Contents lists available at SciVerse ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Privacy preserving shortest path routing with an application to navigation

Yong Xi *, Loren Schwiebert, Weisong Shi

Department of Computer Science, Wayne State University, Detroit, MI 48202, United States

ARTICLE INFO

Article history:
Received 2 April 2012
Received in revised form 3 June 2013
Accepted 11 June 2013
Available online xxxx

Keywords:
Location privacy
Shortest path
Navigation

ABSTRACT

Mobile navigation is a frequently used application, especially with the increasing proliferation of online geographical data. However, the origin and destination are often private information closely tied to a user's personal life. Sharing those with an online map provider greatly increases the chance of the user being profiled. Contrary to existing location privacy problems, the origin and the destination are essential for finding the shortest path in a realtime traffic setting. In this paper, we show that the problem can be solved with Private Information Retrieval (PIR) techniques without disclosing the origin or the destination. We analyze the cost associated with this approach and propose a practical solution with the assumption of a semi-honest third party to improve the efficiency. The proposed practical solution only introduces encryption overhead over the plain scenario where the path is returned by knowing the origin and destination.

1. Introduction

GPS-based navigation is quite common today. It is especially useful when one is visiting a new area. A standalone GPS device contains built-in maps. The map is used for multiple purposes. First, it is used to relate GPS coordinates to the physical context, such as which road the user is currently on. Second, it is used for calculating the shortest path between an origin and a destination. Finally, it often contains additional information such as points of interest so that an user would be able to find places he may be interested in.

In recent years, phone-based navigation is gaining popularity. A typical example is Android-based Google map navigation. There are multiple reasons behind this. First and foremost, cellular phones are becoming much more powerful, with GPS built-in, bigger and better screens that are often comparable with dedicated GPS screens, and faster processors and larger memory capacities that are necessary to run a navigation application. Second, broadband cellular data services are increasingly available and more affordable. This has enabled cheap or free service-based navigation as the map and direction data are retrieved on-demand.

Service-based navigation is a type of location-based service. The origin and the destination information are sent to the server. Based on routing options, such as choosing the fastest or shortest route, a planned route is returned and the navigation application uses the route and location information provided by the GPS to guide the user to the destination.

In location-based services, privacy is a key issue. This certainly applies to service-based navigation as the origin and the destination are most likely associated with the user's personal plans. The privacy is even more sensitive here as it gives a perception of the user's movement being tracked. Krumm [1] gives a thorough review of computational location privacy. Computational location privacy involves interpreting location information as geometric information and quantifying privacy

* Corresponding author.
E-mail addresses: yongxi@wayne.edu (Y. Xi), loren@wayne.edu (L. Schwiebert), weisong@wayne.edu (W. Shi).

1574-1192/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2013.06.002

in such a way. For example, it has been shown that by merely looking at a sequence of locations from a single user, a person could be profiled [2].

The common strategies in protecting location privacy are through anonymity and obfuscation. Anonymity-based approaches mix one person's information with another's. It is intended to remove the uniqueness of a person's location information. Obfuscation-based approaches reduce the precision of the location information so that it becomes less sensitive.

Finding the shortest path between an origin and a destination is significantly different from existing location privacy problems. The pair of origin and destination information is necessary input for finding the path. Besides the privacy of each piece of information, the pair itself represents a unique combination that may be personally identifiable. Yet, they are inseparable.

In this paper, we investigate possible solutions of finding the shortest path between an origin and a destination, without the risk of compromising their privacy. We apply the principle of private information retrieval (PIR) [3] and discuss practical solutions.

The rest of the paper is organized in the following way. In Section 2, we present our problem definition in detail. In Section 3, we apply the principle of PIR and discuss their complexity. In Section 4, we present practical solutions. In Section 5, we discuss related work. Finally, we present our conclusions.

2. Problem

In this section, we use a transportation network as our case study scenario in studying the privacy-preserving shortest path search. First, we describe the application scenario and its motivation. Then, we abstract the problem, turning it into privacy-preserving shortest path search.

2.1. Application scenario

Phone-based navigation is gaining popularity as the mobile Internet is more affordable and GPS becomes a standard option on smart phones. Typical examples include Google map navigation and Microsoft Bing map navigation. A dedicated GPS navigation device uses a built-in map. In contrast, phone-based navigation software does not have a pre-installed map. It thus depends on the service for actual routing.

From a privacy perspective, using a built-in map has great benefits because it does not disclose origin and destination information. Service-based routing, on the other hand, requires the origin and destination being transmitted in order to find the shortest path between the origin and the destination. Although there could be policy-based approaches to limit access to this information, we are focusing on the problem of not disclosing the origin and the destination in this paper. We strongly believe that it should be one of the privacy choices that is presented to users.

The lack of a local map on a phone can be partially alleviated by caching map data. This is especially true if the map data is relatively static. By using the cached data, the phone could compute the shortest path locally, thus removing the privacy concern. Similarly, using cached data to protect location privacy has been considered by [4–6]. It essentially decouples spatial and temporal information and depends closely on the data being relatively static.

In this paper, we will instead focus on the case when the shortest path is provided by the service. There are two practical reasons for this. First, although smart phones are quite powerful today, finding the shortest path might still involve searching through a large graph, which could be slow. Second and more importantly, finding the shortest path should inherently be a server-side task. For example, ideal route planning in transportation is highly dependent on real-time traffic information, which suggests that giving path suggestions is a type of mesoscopic scale traffic control. Thus, protecting privacy in this case is an important scenario that we need to tackle.

In this paper, we will assume that static information, such as the network topology, is already available on the client side. This can either be achieved by caching the topology for later use, or by using pre-installed maps. This is a reasonable assumption as the topology of the transportation network does not change frequently.

2.2. The problem

We formulate the problem as a two party graph searching problem. One party, A, holds the location information of its origin, o, and destination, d. It also holds the topology of the network. However, it does not know the cost of traveling each link in the network as the cost may be constantly changing. The other party, B, holds the graph in which the origin and the destination are connected and it knows the cost of traveling each link. The problem is for A to find the shortest route from the origin to the destination, without disclosing either the origin or the destination information to B. Formally, A holds the pair (o, d). B holds the graph $G = (V, E)$, where $o \in V$ and $d \in V$. To accommodate our application scenario, we restrict our discussion to simple direct graphs with only positive weights on edges.

2.2.1. Basic solution

A basic solution is for B to send to A a representation of all-pairs shortest path information upon request. Then A uses o and d to extract the shortest path from the received representation. A does not disclose any information wrt (o, d) in this process.