Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

# Enhancing privacy through uniform grid and caching in location-based services☆

Shaobo Zhang [a,e], Kim-Kwang Raymond Choo [b], Qin Liu [d], Guojun Wang [c,*]

[a] School of Information Science and Engineering, Central South University, Changsha, 410083, China
[b] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA
[c] School of Computer Science and Educational Software, Guangzhou University, Guangzhou, 510006, China
[d] College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China
[e] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China

## HIGHLIGHTS

- We present a novel UGC scheme to enhance location privacy in LBSs.
- We utilize the *k*-anonymity principle to improve the user's location privacy.
- We design the matching and comparison mechanism based on coordinates and identifiers.
- We employ the uniform grid structure and caching to improve users' privacy.

## ARTICLE INFO

*Article history:*
Received 19 September 2016
Received in revised form 1 June 2017
Accepted 13 June 2017
Available online xxxx

*Keywords:*
Location privacy
Uniform grid
Caching
Order-preserving symmetric encryption (OPSE)
*k*-anonymity

## ABSTRACT

With the increasing popularity of location-based services (LBSs), there is a corresponding increase in the potential for location privacy leakage. Existing solutions generally introduce a fully-trusted third party between the users and the location service provider (LSP). However, such an approach offers limited privacy guarantees and incurs high communication overhead. Specifically, once a fully-trusted third party is compromised, user information would likely be exposed. In this paper, we propose a solution designed to enhance location privacy in LBSs. Our scheme is based on the uniform grid, and adopts both order-preserving symmetric encryption (OPSE) and *k*-anonymity technique. Thus, the anonymizer knows nothing about a user's real location, and it can only implement simple matching and comparison operations. In our approach, we also employ an entity (hereafter referred to as the converter) to transform the user-defined grid structure into the uniform grid structure. This combined with the caching mechanism, allow us to avoid repeated queries from different users on the same query spatial region and consequently, reduce the overhead of the LBS server. The analysis and simulation results demonstrate that our proposal can effectively preserve a user's location privacy, with reduced overheads at the anonymizer and the LBS server.



## 1. Introduction

With the rapid developments of wireless communication, positioning technologies and mobile devices, location-based services (LBSs) have been gaining traction among consumers in recent years [1–3]. In LBSs, a user can obtain his/her current location from the built-in GPS feature in smartphones (e.g. Android and iOS devices), prior to sending a query that contains his location to the LBS server. This allows the LBS server to return points of interests (POIs) near of the user (e.g. restaurants in the vicinity, available taxi services, and obtaining just-in-time coupons). However, the associated potential privacy risks may outweigh the benefits. For example, after compromising a LBS server successfully, an adversary can collect the queries submitted to infer sensitive information about a particular user, such as the workplace, behavior patterns and profiles [4–6]. In addition, the LBS server may leak users' private information to a third-party for financial or other strategic advantage. Unsurprisingly, privacy-preserving in LBSs is a topic of active research.

To reduce the risk of privacy disclosure in LBSs, a number of approaches have been proposed to protect users' location privacy

☆ This is an extended version of the conference paper Zhang et al. (2016), with more than 70% new content.

* Corresponding author.
*E-mail addresses:* shaobozhang@csu.edu.cn (S. Zhang), raymond.choo@fulbrightmail.org (K.R. Choo), gracelq628@hnu.edu.cn (Q. Liu), csgjwang@gmail.com (G. Wang).

http://dx.doi.org/10.1016/j.future.2017.06.022
0167-739X/

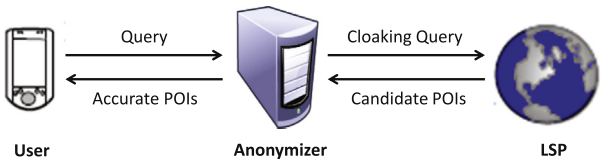


**Fig. 1.** A typical TTP architecture.

such as those based on trusted third-party (TTP) architecture. For example, Chow et al. [7] proposed a robust spatial cloaking algorithm using the fully-TTP model. In a typical TTP system architecture (see Fig. 1), the TTP (also known as the anonymizer) sits between the users and the location service provider (LSP). TTP is mainly tasked to record the exact location of all users and blur the exact location of a querying user into a cloaked region. Thus, the cloaked region includes at least $(k-1)$ other users, and the LSP is not able to distinguish a particular user from at least $(k-1)$ other users.

However, the approaches based on the TTP has three major drawbacks, namely:

1. All users need to constantly update their locations to the TTP, which records the exact location of every users. If the anonymizer is compromised by an attacker, then this will also expose user location information.
2. The anonymizer is the root cause of performance bottleneck, since all submitted queries are processed by this entity.
3. It is challenging to find a fully-trusted TTP, in practice.

To overcome the limitations of the TTP architecture, researchers have examined the potential for preserving user's location privacy based on a centralized architecture. Schlegel et al. [8] proposed a dynamic grid system (DGS) to preserve privacy in LBS. What their scheme requires is merely a semi-TTP, which does not know the exact location of the user. However, this work suffers from the following two limitations. When the user's query spatial region is too small and includes only one user, then the LSP can deduce the true user. In addition, when the same query spatial region is specified by other users with the same POIs and each user defines a different grid structure, then the LBS server will be repeatedly queried on the same query spatial region. This has significant impacts on the overhead of the LBS server's computation and communication.

Inspired by the work in [8], we propose an enhanced privacy through uniform grid and caching (UGC) scheme in LBSs to solve the known limitations. Specifically, our scheme adopts $k$-anonymity and order-preserving symmetric encryption (OPSE) technique, combined with the uniform grid structure and caching to preserve users' location privacy. When a user sends a query request, the user first looks for $(k-1)$ other users in his/her surroundings. Then, they specify a query spatial region respectively, and the two coordinates (which can determine every specified query spatial region) are encrypted using OPSE. Finally, the user forwards it to the anonymizer that forms a cloaked region, and sends it to the LBS server for query. In the query process, the anonymizer only performs some simple matching and comparison operations; thus, significantly reducing the computational overheads of the anonymizer. Moreover, the anonymizer does not know the specific location of each user. Therefore, this anonymizer is considered a semi-trusted entity. At the same time, by converting the user-defined grid structure into a uniform grid structure and combining with the caching mechanism, our scheme omits the need for repeated queries on the same query spatial region for different users. This reduces the overhead of the LBS server. This paper can be summarized as follows:

1. We present a novel UGC scheme to enhance location privacy in LBSs. In our scheme, each user specifies a query spatial region on the uniform grid structure, which will be encrypted using OPSE. Therefore, the anonymizer is not able to identify a user's specific location. This improves user location privacy on the anonymizer.
2. We utilize the $k$-anonymity principle to improve user location privacy on the LBS server. The user looks for $(k-1)$ other users around him/her on the client side, and a cloaked region that contains $k$ users is formed on the anonymizer. This complicates efforts to identify the real user's location; thus, improve the user's location privacy on the LBS server.
3. We design the matching and comparison mechanism based on the encrypted coordinates and identifiers. The anonymizer only carries out some simple matching and comparison operations, which can effectively avoid the performance bottleneck of anonymizer.
4. We employ caching techniques and combine with the uniform grid structure to reduce the mutual dependencies between the user and the LBS server. This allows us to improve the user's location privacy and reduce the overhead of the LBS server.

We will review related work in the next section, prior to providing an overview of our system architecture and definition in Section 3. In Sections 4 and 5, we describe our location privacy protection techniques and its security analysis, respectively. Next in Section 6, we evaluate the performance of the UGC scheme using simulations. Finally, we conclude this paper and outline future work in Section 7.

## 2. Related work

This section reviews existing privacy preserving techniques for LBSs, which can be broadly categorized into non-centralized architectures and centralized TTP architectures [9].

In the non-centralized architecture, users communicate with the LBS server directly without involving a TTP. Typically, the user blurs the location information to prevent the LBS server from recognizing his/her exact location, such as obfuscation methods and collaboration methods. The former is achieved mainly by adding noise to user's location or sending the fake locations to the LBS server. For example, Ardagna et al. [10] presented a obfuscation operators, where the location information is perturbed using sensing technologies to ensure the user's location privacy. However, the quality of service will degrade with the increase of the confusion degree. In collaboration methods, each user collects their location data to generate the cloak region. The communication channels between the users are secure, which can guarantee the user's data privacy with the cryptographic solutions [11–13]. For example, Shokri et al. [14] presented a scheme by collaboration of the users to exchange context information among the interested user, which allows a querying user to answer LBS queries from other user. However, users' interactions pose additional privacy risks in some cases. Generally, in non-centralized architecture, these approaches incur a high preprocessing overhead on the client. In addition, the redundant results returned from the LBS server also incur a high communication overhead between the user and the LBS server.

In a centralized TTP architecture, an anonymizer (a centralized entity) is introduced into the system to preserve the users' location privacy. The main function of the anonymizer is to construct a cloaking region that satisfied $k$-anonymity. The $k$-anonymity is one of the most popular metrics used in ensuring privacy for LBSs, and the LSP cannot distinguish between the location information of the user and the location information of other $(k-1)$ users (see [15,16]). For example, Ghinita et al. [17] proposed a reciprocal

Please cite this article in press as: S. Zhang, et al., Enhancing privacy through uniform grid and caching in location-based services, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.06.022.