Contents lists available at ScienceDirect

Future Generation Computer Systems

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

The flexible and privacy-preserving proximity detection in mobile social network

Ayong Ye*, Qiuling Chen, Li Xu, Wei Wu

Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou, 350007, China

HIGHLIGHTS

- A proximity detection method based on the transfer of neighbor relation is proposed.
- The method takes beacon signals as a reference of neighbor discovery.
- The users whose nearby reference lists have a common item are neighbors.
- Two ways of transmitting signals of beacon nodes are proposed.
- The energy loss and the rate of signal coverage should be well controlled.

ARTICLE INFO

Article history:
Received 28 August 2016
Received in revised form
30 October 2016
Accepted 9 December 2016
Available online xxxx

Keywords:
Mobile social network
Proximity detection
Location privacy

ABSTRACT

With the popularity of mobile social network, proximity detection has become a fundamental service. For the traditional proximity detection methods, users need to upload their locations to a location server so that they can find their neighbors by calculating relative distances among them. It will cause significant privacy concerns when the location server is an untrusted one. To solve this problem, we propose a proximity detection method which is based on the transfer of neighbor relation. Specifically, each request user in our paper only needs to submit a nearby reference list to the social network server (SNS). After that, the SNS searches the neighbors of the request user by judging whether their nearby reference lists have a common item. Moreover, we present two mechanisms to determine the ways of transmitting signals of beacon nodes, i.e., Beacon Node Rotating Mechanism and Beacon Node Competition Mechanism, respectively. Besides, we experimentally demonstrate the effectiveness and feasibility of the proposed method.

1. Introduction

Driven by the rapid development of mobile Internet and social networks [1], the representatives of the social network sites like Facebook [2] and Twitter [3,4] grow fast. And the number of users is growing at an alarming rate. Nowadays, more and more users use the proximity detection service such as "people in the vicinity", "nearby restaurants", which make the proximity detection becomes a basic service in mobile social network. The traditional proximity detection methods require users to submit their location information to the location server in order to find their neighbors. This approach is unsafe when the location server is an untrusted one. For instance, if the location server has security vulnerability or the insider abuses users' location information, the location privacy of users will be disclosed.

In order to solve the problems of traditional proximity detection methods, we propose a novel privacy-preserving proximity detection method. Specifically, instead of using users' locations to find their neighbors, the proposed method takes beacon signals as a reference of neighbor discovery. More specifically, users can find their neighbors by determining whether users' nearby reference lists have a common item. In addition, we also present two distributed mechanisms – Beacon Node Rotating Mechanism and Beacon Node Competition Mechanism – to determine the ways of transmitting signals of beacon nodes. Specifically, in the presented mechanisms, each mobile user upgrades and services as a beacon node. For facilitating other users to find their neighbors, these beacon nodes send beacon signals (i.e., the references) periodically.

The main contributions of this paper can be summarized as follows:

* Corresponding author.
E-mail addresses: yay@fjnu.edu.cn (A. Ye), 695568779@qq.com (Q. Chen), xuli@fjnu.edu.cn (L. Xu), weiwu81@gmail.com (W. Wu).

http://dx.doi.org/10.1016/j.future.2016.12.012
0167-739X/© 2016 Published by Elsevier B.V.

(1) We propose a novel proximity detection method which is based on the transfer of neighbor relation. The SNS searches the neighbors of request user by judging whether their nearby reference lists have a common item.
(2) We present two mechanisms, i.e., Beacon Node Rotating Mechanism and Beacon Node Competition Mechanism, to determine the ways of transmitting signals of beacon nodes. Specifically, each mobile user in these mechanisms acts as a beacon node and periodically sends out a beacon signal as a neighbor discovery reference to other users.

The rest of this paper is organized as follows. Related works are reviewed in the next section. In Section 3, we present the overall scheme and the principle of the new proximity detection method. Besides, we also introduce the detailed process of algorithm to quickly match nearby reference lists. Moreover, the Beacon Rotating Mechanism and Beacon Node Competition Mechanism are the two methods for mobile users to send a beacon signal. We also introduce the process of these two mechanisms, respectively. The security analysis and discussions are presented in Section 4. The experimental results are presented in Section 5. Section 6 concludes this paper and presents the future work.

2. Related work

2.1. Location privacy protection method in LBS

In recent years, the main techniques to preserve location privacy in Location Based Services (LBS) are as follows.

Beresford in [5] proposed a conception of "Mix Zone" to hide all users' locations. Specifically, users in the mix zone have no need to communicate with each other. More specifically, when a user enters a mix zone, he changes his pseudonym and then gets out the mix zone. It is difficult for LBS to know who the user is when the user obtains a new pseudonym and goes out of the mix zone.

Gruteser et al. [6] first introduced k-anonymity into location privacy. It meets location k-anonymity when the location of a mobile user cannot be distinguished from other $k-1$ users. This method protects the location privacy by sending a minimum cloaking region which contains at least k users to the LBS instead of sending a single user's exact location. In this method, a trusted third-party is employed to generate these minimum cloaking regions through collecting the locations of different mobile users.

Spatial cloaking method can be employed to reduce the accuracy of location information and protect location privacy. For example, Ardagna presented a typical spatial cloaking method in [7]: the user sends a circle region to LBS instead of an exact location. However, due to the reason that the LBS cannot obtain the exact locations of users, its service quality will decrease.

The above methods are ineffective in the mobile social network. For instance, an attacker can obtain the location information or non-location information of users through the variety ways. Taking advantage of this information, the attacker can directly or indirectly reconstruct the location privacy of those users.

2.2. The proximity detection method

In order to provide proximity detection service on mobile social network without exposing user's location information, researchers have proposed numerous solutions. To the best of our knowledge, they can be categorized in four main classes: grid dividing, location tags, location anonymity and encryption method.

(1) The proximity detection based on grid dividing

In 2009, Šikšnys et al. in [8] proposed a method "grid-and-hashing", which divides space into a uniform grid unit (cell), and the ID of unit that each user located in has irreversibly hashed before sending them to the location server. In this manner, the server cannot get any location information about users when it is detecting proximity. However, due to the division of grid is pre-specified, this method exists false negative results, namely although two mobile users are close to each other, they are divided into different cells. As a result, they generate different hash values and submit the values to the server. For this reason, a "grid overlay" technology was designed in [9]; each user has a corresponding hash vector by using a series of interlocking grids. It indicates that two users are neighbors if they have a same hash result in a particular vector dimension. In this method, the layout and placing of grid will have a significant impact on reducing false negative rate. Vicinity Locator, is addressed in [10], makes users specify their areas of interest named "vicinity region". This region can be flexibly changed on the fly. One user's friends are the user's neighbors only when they are in the region. In [11], this "vicinity region" is centered on the false location generated by using differential privacy techniques, which can avoid location exposure.

Zhuo et al. [12] presented another proximity detection based on grid dividing. Each user can define his privacy region and two users are neighbors only when their privacy regions have an intersection. Moreover, this method supports users to verify the correctness of proximity test results from the server.

(2) The proximity detection based on location tags

Refs. [13–15] proposed proximity detection methods based on location tags. The spatial–temporal location tags, which are constructed from radio signals captured in a device's surrounding environment, such as WiFi and LTE signals. An attacker cannot forge a location tag if she is not at the corresponding location and time, due to the high freshness (entropy) and spatial variety of environmental signals. The location tags can resist location cheating for malicious users, but there exist some difficulties to construct a suitable location tag.

(3) The proximity detection based on location anonymity

Location anonymity is a location privacy protection method of most proximity detections adopted. Ruppel et al. [16] applied a distance-preserving mapping to transform the user's location q into a location q'. After the transformation, a centralized proximity detection method is presented to detect the proximity among the transformed locations. Nevertheless, Liu et al. in [17] pointed out that such distance preserving mapping is not secure. An outside attacker can easily derive the secret mapping function and recover the original location of users. Hide & Crypt is a privacy-preserving method to achieve proximity detection by taking a filter-and-refine two-phase procedure [18]. In the first phase of [18], all users cloak their locations before sending them to the server. In the second phase, the server computes the minimum and maximum distances between these cloaking regions. The server classifies users' friends being in, not-in, or possibly-in proximity according to the specified thresholds and the computed distances.

(4) The proximity detection based on encryption method

Currently, many privacy-preserving proximity detections based on encryption have been presented. For example, Refs. [19,20] presented a proximity detection method based on homomorphic encryption, respectively. According to the characteristics of homomorphic encryption, the user sends location ciphertexts to the request user. The distance between them can be computed homomorphically without exposing the location of the user.

The above methods can protect the users' location privacy, but there exists some problem, for example, the implementation of encryption method is expensive and the construction of location tag is difficult. Unlike these methods, our new method is simple and effective. It only needs to match the nearby reference lists of request users. Namely, users in our method can find their neighbors without using the location information of them.