Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 129 (2018) 368–371

Procedia Computer Science

www.elsevier.com/locate/procedia

2017 International Conference on Identification, Information and Knowledge in the Internet of Things

A Location Privacy Preserving Scheme Based on Repartitioning Anonymous Region in Mobile Social Network

Lina Ni[a,b], Yanfeng Yuan[a], Xiao Wang[a], Mengmeng Zhang[a], Jinquan Zhang[a,*]

[a] *College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, China*

[b] *The Key Laboratory of Embedded System and Service Computing, Ministry of Education, Tongji University, Shanghai, China*

Abstract

Applying the proliferated location-based services (LBS) to social networks has spawned mobile social network (MSN) services that it allows users to discover potential friends around them. In this paper, we focus on the problem of location privacy preserving in MSN. Particularly, we propose a location privacy preserving (RPAR) scheme via to repartition anonymous region where the central anonymous location minimizes the traffic between the anonymous server and the LBS server while protecting the privacy of the user location.

Selection and peer-review under responsibility of the scientific committee of the 2017 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2017).

Keywords:
Privacy preserving; mobile social network; location-based service; location privacy; anonymous region repartition.

1. Introduction

Internet of Things (IoT), a trend of future networks, is immersing into many aspects of our personal and working life, it also provides more comprehensive intelligent service. Social networks used widely in mobile Internet catalyze mobile social networks (MSN), and users in MSN can not only acquire their own location information and sign in a location but also find nearby friends, access to location-based services (LBS) such as finding the nearest hotel, finding directions, sharing action tracks, and so on [1, 2, 3, 4, 5, 6]. However, when we enjoy the convenience of LBS and MSN services, the mobile users also confront with the risk of location disclosure, which is a severe privacy preserving concern [7, 8, 9, 10].

Recently, research on the privacy protection technology based on location-based services (LBS) has attracted considerable interest. [11, 12, 13, 14, 15]. Besides the above described location privacy preserving technologies, there are

[*] Corresponding author. Tel.: +86-532-86057126 ; fax: +86-532-86057126.
E-mail address: nln2004@163.com, 382334224@qq.com, waxi2016@163.com, tinydeemon@163.com, tjzhangjinquan@126.com

Selection and peer-review under responsibility of the scientific committee of the 2017 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2017).
10.1016/j.procs.2018.03.091

a wealth of methods such as location data randomization [16, 17], fuzzification of space or time data [18], methods based on strategies and encryption [19], sensitive semantic based security anonymity mechanism [20, 21]

In this paper, we focus on the location privacy preserving in MSN aiming at larger communication overhead, larger range and inaccuracy of query results for traditional anonymous schemes.

2. System Model

As shown in Fig. 1, the principles of the model are as follows:

1. When the user requests the location query service, all the query contents, location information and parameters needed to be set are sent to the central anonymous servers.
2. After receiving the query information sent by users, according to certain rules, the central anonymous servers will generate an anonymous user set which meets the requirements, figure out the number of sub-anonymity regions and then partition them, a few scattered sub-anonymity regions are yielded. When the sub-anonymity regions meet the requirements, its central location is computed to replace corresponding sub-anonymity regions to send requests to the LBS server.
3. The LBS server handles the query information sent by the central anonymous servers and returns the query results.
4. After the refinement process, the central anonymous servers return the corresponding results to the users.

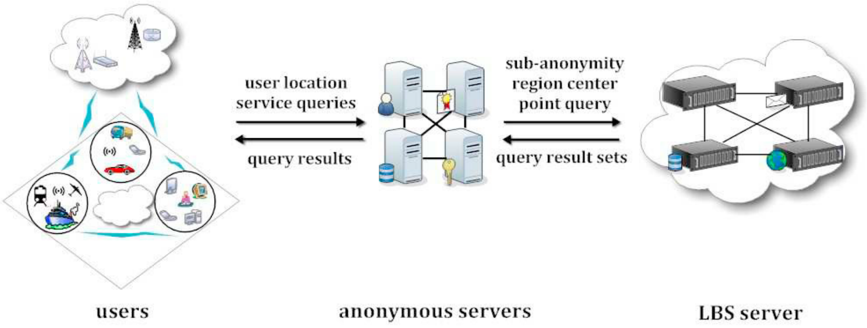

Fig. 1. Architecture of our system model.

3. Location Repartitioning Anonymous Region Scheme

Combined with Fig. 2 (a) and (b), the basic idea of RPAR scheme is elaborated as follows:

1. The solid red dots represent the users initiating query who find $k-1$ users with whom the query users can form k-anonymity regions according to the *nearest neighbor principle*, and k users information set is recorded. It can be seen in Fig. 2 that k=14.
2. According to the parameter n, the number of sub-anonymity regions, the k users are divided into n sub-anonymity regions, so the number of users each sub-anonymity region contains is $k'=k/n$=4. The mobile users (red dots) are as the *center* to search other nearest $k'-1$ users and form the first sub-anonymity region.
3. A user from the rest of the users which is not in the first sub-anonymity region is randomly selected as the *central point*. According to the *nearest neighbor principle*, the sub-anonymity regions are formed with the user and other 3 users who is not the first sub-region form anonymous region, until the rest user number is 0 or below k'.
4. The *tail anonymity user set* is repartitioned into other sub-anonymity regions according to the *nearest neighbor principle*, and the sub-anonymity regions are updated.