Computer Communications 000 (2017) 1–13

Contents lists available at ScienceDirect

Computer Communications

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

Secure hitch in location based social networks

Shiwen Zhang[a,b], Yaping Lin[a,*], Qin Liu[a], Junqiang Jiang[a], Bo Yin[c], Kim-Kwang Raymond Choo[d]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan, 410082, China
[b] College of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, Hunan, 411201, China
[c] College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, Hunan, 410076, China
[d] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Article history:
Received 21 May 2016
Revised 14 January 2017
Accepted 20 January 2017
Available online xxx

Keywords:
Location based social networks
Location privacy
Private proximity detection
Multi-keyword dimensional search

ABSTRACT

Location based services are increasingly popular, partly due to the trend of smartphone and online social network service adoption. However, it is important for location-based service provider (LBSP) to ensure user location privacy in the provision of such services. In this paper, we present a secure hitch service in location based social networks (LBSNs). To provide such a service, we propose a privacy-preserving proximity based location query (PPLQ) protocol, which is based on the hierarchical predicate encryption technique and the prefix membership verification technique. There are two types of users in this system, namely: the querier and the publisher. Our protocol allows a querier to query the location of publishers using multi-dimensional search, and it enforces distance based access control in the location queries. In order to improve the efficiency of our protocol, we use the multi-scale technique to represent user's location information in the query condition and searchable index. The proposed protocol is designed to achieve multi-dimensional keyword search and bilateral private proximity testing simultaneously. Our protocol enables each user to independently define his/her own location policy for private proximity testing. In particular, we propose some solutions to reduce the search time cost of the CSP so that the time cost is acceptable for queriers. Finally, we demonstrate the utility of the protocol using simulated data on the map of the city area of Changsha and a U.S. census dataset.

1. Introduction

Online social networks (OSNs), such as Facebook and Twitter, are increasingly prevalent in our society. One popular feature of OSNs is location based service (LBS), particularly on mobile apps. However, the information collected by location based social network service provider (LBSPs), such as locations and other personally identifiable information, need to be protected to ensure the privacy of the users. Hence, how to provide LBS while protecting users' location privacy in LBSNs is a topic of active research (see [1–4]).

Existing location privacy preserving techniques can be broadly categorized into query enlargement, fake locations, progressive retrieval and encryption based. However, these techniques generally introduce additional system costs or reduce the utility of the data in LBSP context [4], due to degrading of the quality of the service. Other privacy-preserving location query approaches, such as those reported in [3,5,6], impose relatively expensive computational requirements which is not suitable for deployment on mobile devices, such as Android and iOS devices. It could also be challenging for these approaches to support location based queries over encrypted data in a scalable manner [4]. This is the gap we seek to address in this paper. Specifically, we present a solution to ensure user's location privacy when the user requests the secure hitch service from LBSP in a flexible and scalable manner. The hitch service requires that the designed solutions to be able to support secure multi-dimensional keyword search and private proximity testing simultaneously.

Let us consider an application scenario of location based service, secure hitch service, in LBSNs. In deployment of secure hitch service in LBSNs (e.g. cab hailing service), users need to register with the service provider (LBSP). The cab driver as a publisher outsources his/her personal information, such as profile, location, and interests to LBSP, which can also be a cloud service provider (CSP). The ordinary user as a querier can request the hitch service in a convenient, privacy preserving, and secure manner. Alice (a querier) first requests the cab hailing service from the service provider by submitting a query such as "(*Sex* = "*Male*") **AND**

* Corresponding author. Tel.: +008613808459868.
E-mail addresses: shiwenzhang@hnu.edu.cn (S. Zhang), yplin@hnu.edu.cn (Y. Lin).

http://dx.doi.org/10.1016/j.comcom.2017.01.011
0140-3664/

$(20 \leq Age \leq 25)$ **AND** $(Brand = \text{“}BMW\text{”})$”. If Bob (a publisher) satisfies the query condition, then Alice will determine whether Bob is within 1,000 meters of her, without exposing her location information to either Bob or the service provider. Meanwhile, Bob checks if Alice is within 1,500 meters of him, without exposing location information to either Alice or the service provider. We regard 1,000 meters as Alice's location policy P_a and 1,500 meters as Bob's location policy P_b. If Bob is within P_a and Alice is within P_b, then Bob offers his cab hailing service to Alice by exchanging his location information with Alice. Otherwise, neither party know the location information of the other party. There are three key challenges for providing secure hitch service in LBSNs. First, the proposed scheme needs to support privacy-preserving multi-dimensional keyword search. Second, the proposed scheme needs to support bilateral private proximity testing. For example, the policies of Alice and Bob are set to P_a and P_b, respectively. This system allows Alice and Bob to determine whether the distance is within P_a and P_b, respectively. The private proximity testing is bilateral. Third, the proposed scheme needs to support dynamic location policy. For instance, Alice can assign different location policies for different queries by generating different trapdoors. For example, Alice will request drivers in the range of 1,000 meters in the afternoon, 2,000 meters in the evening, etc.

To meet the privacy-preserving multi-dimensional keyword search requirement, a number of privacy-preserving keyword search techniques for encrypted data have been proposed in the literature, such as searchable encryption (SE) [7,8]. However, these schemes generally support only single-keyword search. In order to support flexible and more complex queries, multi-keyword search schemes such as those reported in [9–11] have been proposed. However, the supported query types of these schemes are limited and cannot efficiently support the simple range query. The computation complexity of these schemes is also high. Hierarchical predication encryption (HPE), a new cryptographic primitive proposed by Okamoto et al. [12], allows one to achieve multi-dimensional keyword search supporting arbitrary query types including conjunctive normal form (CNF) and disjunctive normal form (DNF) formals. However, the proposed HPE cannot execute the multi-dimensional keyword search and private proximity testing simultaneously; hence, the scheme cannot be directly applied to the application scenario discussed in the preceding paragraph.

To deal with the private proximity detection or testing problem while ensuring location privacy, a number of private proximity detection schemes have also been proposed [13–15]. However, existing proposals for private proximity detection require users to interact with each other several times in order to achieve privacy-preserving distance computation and distance comparison. This leads to high communication costs, yet lacks flexibility in user's preferences. In other words, existing literature appear to address multi-dimensional keyword search and private proximity testing separately.

In this paper, we propose a privacy-preserving proximity based location query (PPLQ) protocol, which enables each querier to obtain the publisher's location information without compromising the users' location privacy. In this protocol, each user maintains his/her own policy. Each user generates the location coordinate range according to his/her location policy. The proposed protocol adopts prefix membership verification technique to determine whether a user's location coordinate is within the location coordinate range of the other users. To improve the efficiency of private proximity testing algorithm, we adopt the multi-scale technique to represent user location coordinate and location coordinate range. We can change the number of grids of the location coordinate range representation in the last scale level or the number of scale levels to support user's dynamic location policy. To achieve the private proximity testing algorithm, we add the user location coordinate and location coordinate range information into the searchable index. We then utilize the hierarchical predicate encryption technique, which integrates with prefix membership verification technique, to achieve privacy-preserving multi-dimensional keyword search and private proximity testing simultaneously. To summarize, the main contributions of this paper are:

- We propose a privacy-preserving location query protocol. The proposed protocol utilizes multi-scale technique to represent user's location coordinate and location coordinate's range in the index and query condition, and then utilizes prefix membership verification and predicate encryption technique to achieve secure multi-dimensional keyword search and private proximity testing simultaneously.
- Our protocol is secure and flexible, in the sense that it supports bilateral private proximity testing without exposing users' location privacy. If both parties satisfy each other's location policy, then they can exchange location information with each other. Furthermore, the proposed protocol enables each user to maintain his/her own location policy, and can even assign different location policies for different queries.
- We define and establish the corresponding system model and threat model, and carry out extensive experiments for the proposed protocol. The security analysis and performance evaluation show that the proposed protocol is secure and efficient.

We will review related literature in the next section, prior to introducing the system model, threat model, and our design goals in Section 3. The preliminaries are presented in Section 4. We present the proposed PPLQ protocol in Section 5, and a construction of this protocol is presented in Section 6. The performance and security evaluations are given in Section 7. The last section concludes this paper.

2. Related work

2.1. Searchable encryption

Traditional searchable encryption schemes allow a server to tell a user whether a given keyword is present in the encrypted data, without the user without learning anything else about the encrypted data. Song et. al [7] proposed the first practical symmetric key cryptography based on searchable encryption scheme, and subsequent improvements and security definitions are presented by Chang et al. [8] and Curtmola et al. [16]. However, these schemes only support single-keyword queries which are inadequate for real-world location based services.

To enhance the search functionalities, conjunctive keyword search was subsequently proposed, such as those presented in [9–11]. However, these schemes incur significant computation overheads due to the use of fundamental primitives in public-key cryptography, bilinear map and secret key sharing. Furthermore, the supported query types of these schemes are limited. Predicate encryption (PE) scheme [12] allows one to achieve conjunctive and disjunctive search, as well as supporting arbitrary query types and CNF/DNF formulas. However, it is not able to support private proximity testing. Our work is similar to that of [17], where we both consider the secure multi-keyword search problem. However, the scheme in [17] neither protects the user's location privacy nor supports bilateral private proximity testing. This is the gap we seek to address; specifically, our proposed protocol is designed to support both multi-dimensional keyword search and private proximity testing.

Please cite this article as: S. Zhang et al., Secure hitch in location based social networks, Computer Communications (2017), http://dx.doi.org/10.1016/j.comcom.2017.01.011