Information Sciences 372 (2016) 758–772

Contents lists available at ScienceDirect

Information Sciences

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

One-round secure fair meeting location determination based on homomorphic encryption[☆]

Xiaofen Wang[1,*]

Big Data Research Center, Center for Cyber Security and School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, China

ARTICLE INFO

Article history:
Received 10 August 2015
Revised 24 August 2016
Accepted 26 August 2016
Available online 28 August 2016

Keywords:
Location privacy
Fair meeting location
Homomorphic encryption
Cloud service

ABSTRACT

Determination of optimal meeting location without revealing the locations of participants to the location server is an interesting research problem. A major concern for a location based service is location privacy. However, adding privacy protection to a location service will inevitably introduce computational complexity. To provide location privacy with low computational cost is a challenging task. In this paper, we propose a one-round meeting location determination protocol, where the location service provider makes a decision with a semi-trusted cloud server which works as a computation center and conducts most of computation. The user location privacy is preserved against the outside and internal attackers including the computation center, the meeting location determination server and participants. In order to study the performance of the protocol, we test its computational efficiency on smartphones. The simulation results and the performance comparison of our protocol with another protocol of the same functionalities demonstrate that our solution is more efficient and practical.

1. Introduction

The wide availability of location based services including navigation, service recommendation, optimal meeting location determination has brought great benefits and convenience to users. There are two types of location based services: services based on location check-in and services based on location sharing [13]. For the first type, users obtain location-specific services from a third party service provider by checking into it. The applications including special query, range query, nearest neighbor query, shortest path query are of this type. For the second type, a group of users share their locations and gain location services for the whole group. The second type of service is becoming more and more popular, and has various applications, e.g., taxi sharing application, and optimal meeting location determination.

Although these services have great advantages, they are receiving increasing skepticism. The very nature of these applications may disclose users'personal information (such as home address, hobbies, or habits) which may be tracked and misused for purposes such as commercial profiling, unsolicited and instructive advertising. Especially in location sharing services, users'private locations and their shared location may be revealed. Therefore, privacy becomes a critical problem in location-sharing based applications, where the user location information may be revealed to the service provider or the

[☆] Fully documented templates are available in the elsarticle package on CTAN.

[*] Corresponding author.
E-mail address: wangxuedou@sina.com

[1] Since 1880.

http://dx.doi.org/10.1016/j.ins.2016.08.083

other participants. Without effective protection, even sparse location information will help to show users'reliable personal information, which could jeopardize users' social, financial and daily life. Recent studies [16] show that users are sensitive about sharing their location in the services. Hence, the privacy issue in location-sharing based service should be addressed.

Identity protection and *data protection* are required in order to achieve location privacy. The aim of identity protection is to avoid revealing the identity of anonymous users. The aim of data protection is to avoid the disclosure of their personal data. Both non-cryptographic and cryptographic approaches can be applied to provide identity protection and data protection.

k-anonymity [8,14] is a non-cryptographic approach to hide user identity where the user identity is indistinguishable with at least $k - 1$ other identities. Many cryptographic approaches, e.g. ring signature [3] and blind signature [6], can also be used to hide user's identity.

Two traditional approaches employed to provide location data protection are location obfuscation [15] and cryptography based techniques [9]. The former assumes there is an obfuscator which serves as a mediator between the users and the location based server and replaces the client's location with a nearby location [7,11,12]. Location obfuscation offers weak privacy in the sense that the location based server always learns some information about the user's location. The mediator between the users and the location based server must be trusted, which is a strong assumption. Cryptography based techniques offer stronger location privacy [9]. Unfortunately, the protocols based on cryptographic techniques might not be practical due to high computational cost.

A specific application in location-sharing based service is *fair meeting location determination*, by which a set of users agree on an optimal and fair meeting location with the help of a service provider. "Fair" in this application means that the determined meeting location is fair to all users in the group. Bilogrevic, Jadliwala and Jonejah proposed a two-round privacy-preserving meeting location determination protocol [1], where the BGN encryption [2] is employed to protect user location privacy. Unfortunately, it requires two rounds of communication, and needs heavy computation. As all the group users shared one pair of public and private keys in their protocol, if a group user is dishonest, he is able to learn other users'locations by decrypting their messages transmitted to the Location Determination Server (LDS). Therefore, their protocol does not meet their security goal of location privacy against the internal attackers.

As users in the application are equipped with resource constrained mobile devices, e.g., smartphones, efficiency is an important concern in the optimal fair meeting location determination protocol. In order to enhance the efficiency of the protocol, we introduce a mediator to our design. This method has also been utilized in the obfuscation based protocols [7,11,12]. However, the mediator in our protocol serves as an untrusted computation center, which is a cloud server with unlimited computation resources. In this paper, we also address the problem of location privacy in the application of *Fair Meeting Point Determination* against the Computation Center (CC), the Meeting Location Determination Server (MLDS) and other group users. We propose a practical privacy-preserving meeting location determination protocol for resource constrained devices. Our contributions are illustrated with the following four aspects.

- Firstly, we construct a one-round fair meeting location determination (ORFMLD) protocol among a group of users. The fair meeting location is determined with the help of the CC and the MLDS. In our protocol, the group users'location privacy is protected against the internal attacks mounted by the semi-trusted group users, the CC and the MLDS.
- Secondly, we propose a security model where the location privacy properties of identity indistinguishability (which covers the user's preferred location privacy), meeting location indistinguishability (which covers the users'meeting location privacy) and distance indistinguishability (which covers the users'distance privacy) against four types of adversaries, namely the outside adversary, the semi-trusted CC, the semi-trusted MLDS, and the semi-trusted user, are formally defined.
- Thirdly, we formally prove the identity indistinguishability and the meeting location indistinguishability of our protocol against the semi-trusted CC and the semi-trusted MLDS, and the identity indistinguishability and the distance indistinguishability of our protocol against the semi-trusted user.
- Fourthly, from the simulation results we find that our protocol is efficient as the user's computation cost is constant with the number of users take part in the protocol. Differing from Bilogrevic, Jadliwala and Jonejah's two-round protocol [1], our protocol only needs one round communication and less computation and communication cost, while provides stronger security protection, i.e. location privacy protection against internal attackers.

2. System model and problem formulation

2.1. System model

As shown in Fig. 1, a meeting location determination system consists of three types of participants: a group of users $U = \{u_1, u_2, \cdots, u_n\}$ who handle with smartphones, a Computation Center (*CC*) and a Meeting Location Determination Server (*MLDS*). The *CC* is a semi-trusted cloud server which has sufficient computation resources and provides computation services in the system. The *MLDS* is a third party location service provider which provides meeting location determination services to the users. In the system, each user in the group utilizes his mobile phone to communicate with the *CC* and the *MLDS*.

The users u_1, u_2, $\cdots$, u_n in the group want to decide a fair meeting location. Each user $u_i (i \in [1, \cdots, n])$ chooses his preferred meeting point $L_i = (x_i, y_i) \in N^2$ which is the coordinates of a point in a two-dimensional coordinate system. The locations L_1, L_2, $\cdots$, L_n are different from each other. The preferred location L_i chosen by u_i can be his current location or a