and its cooperation. I take this opportunity to express my gratitude and sincere thanks to everyone who helped me in my project. First and foremost, I would like to thank the Management for the Excellent Infrastructure, facilities and the constant support provided for the successful completion of the project work.

I thank Associate Professor Mr P.Dhamodharan M.E., (Ph.D), Head of the Department, Computer Science and Engineering, for his valuable guidance, continuous support and suggestions to improve the quality of the project work. I express my special thanks to my guide, Associate Professor, Ms B. Vinitha Subashini Assistant Professor for her valuable guidance, insightful comments and continuous support to carry out the project work.

I express my deep sense of gratitude to all the Faculty members and supporting staff for their continuous support in completing this project work successfully. My sincere thanks to my family members and friends for their support and motivation to carry out this project successfully

REFERENCE

[1] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the Privacy Risk of Location-Based Services," Proc. Fifth Int'l Conf. Financial Cryptography and Data Security (FC '11), pp. 31-46, 2012.

[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.

[11] 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.

[12] R. Shokri, P. Papadimitratos, and J.-P. Hubaux, "Mobicrowd: A Collaborative Location Privacy Preserving LBS Mobile Proxy (Demonstration)," Proc. Eighth ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2010.

[13] "NIC": Nokia Instant Community," com/2010/05/25/nokia-instant-community-gets-you-social/.

[14] "Wi-Fi Direct", http://www.wi-fi.org/wi-fi_direct.php, 2013.

All rights reserved by *www.ijsrd.com*