Privacy Protection in Location-Based Services Through a Public-Key Privacy Homomorphism

Agusti Solanas and Antoni Martínez-Ballesté

CRISES Research Group
UNESCO Chair in Data Privacy
Dept. Computer Science and Mathematics
Rovira i Virgili University
{agusti.solanas,antoni.martinez}@urv.cat

Abstract. Location-Based Services (LBS) can be accessed from a variety of mobile devices to obtain value added information related to the location of the user. Most of the times, these services are provided by a trusted company (*e.g.* a telecommunications company). However, the massive use of mobile devices pave the way for the creation of ad hoc wireless networks that can be used to exchange information based on locations. In the latter case, these LBS could be provided by an untrusted party. Sending the location to an untrusted LBS provider could put the privacy of the user in jeopardy. In this paper we propose a novel technique to guarantee the privacy of users of LBS. Our technique consists of several modules, but the highest degree of security is achieved thanks to the use of a public-key privacy homomorphism. Unlike the existing approaches, our proposal does not need any trusted third party to anonymise the users and only makes use of a public-key infrastructure.

Keywords: location privacy, public-key privacy homomorphism.

1 Introduction

Location-Based Services (LBS) allow users to receive highly personalised information. These services can be accessed by using a variety of mobile devices that can utilise a plethora of localisation technologies. Mobile devices have become ubiquitous and services related to the current position of the users are growing fast. Some examples of these LBS are tourist information service, router planners, emergency assistance, etc. For a given user of LBS, sending her location could put her privacy in jeopardy.

An LBS basically consists of an LBS provider delivering location-based information and a set of users asking for this information. Mobile devices have a variety of ways for determining their approximate location. Thus, we assume in this paper that the utilised devices have this capability (*i.e.* they can determine their longitude and latitude).

In this scenario, a user u asks the LBS provider P for some information, sending the message $\{ID_u, query, long, lat\}$. Upon this request, P seeks the desired information in its database and returns an appropriate answer to u. Note that, if u sends her exact location to an untrusted LBS provider P_u, it can misbehave

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 362–368, 2007.

because it can relate the real location '$long, lat$' with the unique identifier of u, ID_u, for instance: (i) P_u is able to know if u is in front of certain shops or places, so it can flood her with undesired advertisements; (ii) P_u can track u so it knows where she has been and when; (iii) P_u can send the identifier of u along with her location to a spammer, and the later can send undesired location-based advertisements to the user.

In order to avert these possible misbehaviour of the LBS provider, two main solutions are possible:

- *Hiding the position within other users.* By using this technique inspired in the well-known k-anonymity approach [1,8], P is not able to distinguish u among a set of k users because they share the same fake location. This indistinguishability makes difficult the tracking and habits inference of the user.
- *Giving an inaccurate position to the LBS provider.* The position should be accurate enough so the information received by u is still useful. However, since the locations collected by P are not exact, they become useless to a spammer[1].

To the best of our knowledge, all previous proposals related to privacy in LBS rely on a trusted third party (TTP). One of them is the so-called *anonymizer*, a TTP used for anonymising locations by means of a mediation between users and LBS providers. The *anonymizer* can behave (i) by deleting personal information from the queries of the users before sending them to the LBS providers, or (ii) by hiding the exact position of the user (*i.e.* modifying it).

In the second case, the *anonymizer* hides the real location of the user under a *cloaked region* (*i.e.* a spatial region containing k users) so that each user becomes k-anonymous (*i.e.* not distinguishable among $k-1$ other users). According to [4], the cloaked region must fulfil the requirements of k-anonymity, but must also consider a spatial cloaking. In that sense, the cloaking algorithm considers a minimum and maximum area sizes and the *anonymizer* uses the requests from other users (and the location data contained in them) to compute a *masked* location, taking into account the value of k and the area requirements. The masked location can be computed as the centroid of the current locations of the users in the cloaked area.

In [2], an efficient algorithm for cloaking is presented. Similar approaches are also presented in [3] and [6].

1.1 Contribution and Plan of This Paper

In this paper we present a novel location privacy technique based on a Public-Key Infrastructure (PKI) and a public-key privacy homomorphism. Unlike the existing proposals, our technique does not rely on the LBS server acting as a TTP but on the collaboration of the users and an LBS server certified by a certification authority.

[1] Note that, although this seems to be a strong assumption, it is reasonable to believe that the user, who really knows her location, could make a proper use of the information given by the provider. On the contrary, the provider has access to the fake location only.