IEEE Access February 2016

Dummy-Based User Location Anonymization Under Real-World Constraints

TAKAHIRO HARA[1], (Senior Member, IEEE), AKIYOSHI SUZUKI[2], MAYU IWATA[3], YUKI ARASE[1], AND XING XIE[4], (Senior Member, IEEE)

[1]Osaka University, Osaka 5650871, Japan
[2]Mizuho Bank, Ltd., Tokyo 1008176, Japan
[3]AI corporation, Kyoto 6190237, Japan
[4]Microsoft Research Asia, Beijing 100080, China

Corresponding author: T. Hara (hara@ist.osaka-u.ac.jp)

This work was supported in part by the Microsoft Research Core Project, in part by the Kurata Grant, in part by the Japan Science and Technology Agency through the Strategic International Collaborative Research Program, and in part by the Grant-in-Aid for Scientific Research within the Ministry of Education, Culture, Sports, Science and Technology, Japan, under Grant 2620013.

ABSTRACT According to the growth of mobile devices equipped with a GPS receiver, a variety of location-based services (LBSs) have been launched. Since location information may reveal private information, preserving location privacy has become a significant issue. Previous studies proposed methods to preserve a users' privacy; however, most of them do not take physical constraints into consideration. In this paper, we focus on such constraints and propose a location privacy preservation method that can be applicable to a real environment. In particular, our method anonymizes the user's location by generating dummies which we simulate to behave like real human. It also considers traceability of the user's locations to quickly recover from an accidental reveal of the user's location. We conduct an experiment using five users' real GPS trajectories and compared our method with previous studies. The results show that our method ensures to anonymize the user's location within a pre-determined range. It also avoids fixing the relative positions of the user and dummies, which may give a hint for an LBS provider to identify the real user. In addition, we conducted a user experiment with 22 participants to evaluate the robustness of our method against humans. We asked participants to observe movements of a user and dummies and try to find the real user. As a result, we confirmed that our method can anonymize the users' locations even against human's observation.

INDEX TERMS Location-based service, pervasive computing, privacy.

I. INTRODUCTION

According to growing popularity of mobile devices equipped with a GPS receiver, location based services (LBSs) are getting popular. LBS providers offer a variety of services based on a user's location information, such as local search, route planning, and location based advertisement. However, location information provides, or enables to infer, a lot of private information, e.g., where an LBS user lives, to which school his/her children go, where his/her friends live, etc. Krumm [17] warns about this problem. His experiment shows that only using the last location of a day, it is possible to estimate a user's home location within the range of 60 meter errors. The situation is more serious when the user continuously uses an LBS, such as searching near-by attractions during hanging around a city, since his/her accumulated location histories make private location detection easier. According to the investigation conducted by Busic and Filjar [7], most of commercial LBSs require us to update our position every a few minutes. Beresford and Stajano [3] defined location privacy as the ability to prevent other parties from learning one's current or past location. They also warn that a system collecting users' locations potentially invade their location privacy.

To preserve users' location privacy, a lot of studies have been conducted. There are two requirements to deploy a system to preserve users' location privacy [24]: 1) it should be a closed system, i.e., being executable on the user's mobile device, not to leak the user's location information outside and 2) it should not disturb benefits of the user and LBSs. The second requirement is important to have the entire ecosystem beneficial, otherwise, no users and LBSs would use the privacy preservation system. Among the previous studies, dummy-based methods [16], [20], [26] satisfy these requirements. They generate dummy users and send their locations