Hiding in the Mobile Crowd: Location Privacy through Collaboration

[#]V.Selvakumar
[#]Master of Technology in Computer Science & Engineering, PRIST University
Vallam, Thanjavur- 613 403.
[1]selvakumarpdkt@gmail.com

***Abstract*—Smart phones are very effective tools for increasing the productivity of business users. The smart phones allow end users to perform several tasks and led to offering provide to search a (LBS) Location Based Services. Existing process using Bayesian classification mechanism of location base service security is low privacy and the Adversary can easily access the private information and location based services of the user. The proposed solution of the problem using Epidemic model in a centralized manner of introduce third party system and user centric approach to provide privacy of a system between the users and the LBS.**

***Keywords*— Mobile networks, location-based services, location privacy, Bayesian inference attacks, epidemic models.**

I. INTRODUCTION

This document is a template. Smart phones are now a days state of the art among the peoples. The smart phone users are search location base services via communication infrastructure such as wi-fi access points. The user search location base services on LBS server. The LBS operator operate the LBS server. But sometime the LBS server not convenient for user. Because it sometime release the user location information or private information of the user. So the Adversary easily access the users private information. So existence of user private data is attacked and user logs of LBS queries are obtained by adversary.

The LBS server is not a perfect solution for provide user location base services. Because the existence of LBS server not using the centralized server. For instance, a user could download a large volume of data and then search through it for specific context information as the need arises. The need to enhance privacy for LBS users is understood and several solutions have been proposed, falling roughly into two main categories: centralized and user-centric. The centralized approaches introduce the third party buffer on protect between user and LBS sever. centralized approaches require the LBS to change its operation by, for example,mandating that it process modified queries (submitted in forms that are different from actual user queries, possibly encrypted using PIR, or that it store data differently (e.g., encrypted or encoded, to allowprivate access). Centralized interventions or 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.

The user centric approach is operate on device. This approach used to blur the user location information. We require no change in the LBS server architecture and its normal operation, and we make no assumption on the trustworthiness of the LBS or any third-party server. So the user can get the high privacy of and avoid the unwanted adversary entering the network. Hence, users can minimize their location information leakage by hiding in the crowd. The mobi crowd through the epidemic based differential equation and Bayesian based location interference attacks. The epidemic model is a novel approach to evaluating a distributed location-privacy protocol. We find that our epidemic model is a very good approximation of the real protocol; it reflects the precise hiding probability of a user.

The Bayesian interference framework is to adversary estimate location of user over time. The focus of the existing work in the literature is more on privacy-preserving functions for example obfuscation functions run independently by each user. To the best of our knowledge, this is the first such evaluation, and it is significantly more realistic than our own previous work that quantified privacy with just the fraction of queries hidden from the server. The proposed epidemic model of approaches to provide high privacy the user and user queries are hiding from server.

II. RELATED WORK

An easy One of the popular dynamics on complex networks is the epidemic spreading. An epidemic model describes how infections spread throughout a network. Among the compartmental models used to describe epidemics, the Susceptible Infected-Susceptible (SIS) model has been widely used. In the SIS model, each node can be susceptible, become infected with a given infection rate, and become again susceptible with a given curing rate. In this project, we add a new compartment to the classic SIS model to account for human response to epidemic spread. In our model, each individual can be infected, susceptible, or alert. Susceptible individuals can become alert with an alerting rate if infected individuals exist in their neighborhood. Due to a newly adopted cautious behavior, an individual in the alert state is less probable to become infected.Below the first threshold, infection dies out exponentially. Beyond the second threshold, infection persists in the steady state. Between the two thresholds, infection spreads at the first stage but then dies out asymptotically as the result of increased alertness in the network. Finally, simulations are provided to support our findings.

A. Protecting Location Privacy: Optimal Strategy against Localization Attacks

The mainstream approach to protecting the location-privacy of mobile users in location-based services (LBSs) is to alter the users' actual locations in order to reduce the location information exposed to the service provider. The location obfuscation algorithm behind an effective location-privacy preserving mechanism (LPPM) must consider three fundamental elements: the privacy requirements of the users, the adversary's knowledge and capabilities, and the maximal tolerated service quality degradation stemming from the obfuscation of true locations. We propose the first methodology, to the best of our knowledge, that enables a designer to find the optimal LPPM for a LBS given each user's service quality constraints against an adversary implementing the optimal inference algorithm.In such setting, we develop two linear programs that output the best LPPM strategy and its corresponding optimal inference attack. Our optimal user-centric LPPM can be easily integrated in the users' mobile devices they use to access LBSs. We validate the efficacy of our game theoretic method against real location traces. Our evaluation confirms that the optimal LPPM strategy is superior to a straightforward obfuscation method, and that the optimal localization attack performs better compared to a Bayesian inference attack.

B. Inference Attacks on Location Tracks

Although the privacy threats and countermeasures associated with location data are well known, there has not been a thorough experiment to assess the effectiveness of either. We examine location data gathered from volunteer subjects to quantify how well four different algorithms can identify the subjects' home locations and then their identities using a freely available, programmable Web search engine. Our procedure can identify at least a small fraction of the subjects and a larger fraction of their home addresses. We then apply three different obscuration countermeasures designed to foil the privacy attacks: spatial cloaking, inaccuracy, and imprecision. We show how much obscuration is necessary to maintain the privacy of all the subjects.

C. Quantifying and Protecting Location Privacy

It is a well-known fact that the progress of personal communication devices leads to serious concerns about privacy in general, and location privacy in particular. As a response to these issues, a number of Location-Privacy Protection Mechanisms (LPPMs) have been proposed during the last decade. However, their assessment and comparison remains problematic because of the absence of a systematic method to quantify them. In particular, the assumptions about the attacker's model tend to be incomplete, with the risk of a possibly wrong estimation of the users' location privacy.

The project, we address these issues by providing a formal framework for the analysis of LPPMs; it captures, in particular, the prior information that might be available to the attacker, and various attacks that he can perform. The privacy of users and the success of the adversary in his location-inference attacks are two sides of the same coin. We revise location privacy by giving a simple, yet comprehensive, model to formulate all types of location-information disclosure attacks. Thus, by formalizing the adversary's performance, we propose and justify the right metric to quantify location privacy. We clarify the difference between three aspects of the adversary's inference attacks, namely their accuracy, certainty, and correctness. In addition to evaluating some example LPPMs, by using our tool, we assess the appropriateness of some popular metrics for location privacy: entropy and k-anonymity. The results show a lack of satisfactory correlation between these two metrics and the success of the adversary in inferring the users' actual locations.

D. Evaluating the Privacy Risk of Location-Based Services

In modern mobile networks, users increasingly share their location with third-parties in return for location-based services. In this way, users obtain services customized to their location. Yet, such communications leak location information about users. Even if users make use of pseudonyms, the operators of location-based services may be able to identify them and thus affect their privacy. In this project, we provide an analysis of the erosion of privacy caused by the use of location-based services. To do so, we experiment with real mobility traces and measure the dynamics of user privacy.

E. On the Anonymity of Home/Work Location Pairs

Many applications benefit from user location data, but location data raises privacy concerns. Anonymization can protect privacy, but identities can sometimes be inferred from supposedly anonymous data. This project studies a new attack on the anonymity of location data.We show that if the approximate locations of an individual's home and workplace can both be deduced from a location trace, then the median size of the individual's anonymity set in the U.S. working population is 1, 21 and 34,980, for locations known at the granularity of a census block, census track and county respectively. The location data of people who live and work in different regions can be re-identified even more easily. Our results show that the threat of re-identification for location data is much greater when the individual's home and work locations can both be deduced from the data. To preserve anonymity, we offer guidance for obfuscating location traces before they are disclosed.

F. On the Optimal Placement of Mix Zones

In mobile wireless networks, third parties can track the location of mobile nodes by monitoring the pseudonyms used for identification. A frequently proposed solution to protect the location privacy of mobile nodes suggests changing pseudonyms in regions called mix zones. In this project, we propose a novel metric based on the mobility profiles of mobile nodes in order to evaluate the mixing effectiveness of possible mix zone locations. Then, as the location privacy achieved with mix zones depends on their placement in the network, we analyze the optimal placement of mix zones with combinatorial optimization techniques. The proposed algorithm maximizes the achieved location privacy

in the system and takes into account the cost induced by mix zones to mobile nodes. By means of simulations, we show that the placement recommended by our algorithm significantly reduces the tracking success of the adversary.

III. EXISTING VS PROPOSED

A. Existing System

The existing system of project using is not privacy because the user queries are processed by LBS operator of LBS server. The previous method using the Bayesian classification. Users can be linked to their locations, and multiple pieces of such information can be linked together. The LBS is a convenient process so the Adversary may easily access the user private information and location services.

1) Disadvantages

- 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.
- Low privacy of a user.

B. Proposed System

The proposed system of a project focusing the enhance privacy of a user queries and LBS. So using a develop on Epidemic model of approach using 2category. The one is introduce the third party system between user and LBS and other one is using User Centric Approach to operate devices and blur the location information. So the Adversary not entering the during communication between user and LBS.

1) Advantages

- 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.
- To provide high security and less time processing.

III SYSTEM DESIGN

A. System Architecture

Unfortunately, monitoring personal locations with a potentially untreated system poses privacy threats to the monitored individuals, because an adversary could abuse the location information gathered by the system to infer personal sensitive information. For the location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses a major privacy breach.

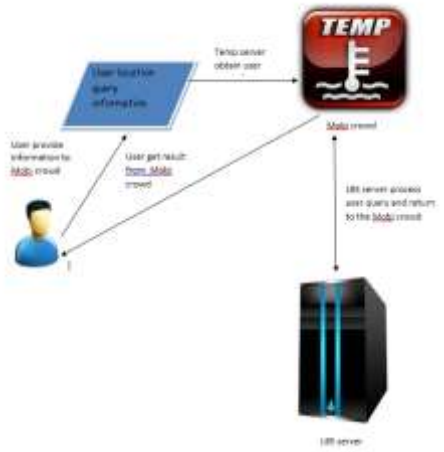

Fig 1. System Architecture

B. Modules

1) User search location base query on server

The smart phone user search location base services to the LBS server. But user some time search the private information via the LBS server. The LBS server is operated by the LBS operator. The LBS operator obtain user query to the LBS server. The LBS server return the location base services to the smart phone user.

2) Using third party Buffer system on a LBS server

The module is present the introduce third party system to a user. The user location base service is go to third party system. That is temporary storage area in LBS. It obtain the user location base query move to LBS operator. The LBS operator is operate the LBS server to provide location base services to the user.

Fig. 2 Key Generation

C. Algorithm Used

The proposed solution of the problem using Epidemic model in a centralized manner of introduce third party system and user centric approach to provide privacy of a system between the users and the LBS.

1) Attribute base Encryption

Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Key Generation (MK,S): The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Encrypt (PK,A, M): The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes.

Decrypt (PK,CT,SK): The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy a, and a private key SK,

Initialize.
For all nodes i:
Mark I susceptible
Mark source infectious append source to the infectious list
Set source's infection time to 0
For time starting at 1:
While the earliest infected node I in infectious list…
…has been infectious longer thanZś
removei from infectious_list
Mark i as recovered
 # Check if the outbreak died.
If infectious_list is empty:
Return #
Go through the SI contacts.
Empty to_change_to_infectious
For nodes i in infectious_list:
For neighbor's j of i:
If j is susceptible:
With a probability ƽś
Append j to to_change_to_infectious mark j as infectious next time
 # Change the ones to be infectious next time step.
For nodes i in to_change_to_infectious:
Mark i as infectious
Append i to infectious_list

D. LBS Services

In this paper LBS service has two main component

1) Mobile devices
2) LBS database server

Cloaking technique is implemented in mobile device, dummy generation technique is used to generate fake locations, and those locations are not actually physically present there. In Dummy there is a fixed sized grid, size of grid is allocated through using k vertices when grid is formed, fake Q with parameter. This search query is reached to LBS server, LBS server performs search operation and generates result, and then mobile user gets answer.

Locations are created .Due to these fake locations the privacy of original user is maintained, due to this user gets protections from attacks. Baye's rule is used to prevent adversary attack, after location gets secured mobile device sends search query

IV. CONCLUSIONS

The project finally proposed method to using enhances user privacy of a location based services. The scheme developed for prevent user private information and hide the crowd on mobi devices finally minimize the adversary entering on network. The MobiCrowd achieves collaboration between users. The epidemic model catch the user locations that are to be hide by use of it. For that reason adversary does not observe query information, the previously Bayesian interference attack not provide the full privacy of a user. So adversaries easily access the user query data and maximize the adversary entry on network. So we have enhanced the resource efficiency of MobiCrowd by implementing in portable devices.

REFERENCES

1. R. Shokri, "Quantifying and Protecting Location Privacy," PhD dissertation cole polytechnique federale de Lausanne, 2013.
2. 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.
3. R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying Location Privacy," Proc. IEEE Symp. Security and Privacy, 2011.
4. R. Shokri, J. Freudiger, and J.-P. Hubaux, "A Unified Framework for Location Privacy," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (HotPETs), 2010.
5. 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.
6. J. Meyerowitz and R.R. Choudhury, "Hiding Stars With Fireworks:Location Privacy through Camouflage," Proc. MobiCom'09, 2009.
7. 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.
8. 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.
9. J. Krumm, "A Survey of Computational Location Privacy," Personal Ubiquitous Computing, vol.13, no. 6, pp. 391-399, 2009.
10. 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.
11. R. Anderson and T. Moore, "Information Security Economics and Beyond," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology, 2007.

