Prediction of user Future Location by Extended Kalman Filter

Sathya. S [1]
M.E – CSE
Akshaya College of Engineering and Technology
Coimbatore, India

Vinitha Subashini. B[2]
Assistant Professor/Department of CSE
Akshaya College of Engineering and Technology
Coimbatore, India

***Abstract:* - 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. In user-collaborative privacy-preserving algorithm, 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 collaboration decreases the users are easily tracked by the server. The user privacy can be increased by using extended Kalman Filter algorithm. Kalman Filters are a form of predictor-corrector algorithm. By Kalman Filter algorithm hiding probability decreases with the prediction of user's future location. When the user sends the query the algorithm finds all the possibility way the user moves from his current position. The details of all the direction has been gathered and will be provided to the user. Thereby the frequent request by the user will be avoided and hence it is difficult for the server to trace the user. When there is no collaboration the request rate will be high but the user's information lifetime will be less on the server side in the Kalman Filter than the Privacy Preserving. The privacy of the user can be increased and the network traffic can also be decreased on the server side.**

Index Terms—Mobile networks, location-based services, location privacy, kalman Filter.

1. INTRODUCTION

Smart phones, which are an powerful increasing mobile computing devices, offer various methods of localization. Based on the nearby communication infrastructure integrated GPS receivers users are allowed to position themselves fairly and accurately. This provides a rise to an wide range of *Location-Based Services* (LBSs): to obtain the relevant information to the current location and surroundings users can query an LBS server, that is contextual data about specific points of interest. The purpose of LBSs is in obtaining exactly and accurate up to date information on the fly. The main problem on getting an on-site on demand high-quality information is the loss of user's privacy: Each time when LBS query is submitted to the server, private information is of the user revealed. The user can be linked to their location with the help of the GPS, and multiple pieces of such information can be linked together with the help of the LBS. Thus the current location of users becomes possible to the server. Clearly, the user could earn the LBS benefits; e.g., the user could download a very large amount of data volume and then search locally about specific context information which is required for them. But this would be cumbersome and it would be inefficient when obtaining the information that change frequently over time. When the user wants to obtain more information as much as possible about the LBS, the server, which is mainly used for sending the required information, the service provider will track the user using various techniques 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 provide any details about them to the server or even if the server does not identify the details of the user who are connected with the GPS for obtaining the details of the current location, the server will trace the user by tracing their IP addresses or their location[13], and then trace their whereabouts. Moreover, whether the user is identified or not, or placing too much trust in the LBS provider by the user which is undesirable. Indeed, the LBS operators mainly targeted to misuse the private information of the user and gather the details of the user, as opposed to cellular operators (who have a contract with their users), share the data with third party companies that offer, the targeted advertisements, who break into the LBS servers and obtain logs of user queries. The result in all cases is the same: users private and sensitive data will fall in the hands of untrusted parties. Tracking the user over time and location, and then identifying the user, implies not only loss of privacy of data and information for the user but possibly other dire consequences such as absence disclosure: learning that the user is outside and away from their home could allow the untrusted party to break the house or could blackmail them [3].

As a result, the need to enhance privacy for LBS users has been understood and several solutions have to been identified and should be proposed. One of the approach to avoid the problem of tracking the user could be to blur the user current location information, e.g., by having the user's smart phone (or the privacy proxy) they can submit inaccurate samples to the LBS server. However, obfuscation approaches (e.g., spatial/temporal cloaking introduced in [16]) which can protect the users current location-privacy, degrade the user request data which is needed for them to identify the location which is unknown to them, if users need high privacy: e.g., LBS responses for the request which is updated by the user would be inaccurate or untimely. Moreover, obfuscation cannot be effective against absence of accurate data of the current location and disclosure [9].

Another approach for protecting the privacy of the user against the untrusted party could be introducing a trusted third party in the system, acting as an intermediate between the user and the LBS: its main role is to protect the users' privacy. Such an intermediary proxy server, between the user and the LBS, could anonymize (and obfuscate) queries by removing any information that identifies the user or her device [13], [15] that is the information which is updated by the user to the LBS server. Or it could blend 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 wrong or one user's information to other user leading the user's to be get confused [14]. However, such approaches only shift the problem: the threat of an untrustworthy LBS server is by trusting or by the introduction of a new third-party server.

Many other approaches has been needed or required to changed 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 different form than actual queries of the user),or that these user's query can be stored differently (e.g., encrypted or encoded, to allow private access [14]). Any such centralized intervention or any substantial changes to the LBS operation would be hard to adopt, simply because the LBS providers would have little incentive to fundamentally change their operation. Perturbation algorithm is applied in cross paths where at least two user will meet together. This increases the confusion in paths of different users[2]. Changing pseudonyms of each user while passing through pre-defined spots known as mixed zones[12], 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 zone are optically placed, the success of adversary is relatively high[13]. Misaligned incentives have been identified as the root cause of many security problems in the mobile crowd[6]. Additionally, new proxy servers become as attractive for attackers as centralized LBSs when the query has been submitted. Hence, the lack of incentives and guarantees for protecting the users' location information, make these approaches infeasible in practice. In order to provide and to enhance the location privacy of LBS users without any of the above-mentioned limitations, an propose method has been in this method with a user-centric scheme. In order to protect the privacy, mobile user are concerned with their location privacy which are indeed with the most motivated entities by engaged in protecting themselves. The solution to the above problem has been solved by introducing a new scheme, called Extended Kalman Filter algorithm for protecting the privacy of the user against the attack of the other untrusted party and also by the server. This approach does not require any change in the LBS server architecture and its normal operation, it makes no assumption on the trustworthiness of the LBS or any other third-party.

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

2. RELATED WORK

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

Many techniques has been proposed to protect location privacy in LBSs can be classified based on how they distort the users' queries before they arrive at the LBS server. The user queries can be *anonymized* (by removing user's identities) original details of the user should not be submitted. The server will ask the user contact details to provide the information but the original and full detail should not be provided. Another method is by providing the *pseudonym* (by replacing users' real names with temporal identifiers called pseudonyms), or they can used by *obfuscation* (by generalizing or perturbing the spatial temporal information associated to the queries). They can also be camouflaged by adding some dummy queries with the original queries which has been send to the server, or be completely eliminating the full original query and be hidden from the LBS [13].

Combinations of these methods have been employed in the existing (centralized or distributed) mechanisms. The mere anonymization of (especially the continuous queries from the user side) queries does not protect users' location privacy: the queries of a user are correlated in time and location, hence, the adversary can successfully link them by using target tracking algorithms [7] or identify the real names of the users [15], [11]. While changing the user pseudonyms while the users are passing through pre-defined spots, called mix zones [7], makes it difficult to track the users along their trajectories. However, such users must remain silent 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 benefit from the LBS. 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 addition to anonymization by the trusted third party (central anonymity server), is proposed for obtaining a higher level of privacy [13], [16].

The main drawback on a centralized third party that limits the practicality. For example, the queries sent to the anonymity server[13] has to be waited until enough anonymization has been achieved for a group of users. Similarly in [8], the necessity for constructing the cloaking regions and also to receive the responses from the server through other users can considerably will degrade the service. Finally, most of the obfuscation based techniques shown inadequate to protect location privacy [11], [14] which are based on k-anonymity. Adding dummy queries to the user actual queries might help to confuse the adversary of the server about the actual user location. But while generating effective dummy queries for diverting the adversary is a difficult task [9], since they need to look like actual queries over time and location. In all the above-mentioned mechanisms, there is always a trade-off between user's private information and the quality of service which they experience. The tension gets maximized when hiding queries from the LBS server. Hiding the user query from the LBS server minimizes the revealed user information, hence, maximizes user privacy with respect to that of query.

3. 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).Users submit queries for their current location, and the type of information which is needed for them (context, point of interest, etc) they are interested in. The server in turn *replies* to the corresponding user, providing the latest requested context information around the submitted location; e.g., on hospitals, restaurants, gas stations, colleges, movie theaters, ongoing events, schools or current street traffic. Depending on the type of requested information the frequency of the users LBS queries varies, the dynamics of information updated in the LBS database, or the geographical region.

Based on the observed queries the Inference attacks are classified into two tightly-related categories: tracking and identification attacks. Such type of attacks can lead into two types of location-privacy: presence and the absence of disclosure of attack. In other words, the untrusted party can learn that the user is at a given location where they have send the query, or that the user is absent from certain locations, e.g., from their home. The more queries given by the user to the server the adversary observes, the higher its location inference attack success will be. Less information about the user current locations makes it harder 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.

In privacy preserving mechanism collaboration is the main concept used. This mechanism is mainly used in the crowd area (collaboration). In the crowd area if the user send the query request to the server, the server sends the response to the user but cannot tack the user since the location of the user can be identified by the server but the exact point cannot be identified by the server since in the crowd area there will be n number of user and they will be connected to the server with help of the network. Hence the user is protected from the server in the crowd area (MOBILE-CROWD). Therefore privacy of the user is protected in the privacy preserving method. But when the user is away from the crowd area the users are easily tracked by the server since there will be very few numbers of users. Hence the privacy of the user is not protected at this crowd less area. This is the main problem in the privacy preserving method. To overcome this problem Extended Kalman Filter method is proposed.

4. DESIGN OBJECTIVES

Overall, to overcome the above a practical and highly effective location-privacy preserving mechanism for LBSs has been introduced with the help of the Extended Kalman Filter algorithm. This algorithm method is a form of predictor corrector method.

The details of all the location has to be updated frequently in server or cloud database. Only then the updated information can be provided to the user when they send the query for a particular location. Each time when the user submit the query to the server, the server in turn check whether only the authorized user has send the request. The server in turn response to the user by sending the details which is requested by the server. If the user send the request for the location frequently to the server, the user will be easily tracked by the server and also by the untrusted party. Hence the user will be tracked and can blackmail the user. These are the way by which the user are tracked by the server and also by the unauthorized person when the user submit the query.

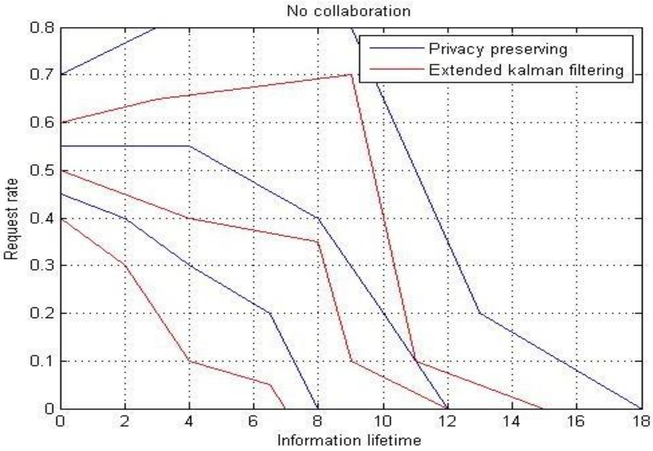

Fig.1 Privacy vs Extended Kalman Filter when collaboration is one

In the above figure comparison between preserving method and Extended Kalman Filter is obtained. It shows that when there is no collaboration that is when there is less number of user in the particular location where the user is connected to the server, the information lifetime of the user on the server side is high in the privacy preserving method. Hence the user will be easily tracked by the server in the privacy preserving method. But in the Extende Kalman Filter method when there is no collaboration and also when the request rate is high the information lifetime of the user on the server side is less. Therefore the privacy of the user in Extended Kalman Filter can be protected. Even when the collaboration is high in privacy preserving method the information lifetime of the user on the server side will be high compared to the proposed method.

4.1Our scheme:

Based on the design objective which has been stated above, a novel approach has been proposed for the location based service LBS which is known as Extended Kalman Filter. It is form of predictor corrector method. Extended Kalman finds all the data in all possible direction. When the user sends the query request to the server for a particular location which is needed for the user, the algorithm find all the possible direction the user can move from his current position. These data has to be uploaded frequently in the LBS server database. Since each data at in the different location will vary frequently and also new area will be added. This database will be controlled and will be managed by particular cloud server database. For each location there will be different latitude and the longitude value which is used for identifying the particular location

by the server when the user sends the query request. When the user sends the query request to the server, the server of this latitude and the longitude value the Extended Kalman finds the location of the user with the help of the latitude and the longitude value of that current location with the help of the GPS.

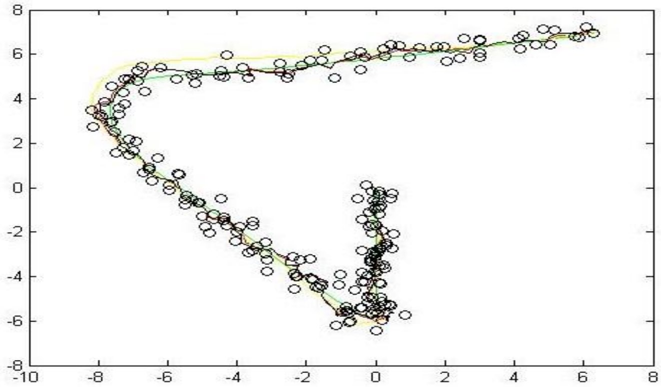

Fig.2 Extended Kalman Filter for one future location

In the above figure shows that when the user send the request to the server the data in a particular direction will be provided to the server. The circle in the figure represents the data available in the particular direction. The line passing through this circle represents that the user has travelled through that the path which is provided by the server which is requested by the server. The value in the x-axis represents the latitude and the value in the y-axis represents the longitude value.

4.2 Scheme Details

For each and every point of values or the landmark in each location the latitude the longitude value has to be created by the server and should be stored in the cloud database For every point the latitude and the longitude value varies. This is done in order to avoid confusion and also the server will find the location of the server only in the form of values. Hence each point of location is provided with the values. At the user side these values will be provided in the form of landmark and the name of the location. Hence the frequent request by the user to the server can be provided. Hence the user is protected from the tracking of server and also from the untrusted party. The GPS is now mostly available in all the android mobile phone which is developed for finding the particular location and also to find the route for a particular direction. With the help of this latitude and the longitude value the server will find all the possible direction the user can move from his current position. The data and the information in all these direction will be provided to the user. Hence the user will get additional information.

With the help of these data the user can travel to his desired direction without sending frequent request to the server. Hence the server does not know in which direction the user has travelled. Thereby the frequent request by the user can be avoided and so the privacy of the user can be protected. At the same time when the frequent request is avoided by the user on the server side the network traffic on the server side can be reduced.

A .Location Based Searching

To get the details of a particular location for eg, about colleges, hospitals, theater, hotels, etc, the user can enter the query and can send the request to the server. The server in turn response to the user by providing the information which is requested by the user.

B. Extended Kalman Filter

When the user enter the query to the server the Extended Kalman Filter algorithm finds the user future location. There will be many way from the point where the user sends the query. The Extended Kalman Filter finds all possible direction where the user can move. The server in turn does not know in which direction the user has travelled since all the data are provided previously to the user. Hence the frequent request will be avoided and therefore the users privacy will be protected.

5. CONCLUSION

With the help of the location based service the user can get the details of the particular location. But most of the server will trace the location of the user and could get the details of the user. Most of the literature review focus on gathering the details of the location but the security has not been considered as a major factor. By Extended Kalman Filter hiding probability decreases with the prediction of user's future location. When the user sends the query the algorithm finds all the possibility way the user can move from his current position and could be provided to the user. Thereby the frequent request by the user will be avoided and hence it is difficult for the server to trace the user. At the same time the network traffic on the server side can be reduced and the privacy of the user can be increased.

5.1 Future Work

Extended Kalman Filter has been used for the prediction of users future location. In this way all the future path direction and the details will be provided. In future work the required data from other data which is provided to the user can be displayed first. Thereby it is easy for the user to find the required details from the other information.

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.

6. 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.

[15] 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.

[16] Y. Liu, A. Rahmati, Y. Huang, H. Jang, L. Zhong, Y. Zhang, and S. Zhang, "xShare: Supporting Impromptu Sharing of Mobile Phones," Proc. Seventh Int'l Conf. Mobile Systems, Applications, and Services, 2009.

AUTHORS PROFILE

S.Sathya received the **B.E.** degree in Computer Science and Engineering from the P.A College of Engineering and technology, Pollachi, Anna University, Chennai, India, in 2013.Currently doing **M.E.** degree in Computer Science and Engineering in Akshaya College of Engineering and technology, Kinathukadavu, Anna University, Chennai**, India.**

B.Vinitha Subashini received **B.**E degree in Computer Science and Engineering from the Avinashilingam University. **M.E.** in Computer Science and Engineering from Anna University, Coimbatore. Currently working as Assistant Professor in Akshaya college of Engineering and technology, Kinathukadavu, Anna University, Chennai, India.