Providing Privacy for User Location by Collaboration

Authors

Shree Guru TG¹, DR Arun Biradhar²

¹Student, East West Institute of Technology Bangalore, Karnataka

²Professor, HOD of Computerscience, East West Institute of Technology Bangalore, Karnataka

Email- guru.jesta@gmail.com, Arunbiradhar@ewit.edu

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. The results show that our scheme hides a high fraction of location-based queries, thus significantly enhancing users' location privacy. Our simulations with real mobility traces corroborate our model-based findings. Finally, our implementation on mobile platforms indicates that it is lightweight and the cost of collaboration is negligible.

Key words—Mobile Networks, Location-based Services, Location Privacy, Bayesian Inference Attacks, Epidemic Models

1.INTRODUCTION

Smartphones, among other increasingly powerful mobile computing devices, offer various methods of localization. Integrated GPS receivers, or positioning services based on nearby communication infrastructure (WiFi 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.

All this information is collected by the LBS operators. So, they might be tempted to misuse their rich data by, e.g., selling it to advertisers or to private investigators. The mere existence of such valuable data is an invitation to attackers, who could break into the LBS servers

and obtain logs of user queries, or governments that want to detect and suppress dissident behavior. The result in all cases is the same: usersensitive data fall in the hands of untrusted parties. The difficulty of the problem lies in protecting privacy of users who also want to earn the benefits of LBSs. Therefore, solutions such as not using LBSs are not acceptable. For instance, a user could download a large volume of data and then search through it for specific context information as the need arises. But this would be cumbersome, if not impractical, and it would be inefficient for obtaining information that changes dynamically over time. 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. 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. 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. Why would the new server be any more trustworthy? Additionally, new proxy servers become as attractive for attackers as centralized LBSs. Other 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 allow private 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. Indeed, if a revenue stream is to be lost by user data not being collected, then not many LBS providers can be expected to comply. Misaligned incentives have been identified as the root of many security problems. User-centric ap-

proaches 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 userlocation-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. Our approach avoids the problems of these two extremes by having users collaborate with each other to jointly improve their privacy, without the need for a trusted third-party (TTP). In effect, the mobile crowd acts as a TTP, and the protection mechanism becomes a distributed protocol among users. We implemented our scheme on Nokia N800, N810 and N900 mobile devices, and we demonstrated it with the Maemo Mapper (a geographical mapping software for points of interest). Our approach can be used in the upcoming technologies that enable mobile devices to directly communicate to each other via (more energy-efficient) Wi-Fi-based technologies that aim at constructing a mobile social network between mobile users. The rest of the paper is organized as follows.

2. LITERATURE SURVEY

Paper 1: Achieving Efficient Query Privacy for Location Based Services

Mobile smartphone users frequently need to search for nearby points of interest from a location based service, but in a way that preserves the privacy of the users' locations. We present a technique for private information retrieval that allows a user to retrieve information from a database server without revealing what is actually being retrieved from the server. We perform the retrieval operation in a computationally efficient manner to make it practical for resource-constrained hardware such as smartphones, which have limited processing power, memory, and wireless bandwidth. In particular, our algorithm makes use of a variable-sized cloaking region that increases the location privacy of the user at the cost of additional computation, but maintains the same traffic cost. Our proposal does

not require the use of a trusted third-party component, and ensures that we find a good compromise between user privacy and computational efficiency. We evaluated our approach with a proof-of-concept implementation over a commercial-grade database of points of interest. We also measured the performance of our query technique on a smartphone and wireless network.

Paper 2: Collaborative Location Privacy by †Reza Shokri, ‡Panos Papadimitratos, †George Theodorakopoulos, and †Jean-Pierre Hubaux

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 identify and track users. We address this problem by proposing the first, to the best of our knowledge, user-collaborative privacy preserving approach for LBSs. Our solution, MobiCrowd, is simple to implement, it does not require changing the LBS server architecture, and it does not assume third party privacy-protection servers; still, MobiCrowd significantly improves user location-privacy. The gain stems from the collaboration of MobiCrowd-ready mobile devices: they keep their context information in a buffer, until it expires, and they pass it to other users seeking such information. Essentially, the LBS does not need to be contacted unless all the collaborative peers in the vicinity lack the sought information. Hence, the user can remain hidden from the server, unless it absolutely needs to expose herself through a query. Our results show that MobiCrowd hides a high fraction of location-based queries, thus significantly enhancing user location-privacy. To study the effects of various parameters, such as the collaboration level and contact rate between mobile users, we develop an epidemic model. Our simulations with real mobility datasets corroborate our model-based findings. Finally, our implementation of MobiCrowd on Nokia platforms indicates that it is lightweight and the collaboration cost is negligible.

Paper 3: Quantifying Location Privacy: The Case of

Sporadic Location Exposure

By Reza Shokri¹, George Theodorakopoulos¹, George Danezis², Jean-Pierre Hubaux¹, and Jean-Yves Le Boudec¹

Mobile users expose their location to potentially untrusted entities by using location-based services. Based on the frequency of location exposure in these applications, we divide them into two main types: Continuous and Sporadic. These two location exposure types lead to different threats. For example, in the continuous case, the adversary can track users over time and space, whereas in the sporadic case, his focus is more on localizing users at certain points in time. We propose a systematic way to quantify users' location privacy by modeling both the location-based applications and the location-privacy preserving mechanisms (LPPMs), and by considering a well-defined adversary model. This framework enables us to customize the LPPMs to the employed location-based application, in order to provide higher location privacy for the users. In this paper, we formalize localization attacks for the case of sporadic location exposure, using Bayesian inference for Hidden Markov Processes. We also quantify user location privacy with respect to the adversaries with two different forms of background knowledge: Those who only know the geographical distribution of users over the considered regions, and those who also know how users move between the regions (i.e., their mobility pattern). Using the Location-Privacy Meter tool, we examine the effectiveness of the following techniques in increasing the expected error of the adversary in the localization attack: Location obfuscation and fake location injection mechanisms for anonymous traces.

Paper 4: Protecting Location Privacy: Optimal Strategy against Localization Attacks by Reza Shokri[†], George Theodorakopoulos[‡]

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. Such LPPM is the one that maximizes the expected distortion (error) that the optimal adversary incurs in reconstructing the actual location of a user, while fulfilling the user's service-quality requirement. We formalize the mutual optimization of user-adversary objectives (location privacy vs. correctness of localization) by using the framework of Stackelberg Bayesian games. 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.

Paper 5: Selfish Response to Epidemic Propagation

By George Theodorakopoulos, Jean-Yves Le Boudec, and John S. Baras *†‡

An epidemic that spreads in a network calls for a decision on the part of the network users. They have to decide whether to protect themselves or not. Their decision depends on the trade-off between the perceived infection and the protection cost. Aiming to help users reach an informed decision, security advisories provide periodic information about the infection level in the network. We study the best-response dynamic in a network whose users repeatedly activate or deactivate security, depending on what they learn about the infection level. Our main result is the counterintuitive

fact that the equilibrium level of infection increases as the users' learning rate increases. The same is true when the users follow smooth best-response dynamics, or any other continuous response function that implies higher probability of protection when learning a higher level of infection. In both cases, we characterize the stability and the domains of attraction of the equilibrium points. Our finding also holds when the epidemic propagation is simulated on human contact traces, both when all users are of the same best-response behavior type and when they are of two distinct behavior types.

.2.Existing system:

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.

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.

User centric approach operates on the Every device, typically aim to blur the location , incorrect and noisy gps .

3. PROPOSED SYSTEM

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. The results show that our scheme hides a high fraction of location-based queries, thus significantly enhancing users' location privacy. Our simulations with real mobility traces corroborate our model-based findings. Finally, our implementation on mobile platforms indicates that it is lightweight and the cost of collaboration is negligible.

4. ADVANTAGES OF PROPOSED SYSTEM:

It is more secure.

It will improve privacy, without the need for a trusted third-party (TTP).

It will not change in the LBS server architecture and its normal operation.

Module description

Location base server

The server which provide location information to the user devices .

In our key idea The user device when in seeker state if it wont get the information it would search and get info from LBS .

Mobile crowd

Mobicrowd is a distributed protocol running on multiple collaborating devices .

Key idea of mobicrowd through both epidemic based differential equation model and bayesian frame work for location Inference attacks.

Mobicrowd effective when number of users more in location at time t.

User

Smart phones wifi enable device each device maintaine transparent proxy buffer with location specific information.

User device in crowd may be a seeker, informer, remover .0

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 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 safe guard 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>."
2. J. Meyerowitz and R. Roy Choudhury, "Hiding stars with fireworks: location privacy through camouflage," in *MobiCom '09: Proceedings of the 15th annual international conference on Mobile computing and networking*, 2009.
3. F. Olumofin, P. K. Tysowski, I. Goldberg, and U. Hengartner,
4. "Achieving efficient query privacy for location based services," in *Privacy Enhancement Technologies (PETS)*, 2010.
5. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the ACM SIGMOD international conference on Management of data*, 2008.
6. R. Anderson and T. Moore, "Information Security Economics—and Beyond," *Advances in Cryptology-CRYPTO*, 2007.
7. R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A distortion-based metric for location privacy," in *WPES '09: Proceedings of the 8th ACM workshop on Privacy in the electronicsociety*. New York, NY, USA: ACM, 2009, pp. 21–30.