Sharing locations through semantic labels

Antonio M. Bellido, Juan Antonio Álvarez, Juan Antonio Ortega
Universidad de Sevilla. ETS. Ingeniería Informática
Departamento de Lenguajes y Sistemas Informáticos
{abellido}@us.es, {jaalvarez, ortega}@lsi.us.es

Abstract

Given the lack of privacy offered by web applications that integrate geo-positioning systems and the huge growth of internet use on mobile devices that use these systems, this paper proposes a solution to the problems of privacy and security in ubiquitous computing using semantic labeling techniques. This will get users to share information about their location with their environment more in a more secure and private way. The work will lay the foundation to develop care applications targeted to investigations related to improving human memory, which will help to explore the interaction between man and machine and find the social utility of this work.

1 Introduction

We are in the information age, much of our life is captured in digital media, that information needs to be well protected and it safety should be high. But we, as owners of our own privacy sometimes inadvertently expose sensitive data accessible to strangers. It is very common for users to record their real data in web applications and social networks without reading the terms and conditions of the site where they will share their information, these sites publish vast amounts of information that could be sensitive. The main motivation of this work is to provide a proposal to improve the privacy and security in the area of ubiquitous computing.

Today, the capabilities of traditional GPS are included in the smartphones. These mobile devices support Internet connectivity through wireless networks, GSM or both. The features and possibilities of these devices are fired due to their capacities, the large number of application developers and the huge market they serve.

Much of the information shared in social networks is highly sensitive and it should be take much care with the privacy and security issues by both parts the users and the service managers.

The scientists and technologists have a moral duty to provide service techniques and methods to protect the security of such information that is largely protected by a little-known law.

In our work we will focus on improving the privacy and security information related to the location of users when they move outdoors.

2 Problem description

The problem that gives rise to the approach of this work is the privacy and security of the localization data that are shared across different applications on the Internet especially in social networks. The root of the problem is in the location-based services (LBS) in use today. These services make use of the coordinates of latitude and longitude give to offer a standard service as accurate as possible. The currently most widely used LBS are based on the concepts of geocoding and reverse geocoding.

The geocoding service is based on the textual description of a place (for example street address, city, zip code, country and so on) to get the coordinates of that location. The reverse geocoding service is the opposite, from the coordinates in latitude and longitude it obtains the textual description of the place. These textual descriptions of the localization are always found in urban and political maps to achieve a standard service. The advantage offered by using this kind of systems is that these services are standard and from one of the two types of information anyone can get the other if the information is right.

From the latitude and longitude coordinates obtained using any location-based service, the precise location point can be represented on a map and it can be obtained an accurate information about the location gathered by a device, threatening the privacy and safety of users. The intention with this work is to hide the coordinates shared by users to those outside their circle of friends.

3 Related work

There are various researchers who have performed several studies to examine privacy in the use of location applications that allow information sharing. Some of these studies have used practical methods where users have used mobile devices to simulate location requests [Anthony et al, 2007] or [Consolovo et al, 2005], or experiments where participants have simulated laboratory information sharing scenarios related to the location [Brown et al, 2007] or [Barkhuus

et al, 2008]. The results show that the use and context are key factors in the disclosure of location data, i.e. the desire to share a place and level of detail depends largely on who is requesting this information [Consolovo et al, 2005] and [Tsai et al, 2009] and the social context of the application [Khalil et al, 2006].

Location cloaking is a popular method to provide privacy to the user locations [Gedik et al, 2005] and [Cheng et al, 2006] or [Mokbel et al, 2006]. In this method, an individual device or a third party hides the location of the individual before giving it to a service provider location. For each individual, the service provider offers a particular region in which the user is located, but not the exact location.

In 2010, Bernheim Brush collected some of the existing techniques to hide the exact position of the GPS traces of users based on mathematical techniques [Bernheim Brush, 2010]. But these techniques are characterized to hide or confuse the true positions in these traces. Therefore, it is losing accuracy.

4   Proposed solution

In our proposal we suggest is the use of semantic labels to increase the privacy of users without sacrificing accuracy in the location you want to share with our circle of friends. The concept is simple, consists in doing a translation of the location you want to share to a label previously defined by users. Therefore, these labels provide significant value to the user and his contacts, but not for other network users (see figure 1).
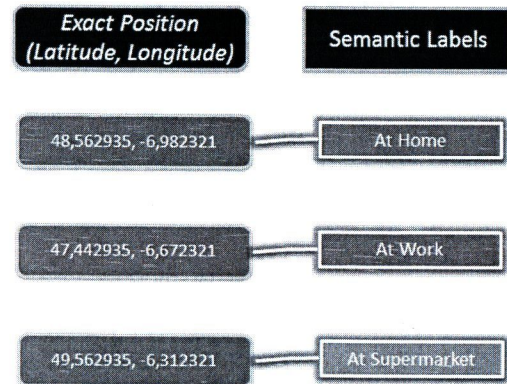

Figure 1: The Semantic label concept

As a simple example, the semantic label "At home" that corresponds to the coordinates (-6.341234, 48.123344) latitude and longitude does not make sense for those who do not know me, but it has to my friends. With other methods discussed above it would be translated the same place as "Seville" if we use location cloaking techniques or in other cases, giving no precise positions. We get to reveal our position to people who we really want and hiding the others,

so anyone can't know the exact location that corresponds to the label "At home".

Obviously it is intended that these labels are customizable and allow users to modify them, create new and delete as they wish.

The intention is that a location that has particular relevance to a user can be identified with a label that provides the following improvements (see figure 2):
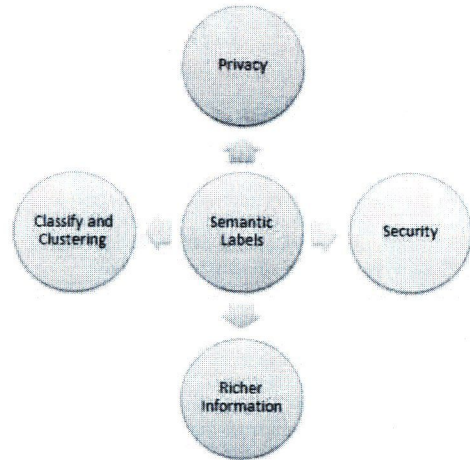

Figure 2: Semantic label improvements

❖ Provision of greater meaning for users, richer information.
❖ Provision of greater privacy by sharing locations.
❖ Provision of greater safety by sharing locations.
❖ Allow the classification and clustering of locations by labels.

4   Conclusions and future work

One of the most interesting trends of marketing in recent years in search advertising relevance, is to join the geolocation technology to the Social Media environment through mobile devices by opening endless new possibilities for marketing professionals, called "social geo-location". In this context, privacy and security of users is one aspect that we should always keep in mind with the advancement of information technology. Social networks that offer services based on geo-locations (Geo-Social Networks) and the own location-based services are increasingly used in our society.

As future work aims to develop applications that leverage the use of semantic labels in different areas in which location-based systems are integrated. Among the applications to be developed we highlight a diary with the locations that users visited based on semantic labels that allow a user remember what he did during a period of time. Then it can be used to develop memory aid-systems.

References

[Anthony et al, 2007] Anthony, D.; D. Kotz; T. Henderson. "Privacy in location-aware computing environments". *IEEE Pervasive Computing*, 2007.

[Barkhuus et al., 2008] Barkhuus, L.; B. Brown, M. Bell, S. Sherwood, M. Hall, and M. Chalmers. "From awareness to repartee: sharing location within social groups". *In CHI '08*, 2008.

[Bernheim Brush et al, 2010] Bernheim Brush; A.J., John Krumm and James Scott. "Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location". *Ubicomp, 2010*.

[Brown et al, 2007] Brown, B.; A. Taylor; S. Izadi; A. Sellen; J. Kaye; R. Eardley. "Location family values: A field trial of the whereabouts clock". *In Ubicomp '07*, 2007.

[Cheng et al, 2006] Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S. "Preserving User Location Privacy in Mobile Data Management Infrastructures". *In: Danezis. G., Golle, P. (eds.) PET 2006. LNCS, vol. 4258, pp. 393–412. Springer, Heidelberg (2006)*.

[Consolovo et al, 2005] Consolovo, S.; I. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. "Location disclosure to social relations: Why, when, & what people want to share". *In CHI '05*, 2005.

[Gedik et al, 2005] Gedik, B., Liu, L. "Location Privacy inMobile Systems: A Personalized Anonymization Model". In: ICDCS 2005. *Proceedings of 25th International Conference on Distributed Computing Systems, 2005*.

[Khalil et al, 2006] Khalil, A. and K. Connelly. "Context-aware telephony: Privacy preferences and sharing patterns". *In CSCW '06*, 2006.

[Mokbel et al, 2006] Mokbel, M.F., Chow, C.-Y., Aref, W.G.: The New Casper: Query Processing for Location Services without Compromising Privacy. *In: Proceedings of the 32nd International Conference on Very Large Data Bases, 2006*.

[Tsai et al, 2009] Tsai, J.; P. Kelley, P. H. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh. "Who's viewed you? the impact of feedback in a mobile-location system". *In CHI '09*, 2009.