Chapter 3.10
Memorizing Algorithm:
Protecting User Privacy using Historical Information of Location-Based Services

Quynh Chi Truong
National University of Ho Chi Minh City, Vietnam

Anh Tuan Truong
National University of Ho Chi Minh City, Vietnam

Tran Khanh Dang
National University of Ho Chi Minh City, Vietnam

ABSTRACT

The rapid development of location-based services, which make use of the location information of the user, presents both opportunities and challenges. Users can benefit from these services; however, they must often disclose their location information, which may lead to privacy problems. In this regard, the authors propose a solution with a memorizing algorithm, using trusted middleware that organizes space in an adaptive grid where it cloaks the user's location information in an anonymization area before sending it to the service providers. This newly introduced memorizing algorithm calculates on the spatial grid to decrease the overlapped areas as much as possible, which helps conceal users' locations. This solution protects the user's privacy while using the service, but also against data mining techniques with respect to their history location data. Experimental results with a user activities map establishes this theoretical analyses as well as the practical value of the proposed solution.

INTRODUCTION

Advances in location technologies and wireless communication technologies enable the widespread development of location-based services (LBS) that make use of the location information of users (Kupper, 2005; Schiller & Voisard, 2004). As location information is a part of users' private information, it requires a number of solutions to protect the location privacy of users while not affecting much on the quality of the location-based services. Location privacy can be defined as the

DOI: 10.4018/978-1-61350-323-2.ch3.10

right of individuals, groups, and institutions to determine themselves how, when, to whom, and for which purposes their location information is used (Ardagna, Cremonini, Vimercati, & Samarati, 2008; Kupper, 2005; Mohamed, 2007). When the user location information is not well protected, the user can face various kinds of location attacks. Some attacks just make the user annoying, for instance unconsenting advertisements, while the others can endanger the user such as stalking or physical harassment (Ardagna, Cremonini, Vimercati, & Samarati, 2008; Atluri & Shin, 2008; Bettini, Mascetti, & Wang, 2008). The problem of privacy preserving in LBS attracts numerous attentions from both research communities and industry sectors (Bettini, Mascetti, & Wang, 2008). The user's location privacy should be safeguarded in two stages. In the first stage, the location privacy should be protected at the time of using services. One popular method is to obfuscate the location with the service providers in order to hide the user's true location information (Mohamed, 2007). The solution focuses on preventing the user's locations from an illegal observation at the time of service calls. However, when a user uses the service several times in a specific area, it will cause an overlapping problem which can be exploited to identify the highest possible area where the user is (Gidófalvi, Huang, & Pedersen, 2007). Then, it leads to the second stage which ensures the user's privacy when the user's location information is stored in the database for data mining purposes (Gidófalvi, Huang, & Pedersen, 2007).

Although there are many researches on this field, they only concentrate on privacy preserving in either the first stage or the second stage. This paper proposes a novel approach for privacy preserving in both stages. Our solution bases on a LBS framework consisting of a trusted middleware (see Figure 1b). We also introduce an algorithm that applied in the middleware.

The algorithm receives the user's location and privacy requirement as inputs; then it cloaks the user's location in a grid-based map. The anonymiztion area yielded by the algorithm will satisfy the user's privacy requirement and also solve the overlapped-area problem. More importantly, the grid-based map is dynamically sizeable according to the user's privacy requirement.

The rest of this paper is organized by briefly summarizing related work. We will present our discussion on the privacy problem of overlapped areas and present our grid-based approach for the problem. Next, we introduce our memorizing algorithm that works on the grid for preserving user privacy in LBS in both cases, namely, fixed-grid-based map and adaptive-grid-based map. Finally, experimental results are discussed, as well as concluding remarks and future work.

Figure 1. The privacy architectures. a) The non-cooperative architecture. b) The centralized trusted party architecture. c) The peer-to-peer cooperative architecture.