Computer Standards & Interfaces 44 (2016) 102–109

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

An efficient and privacy-preserving location sharing mechanism

Nan Shen [a], Jun Yang [a], Ke Yuan [b], Chuan Fu [a], Chunfu Jia [a,*]

[a] College of Computer and Control Engineering, Nankai University, Tianjin, China
[b] School of Computer and Information Engineering, Henan University, Kaifeng, Henan, China

ARTICLE INFO

Article history:
Received 28 January 2015
Received in revised form 27 May 2015
Accepted 3 June 2015
Available online 11 June 2015

Keywords:
Mobile online social networks
Location sharing service
Privacy-preserving
The Bloom Filter

ABSTRACT

The rise of Internet of Things has been improving the so-called mobile Online Social Networks (mOSNs) in sense of more ubiquitous inter-communication and information sharing. Meanwhile, location sharing service is known as the key cornerstone of mOSNs. Unfortunately, location sharing has also caused similarly serious concerns on the potential privacy leakage. We propose *BMobishare*, a security enhanced privacy-preserving location sharing mechanism. It employs the Bloom Filter to mask sensitive data exchanges, such that exchange of both sides cannot obtain unauthorized privacy information. Analyses and evaluations show that BMobishare's enhanced location sharing procedure achieves significantly better performance when compared to existing approaches.

1. Introduction

The Internet of Things (IoT) integrates a large number of technologies and envisions a variety of things or objects, such as Radio Frequency IDentification (RFID) tags, sensors, mobile phones around us. Through unique addressing schemes, they are able to interact with each others and cooperate with their neighbors to reach common goals [1]. In combination with IoT, a new mode of the social networks services known as the *mobile Online Social Networks* or mOSNs, have gradually emerged, in which IoT is to enable more convenient user interactions for either maintaining or establishing social relationships. For example, RFID technique can be used for automatic updating of people's social activities in applications such as Twitter [2].

Compared with the traditional social network, mOSNs are not restricted by time or location, as mobile devices are capable of accessing the Internet over WiFi or cellular networks in real time. Since mOSNs can break the boundaries of time and space, no matter when and where they are, people can communicate with their friends in social networks [3].

The mOSNs service consists of two parts, which support the location based services and the social network services. The location based services offer users the points of interest close to their locations such as restaurants, gas stations, shopping markets and social events. By now, instead of inputting locations done by users' themselves, smart phones and tablets can determine their own locations through GPS or cellular positioning technology. The mOSNs not only allow the user to share his location information by means of 'check-in' (which refers to an event when their time and location are recorded [4]), but also allow the user to use location sharing services to find their friends nearby [5]. With billions of people as members, mOSNs have pervaded all aspects of our daily life, gone beyond general social and information sharing platform, and become a kind of indispensable tool for our communication in work and life.

Location sharing is a fundamental component of mOSNs. However, with great convenience, it also inevitably raises significant privacy concerns [6]. This is because in mOSNs, location information is associated with user's social network identity information, which will make the protection of user's privacy information more and more complex and difficult. For example, it is likely that the user's location may give away the sensitive private information, such as the personal data, living habits and health conditions [7], especially at the time when they are in the control of the adversaries. Since the current mOSNs are under centralized control, the users' location privacy data will be compromised if the location information collected by mOSNs are inadvertently leaked or under the control of malicious attackers [8]. Therefore, how to enjoy convenient service without leaking their sensitive private information has become a more and more popular problem concerned by researchers. Previous researches have shown that the users tend to be hesitant to share their locations if privacy is not guaranteed sufficiently [9]. To address this issue, some researches have been conducted about hiding the relations between user identity and location, including location anonymity, identity anonymity and so on.

Anonymity has proved to be an effective technique for privacy protection. Its essence is to let mobile devices (or the trusted third party) process their queries in a way that conceals user's real identity and

* Corresponding author.
E-mail address: cfjia@nankai.edu.cn (C. Jia).

http://dx.doi.org/10.1016/j.csi.2015.06.001
0920-5489/

location, before sending the processed queries to service provider. There are at least two kinds of anonymous methods:

- *K*-anonymity, which is to obfuscate users' real location/identity by establishing cloaking regions covering the records of *k* anonymous users, which makes the attacker fail to tell which is true. It was Sweeney who proposed *K*-anonymity technology in 2002 [10], and Gruteser et al. [11] who firstly used it to locate privacy protection. In 2014, Lu et al. proposed a privacy-preserving framework, called PLAM [12], which employs an aggregation protocol with *K*-anonymity and *L*-diversity properties.
- Anonymous by encryption, which is considered to be the most effective means of privacy protection. For example, the encryption method based on Hilbert curves has been proposed by Khoshgozaran [13], who used Hilbert curves to transform original location to an encoded location. In addition, Rahman et al. [14] also proposed privacy context obfuscation which is used obscure information based on the parameters which the users themselves set, such as user identity, the time of day and so on.

In social network services, privacy protection must be flexible to sharing location. In 2007, SmokeScreen [15] put forward a mechanism with shares presence among trusted friends and untrusted strangers by opaque identities. The previous work [16] has resolved the problem of how to flexibly handle location sharing in a privacy-preserving way. Because of the strictness of the method, they can't be used directly. Recently, Wei et al. proposed the Mobishare mechanism [17] which provides flexible privacy-preserving location sharing among both trusted social relations and untrusted strangers in mOSNs. Their mechanism is in fact an extension of SmokeScreen and they used dummy technique (e.g. real fake identity) to prevent the location based services provider and the social network services provider from obtaining users' complete identities and locations information. Liu et al. made an improvement on the basis of Mobishare. They used the broadcast encryption to preserve users' location privacy and allowed the users to add or remove friends [18].

However, these mechanisms are not perfect enough. It is noted that in the aspect of location sharing among trusted social relations, the user's real fake identity will suffer a potential risk of leakage, especially when we consider many queries without location updates. The location based services provider is easy to identify which record is true. More seriously, through multiple attacks, the location based services provider is able to obtain all the friends' relations of users and their locations in real time. Li et al. used the Paillier Cryptosystem to solve this problem [19]. They proposed a security improved mechanism named Mobishare +, which employs private set intersection protocol to prevent the social network server and the location server from learning individual information. Although security has been improved, this scheme needs to perform a lot of complex encryption and decryption operations which incurs appreciably computation overhead. There are still other methods based on encryption and decryption operation and have also been applied to the privacy protection in cloud environment [20–22].

Motivated by the above issues, a further research was made on privacy-preserving location sharing on mOSNs and a new protection mechanism based on Mobishare, which is named BMobishare, was proposed. Actually, BMobishare is generally identical with Mobishare in system architecture. But compared with the previous mechanism, BMobishare uses dummy query information and allows us to protect user's real fake identity. Moreover, the Bloom Filter [23] between the location based service provider and the social network service provider is also employed, which hides sensitive private information and ensure that nothing individual will be leaked to each other. Finally, analysis and evaluations were provided to attest that BMobishare can make the information processing more secure and effective.

2. Problem statement

2.1. Location sharing: system architecture

As shown in Fig. 1, the scenario of location sharing consists of four entities in mobile online network. A summary of the notations used in this scenario is given in Table 1.

1. User is able to access the Internet with wireless techniques such as 3G/4G by using his mobile devices. As a result, user can share his own location and query nearby his friends' locations.
2. SNS can be a server of any existing mOSNs that want to provide the location sharing service. It manages user's identity-related information, e.g. user's personal profiles and friend-list, etc.
3. LBS is able to store user's anonymized location update information and provides location based services according to users' request with nearby persons' locations in real time.
4. CT is an entity, which helps user communicate with SNS and LBS. The wireless enhanced rules of the Federal Communications Commission (FCC) require that a cellular tower can locate the subscribed mobile phones with an accuracy of 300 m.

We assume that LBS, SNS and CT are connected through high-speed secure links. SNS can't identify the communicating CT by observing the IP addresses in the connections.

2.2. System workflows

Based on the proposed system architecture, there are four main workflows described as following:

1. User firstly needs to register his profile for the location based service at the SNS and local CT. We assume that each user has a unique identifier at the SNS. Each CT has a unique identifier too. During registration, user must define his access control policy for his shared location, which will be stored at SNS.
2. Occasionally, or when arriving at a new place, user updates his location information at LBS through SNS.
3. User queries LBS and SNS through local CT when he wants to know his nearby friends' current location information. Through a series of processing, user will receive the locations of friends whose specified access control policy is satisfied by the querying user.
4. User queries LBS and SNS through local CT, when he wants to know nearby strangers' current location information. Through a series of processing, user will receive the locations of some strangers whose specified access control policy is satisfied by the querying user.

We formalize location sharing system in mobile online social network as follows:

Let us suppose that $\Phi = \{ID_1, ID_2, \ldots, ID_n\}$ to be the identity set of all the registered users involved in the location sharing service. SNS stores all social relation networks $\Psi = (V, E)$ on Φ, where $V \subseteq \Phi$ is an identity point set and $E \subseteq V \times V$ is a set of relationship as edges in Ψ. Without privacy concerns, we consider that a location database in the form of $\{(ID, (x, y), df_{ID}, ds_{ID})\}_{ID \in \Phi}$ is stored by LBS, where (x, y) is the user's current location coordinates, df_{ID} is the threshold distance within which user agrees to share location with his friends, and ds_{ID} is the threshold distance within which user is willing to share location with strangers.

The main challenge is to query the current location information of friends or strangers in certain ranges.

- To query friends' location within a certain range *qf*, an authorized user *A* will submit a query in the form of (ID_A, qf) to obtain all user *A*'s nearby friends' locations $\{(ID_i, (x_i, y_i))\}$ satisfying the conditions $(ID_A, ID_i) \in \Psi$. *E* and $dist((x_A, y_A), (x_i, y_i)) \leqslant min(qf, df_i)$, where (x_A, y_A) is user *A*'s current location, $dist(.,.)$ returns the distance between the its inputs and $min(.,.)$ is a minimum value function.