Chapter 14
Positioning and Privacy in Location–Based Services

Haibo Hu
Hong Kong Baptist University, China

Junyang Zhou
Hong Kong Baptist University, China

Jianliang Xu
Hong Kong Baptist University, China

Joseph Kee-Yin Ng
Hong Kong Baptist University, China

Location positioning by GPS has become a standard function in modern handheld device specifications. Even in indoor environments, positioning by utilizing signals from the mobile cellular network and the wireless LAN has been intensively studied. This chapter starts with some review of the state-of-the-art technologies. Positioning technologies propel the market of location-based services (LBS). They are mobile content services that provide location-related information to users. However, to enjoy these LBS services, the mobile user must explicitly expose his/her accurate location to the service provider, who might abuse such location information or even trade it to unauthorized parties. To protect privacy, traditional approaches require a trusted middleware on which user locations are anonananonymous ymized. This chapter presents two new privacy-preserving approaches without such a middleware. The first is a non-exposure location cloaking protocol where only relative distances are exchanged. The second is a protocol for nearest neighbor search with controlled location exposure.

INTRODUCTION

With the advent of new-generation smart mobile devices such as Apple iPhone and Google gPhone, location positioning by GPS and aGPS (assisted-GPS) become a standard function in handheld device specifications. Texas Instruments forecasts that by 2012, 34% of mobile handsets will be shipped with GPS modules. Even in indoor environments, positioning by utilizing signals from the mobile cellular network and the wireless LAN has been intensively studied and its accuracy has been sig-

nificantly improved recently. In the first half of this chapter, we will review some of the state-of-the-art technologies.

Positioning technologies propel the market of mobile value-added services, in particular the location-based services. Location-based services (LBS) are mobile content services that provide location-related information to users. A typical LBS is the nearest neighbor query, in which the user quests for the nearest point of interest (e.g., gas station, restaurant) from where he/she is.

However, in order to enjoy these LBS services, it appears that the mobile user must explicitly expose his/her accurate location to the service provider, who might abuse such location information or even trade it to unauthorized parties. Even worse, the nature of location-based services seems to leave the users with no choice but to see their location privacy compromised in exchange for services. This rising concern is hindering the prosperity of LBS market and the mobile industry as a whole. The research community have identified this issue lately and attempted to solve it using "attribute generalization", a common approach used for privacy protection in RDBMS. The main idea is to blur the user location in a service request, that is, to replace the accurate user location with a cloaked region (usually a circle or a rectangle). This region encloses the accurate user location and satisfies some privacy metric such as k-anonymity (at least k users share the same region so that they are indistinguishable).

However, a centralized and trusted middleware (usually called "anonymizer") is required to form such cloaked regions for users before their LBS requests reach the service provider, and ironically the users have to expose their accurate locations – exactly what they want to hide – to this middleware. In case such middleware is not available or cannot be trusted, the LBS request cannot proceed without privacy compromise. In the second half of this chapter, we will study two approaches that address this issue.

First, we design a non-exposure location cloaking protocol. This protocol consists of a clustering stage and a secure bounding stage, during which only relative distances are exchanged among users to obtain the cloaked region. Furthermore, an anonymizer is not required in this protocol. Second, we take one step further – to allow users to skip the location cloaking phase and request location-based service directly from the (untrusted) server. In particular, we study the nearest neighbor (NN) query, an important location-based service. We learn from computational geometry that the query space forms a Voronoi Diagram, which is composed of Voronoi cells. Each data object corresponds to one Voronoi cell and this object is always the NN in this cell. As such, the essence of an NN query is matching the user location to some Voronoi cell. However, this matching implicitly exposes the user location to the server. We therefore study a client-server protocol that allows the users to learn the cell information in their neighborhood, so that they can resolve NN queries with controlled location exposure to the server.

BACKGROUND: LOCATION POSITIONING TECHNOLOGIES

Satellite-Based Position System

There are several satellite-based navigation systems, including the US's **G**lobal **P**osition **S**ystem (GPS) (Dana, 1998), the Russian Federation's **GLO**bal **NA**vigation **S**atellite **S**ystem (GLONASS) (Russian Space Agency) and the European Union's Galileo navigation system (European Space Agency). They enable receivers or terminals on the earth to gain location information.

Among these systems, the Global Position System is the most widely used one. In the following, we introduce this system in detail in order to have an overview of satellite-based navigation

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/positioning-privacy-location-based-services/41637

Related Content