2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware

Interactive Location Cloaking with the PROBE Obfuscator

Gabriel Ghinita[1], Maria Luisa Damiani[2], Elisa Bertino[1] and Claudio Silvestri[2]
[1]Purdue University [2] University of Milan
{gghinita, bertino}@cs.purdue.edu {damiani, silvestri}@dico.unimi.it

Abstract

The problem of private location-based queries has been intensively researched in recent years. Several location protection algorithms exist, most of which use some form of location cloaking. However, existing work focuses on the analysis of privacy and performance, and less on the user's perspective on location privacy. We developed a prototype of the PROBE [1] system with an emphasis on visualization of the location cloaking process, which improves user experience and increases privacy awareness.

1. Introduction

To protect their privacy, mobile users of location-based services (LBS) must replace their exact locations with *cloaked regions (CRs)* [2]. Past research investigated theoretical properties of cloaking, such as privacy and performance. However, users perceive LBS in the context of geo-spatial visualization and map navigation. Therefore, an intuitive interpretation of cloaking is more appealing to them than abstract analyses. Providing a visual representation of cloaking has two important advantages: *(i)* users are presented with an intuitive interface common to existing mobile applications and *(ii)* users have a visual confirmation of the effectiveness of location cloaking. Such features are essential to enhance privacy awareness and to facilitate adoption of location protection services.

We propose a prototype for interactive cloaking of user locations, based on the PROBE [1] privacy system. PROBE provides privacy guarantees against the association of users with sensitive locations (e.g., hospitals, bars, etc). Moreover, privacy can be easily personalized by specifying preferences about the sensitive locations and the desired degree of protection. Based on the user's profile and the map of sensitive locations, PROBE efficiently generates an *obfuscated map* that disguises sensitive locations.

Assume that Bob does not want to reveal his whereabouts when he is in the proximity of bars. PROBE replaces Bob's exact location with an *obfuscated cell*: an area that contains a mix of sensitive (i.e., bar) and innocuous *feature types*. The association probability with a certain feature type is thus bounded below a user-specified threshold. Our tool lets users gather sensitive features information and request obfuscated maps from trusted entities. Users are presented with a clear and intuitive picture of how their location is protected, improving user experience and increasing privacy awareness.

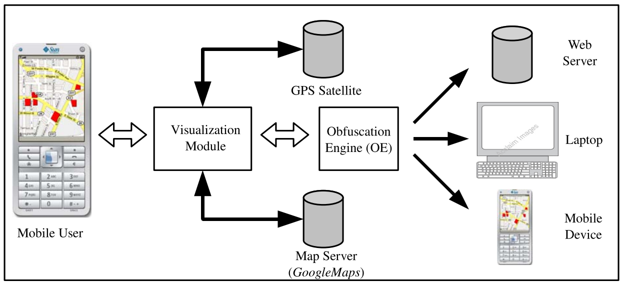


Figure 1. System Architecture

2. System Architecture

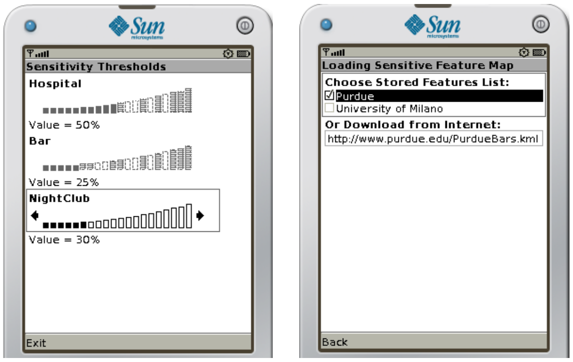
The mobile user connects to the Internet using a GPS-enabled device (Fig. 1), and retrieves maps and sensitive features information from a map repository (e.g., *GoogleMaps*). The device interfaces with an *obfuscation engine (OE)* that transforms maps according to the user's privacy profile. The OE can be either *(i)* a web-based application, *(ii)* a laptop accessible through a low-cost channel (e.g., Bluetooth), or *(iii)* the mobile device itself (if sufficient resources exist). Our prototype is based on JavaME, and compatible with CLDC 1.1 and MIDP 2.0 specifications. To visualize maps, we use the *J2MEMap*[1] library, which can interface with a variety of map providers (e.g., GoogleMaps, YahooMaps, etc). Maps can also be stored locally, saving communication costs. For better readability, we show snapshots captured with the Sun Wireless Toolkit v2.5[2]. However, we have successfully tested our prototype with a Nokia N95 device.

3. Demonstration Overview

We walk through the most important features of the proposed prototype: setting the user profile, loading and visualizing sensitive features, and visualizing obfuscated maps.

[1] http://j2memap.8motions.com/
[2] http://java.sun.com/products/sjwtoolkit/

978-0-7695-3650-7/09 $25.00 © 2009 IEEE
DOI 10.1109/MDM.2009.49



Sensitivity Thresholds

Hospital

Value = 50%

Bar

Value = 25%

NightClub

Value = 30%

Exit

Loading Sensitive Feature Map

Choose Stored Features List:

☑ Purdue

□ University of Milano

Or Download from Internet:

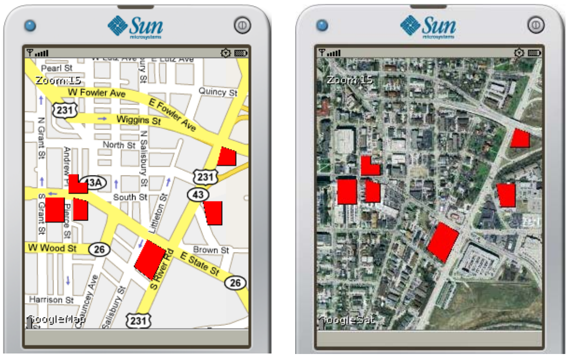
http://www.purdue.edu/PurdueBars.kml

Back

(a) Choosing Sensitivity Thresholds

(b) Loading Sensitive Features List

Figure 2. Managing the Privacy Profile



(a) Map View

(b) Satellite View

Figure 3. Visualizing Sensitive Features

Setting the User Profile. The user creates a privacy profile as shown in Fig. 2(a). The sensitive feature types can be generated from a comprehensive (possibly hierarchical) list[3]. The thresholds are specified as maximum probabilities of association, and are expressed as percentages. The next step is to load the sensitive features data. We adopt the widespread KML format to specify sensitive features, which are represented as polygonal lines. Fig. 2(b) shows how the user can load the features from a locally stored list, or can download them from a trusted web site. In this demo, we consider a list of bars on the Purdue campus.

Visualizing Sensitive Features. Upon loading the KML file, the application automatically navigates the map to the location specified, with an appropriate zoom level to enclose the entire map. The features relevant to the user's profile are represented as red polygons, both in map view (Fig. 3(a)) and satellite view (Fig. 3(b)). The user can navigate the list of sensitive features using the device keys, as shown in Fig. 4. The name and type are specified for each sensitive feature.

Creating and Visualizing Obfuscated Maps. The user sends the sensitive feature list and the privacy profile to the trusted OE. To save bandwidth, only a link to the location of the KML file can be specified. The user will receive back a list of polygonal regions corresponding to the obfuscated cells. Fig. 5(a) shows the user view, where obfuscated cells are marked with a blue line. The user also has the option to isolate the cell that currently encloses him/her (Fig. 5(b)), by joining the obfuscated cell list with the GPS-retrieved user location. The user can inspect the actual location information that is disclosed to the LBS. Such visual confirmation is an important factor to improve user experience and increase adoption of anonymization services.

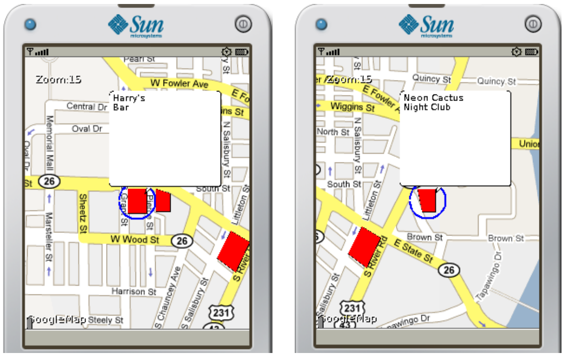
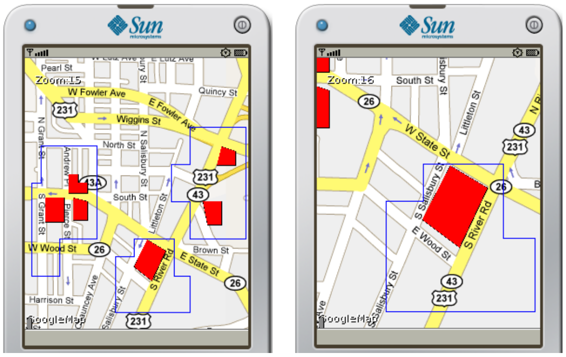


Figure 4. Navigating the Features List



(a) Obfuscated Map

(b) Obfuscated Cell Enclosing the User

Figure 5. Visualizing Obfuscated Maps

4. Conclusions

We developed a tool for retrieving and visualizing obfuscated maps on mobile devices. Our tool is not restricted to a particular paradigm, and can be used with other cloaking-based techniques (e.g., [2], [3]).

References

[1] M. Damiani, E. Bertino, and C. Silvestri. PROBE: an Obfuscation System for the Protection of Sensitive Location Information in LBS. Technical Report 2001-145, CERIAS, 2008.

[2] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *USENIX MobiSys*, 2003.

[3] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias. Preventing Location-Based Identity Inference in Anonymous Spatial Queries. *IEEE TKDE*, 19(12):1719–1733, 2007.

[3] Users can create profiles using a computer (with superior ergonomy), and import them on the mobile device