W^3-Privacy: the Three Dimensions of User Privacy in LBS

Pablo A. Pérez-Martínez
UNESCO Chair in Data Privacy
Universitat Rovira i Virgili
Tarragona, Catalonia, Spain
pabloalejandro.perez@urv.cat

Agusti Solanas
UNESCO Chair in Data Privacy
Universitat Rovira i Virgili
Tarragona, Catalonia, Spain
agusti.solanas@urv.cat

ABSTRACT

Thanks to the generalisation of smartphones, location-based services (LBS) are steadily gaining importance. Although LBS have an enormous potential, the privacy risks that they might suppose to users could put the break to their growth. Thus, it is paramount to propose countermeasures to fight against the privacy breaches of LBS. In this article, we describe the three dimensions of user privacy in LBS. We introduce the concept of W^3-privacy, and we propose a new obfuscation method based on population density, anonymous payments and query uncertainty.

1. INTRODUCTION

Due to the growing use of mobile devices with self-location capabilities, a large number of LBS are being implemented worldwide. Using LBS might be very beneficial but could lead to undesired privacy risks. Indeed, users share their locations, their identities and their queries with third parties (*e.g.* LBS providers). Thus, a lot of users' private information can be derived by LBS providers, namely consumer habits, economical status, workplace, etc. There is a clear need for methods that protect the privacy of the users of LBS whilst they can still enjoy all their benefits.

In this article, we describe the three dimensions of user privacy in LBS and we coin the term W^3*-privacy*. Also, we propose a density-based method to obfuscate the location of LBS users. We show that our proposal achieves W^3-privacy when it is properly combined with anonymity and uncertainty methods.

2. W³-PRIVACY

If we consider the privacy of LBS users we can distinguish three main independent dimensions, namely identity privacy (*i.e.* **Who** you are), location privacy (*i.e.* **Where** you are), and query privacy (*i.e.* **What** you want to know). We say that a LBS is W^3-private if the service is given whilst the provider (i) does not know who is the user, (ii) where is the user, and (iii) what does the user ask for.

Most proposals concentrate on solving the privacy problems in a single dimension. Due to space limitations we will not elaborate on all the proposals; the reader can refer to [1] for a survey on privacy methods for LBS. To address "identity privacy" most solutions rely on trusted third parties (TTP), that mediate between users and providers to hide their real identities using, for example, pseudonyms. Others try to hide users by means of onion routers [2]. In the first case, "identity privacy" is not guaranteed because the intermediaries know the real identities.

Method	Who	Where	What
Pseudonymiser (TTP)		√	
Annonymiser (TTP)		√	
Individual Obfuscation	√	√	
Collaborative Obfuscation		√	
PIR		√	√
Our proposal	√	√	√

Table 1: Brief comparison of private LBS methods with regard to W^3-privacy

The most popular topic in LBS privacy is "location privacy". Several methods have been proposed to protect it, namely spatial and temporal cloaking (anonymisers and psudonymisers), individual location obfuscation, collaborative location obfuscation, etc. Most methods use TTP or collaboration to hide real locations, thus, they obtain location privacy at the cost of identity privacy. Only individual obfuscation methods guarantee location privacy without sacrificing identity privacy. "Query privacy" has captured the attention of the research community in the fields of Internet search engines and privacy preserving data mining. Several techniques to achieve query k-anonymity have been proposed and also private information retrieval (PIR) techniques are used. However, both approaches have serious practical limitations (mainly for computational reasons). Table 1 shows a brief summary of the privacy features of several methods to protect privacy in LBS.

3. OUR PROPOSAL

In this section we describe our proposal to achieve W^3-privacy in LBS that require payment. First, we show how to guarantee "identity privacy". Second, we

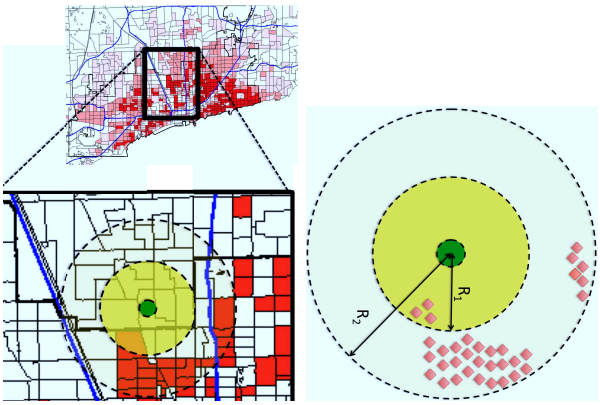


Figure 1: *(left)* Chicago's density map and user located on it. *(right)* Radius of uncertainty around the user and candidate points.

present a new obfuscation method to protect "location privacy", and finally we describe how "query privacy‘" is achieved.

3.1 WHO

As we have previously introduced, a good way of protecting "identity privacy" is the use of onion routers [2]. Notwithstanding, this is not enough when LBS providers require the authentication of the subscribers. In these cases, an anonymous payment protocol has to be used. We suggest using the partially blind signature of Abe-Okamoto [3]. Before sending queries to a LBS provider, every user subscribes using the protocol described in [3], by doing so, users can authenticate without revealing their identity and providers can charge them for the service properly. Due to space limitations, we cannot recall the protocol here; we suggest the reader to refer to [3] and [4].

3.2 WHERE

People living and moving in cities do not distribute uniformly. On the contrary, every city has streets, avenues and squares having a greater population density. Thus, it is feasible to obtain a density map such as the one shown in Figure 1. We assume that these maps are common to every LBS user and can be freely accessed. They can be understood as a set of points in $\Re^3$, (x, y, d), where x, y represent longitude and latitude, and d is the density in those coordinates. By using this information, users can determine the points/locations of maximum density, which are excellent candidates to be used as fake locations because they make difficult the object identification (OI) and restricted space identification (RSI) attacks.

To preserve their "location privacy" users define a series of uncertainty radius $\mathcal{R} = \{R_1, R_2, \ldots, R_m\}$ in which they try to find points with, at least, a minimum density d_{min}. These points could be used as fake points.

First, users locate themselves (*e.g.* with a GPS). Then, they select the area (defined by the radius) in which they want to find fake points. Finally, they use the information of the density map to determine the points that have a density greater than d_{min} that are within a range smaller than a given R_i. If no points fulfilling the required conditions are found, the user should relax the constraints and restart the procedure. Once the candidate points are found, users can select one of them randomly (alternatively, users can select the point which is closer to them, thus, reducing the error whilst maintaining the uncertainty).

3.3 WHAT

With the aim to preserve "query privacy", users generate a number k of different queries $\{q_1, q_2, \ldots, q_k\}$. Thus, the provider is not able to determine which is the real query. This idea resembles the concept of k-anonymity and has been widely used to guarantee query privacy with Internet search engines [5].

4. CONCLUSIONS

In this article we have introduced the concept of W^3-privacy related to the three dimensions of user privacy in LBS. We have shown that most methods do not consider all dimensions and we have proposed a new method based on density maps to preserve "location privacy". Also, we indicate that combining our proposal with partially blind signatures and query k-anonymity, we can obtain a W^3-private location-based service.

5. REFERENCES

[1] A. Solanas, J. Domingo, and A. Martínez, "Location privacy in location-based services: Beyond TTP-based schemes," *PiLBA'08 Privacy in Location-Based Applications*, p. 12, 2008.

[2] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *In Proceedings of the 13th USENIX Security Symposium*, 2004, pp. 303–320.

[3] M. Abe and T. Okamoto, "Provably secure partially blind signatures," in *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '00, 2000, pp. 271–286.

[4] Q. Wu, J. Castellà, J. Domingo, A. Solanas, and B. Qin, "Portable device-centric mutual privacy in priced location-based services," manuscript.

[5] J. Domingo, A. Solanas, and J. Castellà, "h(k)-private information retrieval from privacy-uncooperative queryable databases.","*Online Information Review*, vol. 33, no. 4, pp. 720–744, 2009.