Privacy in Geolocation Systems

Miguel E. Andrés
INRIA and LIX, Ecole Polytechnique, France

Abstract. The growing use of mobile devices equipped with GPS chips has significantly increased the use of Geolocation Systems. This kind of systems employs geographical information (typically expressed as latitude and longitude coordinates) identifying the position of an entity in order to provide a service. Examples of Geolocation Systems include (1) Location-Based Services (LBS) such as mapping applications, GPS navigation, and location-aware social networks as well as (2) Location-Data Mining algorithms used to determine, among others, points of interest, traffic patterns, and disease geographical distributions.

While Geolocation Systems have demonstrated to provide enormous benefits to individuals and society, its popularity raises important privacy issues. For example, by using a LBS, users may unknowingly allow companies to compile detailed profiles of their daily activities including places they visit, people they meet, and events they attend. Similarly, Location-Data Mining algorithms can be used, for example, to determine the home location of individuals using their GPS navigation information.

In this work we present a novel technique that allows one to use Geolocation Systems while still providing formal privacy guarantees to the users confiding the underlying geographical information. In order to illustrate our technique, consider a user who wishes to use a LBS that takes as input his location and returns information about restaurants nearby his location (this is a standard use of LBS; popular mobile applications like AroundMe, Google Places, and Localscope – available for Iphone and Android based smartphones – provide this kind of service). In addition, suppose that this user wishes to keep his current location secret. The techniques presented in this work allow to accomplish both goals, i.e., obtaining useful information from the LBS and keeping the user's location private.

Roughly speaking, our mechanism works by first adding controlled noise to the user's location in order to obtain an (sanitized) approximate version of the user's location and then providing the LBS with the user's approximate location (instead of the real one). Our mechanism offers a privacy guarantee, that we call (ϵ, r)-geo-indistinguishability, which assures the user that by revealing his approximate location, his current location will remain indistinguishable within a certain area around him (regardless of any side knowledge that the adversary, in this case the LBS party, might have about his current location). Or, more precisely, the reported location is almost as likely (at most e^{ϵ} times more likely) to have been generated from the user's location as to have been generated from any other location within a radius r of the user's location.

We show a correspondence between our privacy definition and the popular notion of Differential Privacy. In particular, we show that geo-indistinguishability is an instance of a (non-standard) generalization of differential privacy. In addition, we report on the challenges we needed to overcome in order to provide a mechanism satisfying geo-indistinguishability.

We conclude our work by demonstrating the applicability of our approach through two case studies, one based on LBS and the other on Location-Data Mining.

In the former case, we show that, by trading privacy for bandwidth usage, geo-indistinguishability can be obtained without degrading the utility of the information provided by LBS. In the latter case, we show how to apply our technique to sanitize datasets containing geographical information. In particular, we show how to sanitize publicly available geographic information released by the US Census Bureau. Our experiments reveal that providing (ϵ, r)-geo-undistinguishability to all users in the dataset (i.e., US inhabitants) does not significantly decrease the quality of the sanitized data (the degree of decrease being inversely proportional to the parameters ϵ and r of the privacy guarantee).