Author's Accepted Manuscript

User-Defined Privacy Location-Sharing System in Mobile Online Social Networks

Gang Sun, Yuxia Xie, Dan Liao, Hongfang Yu, Victor Chang

www.elsevier.com/locate/jnca

Cite this article as: Gang Sun, Yuxia Xie, Dan Liao, Hongfang Yu and Victor Chang, User-Defined Privacy Location-Sharing System in Mobile Online Social Networks, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2016.11.024

User-Defined Privacy Location-Sharing System in Mobile Online Social Networks

Gang Sun[1,2], Yuxia Xie[1], Dan Liao[1,3], Hongfang Yu[1,2], Victor Chang[4]

[1]Key Lab of Optical Fiber Sensing and Communications (Ministry of Education), University of Electronic Science and Technology of China, Chengdu, China
[2]Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu, China
[3]Guangdong Institute of Electronic and Information Engineering, UESTC, China
[4]Xi'an Jiaotong Liverpool University, Suzhou, China

Abstract
With the fusion of social networks and location-based services, location sharing is one of the most important services in mobile online social networks (mOSNs). In location-sharing services, users have to provide their location information to service provider. However, location information is sensitive to users, which may cause a privacy-preserving issue needs to be solved. In the existing research, location-sharing services, such as friends' query, does not consider the attacks from friends. In fact, a user may not trust all of his/her friends, so just a part of his/her friends will be allowed to obtain the user's location information. In addition, users' location privacy and social network privacy should be guaranteed. In order to solve the above problems, we propose a new architecture and a new scheme called User-Defined Privacy Location-Sharing (UDPLS) system for mOSNs. In our scheme, the query time is almost irrelevant to the number of friends. We also evaluate the performance and validate the correctness of our proposed algorithm through extensive simulations.

Key words: Location privacy; Mobile online social networks; Friend attacks; Anonymity; Location sharing

1. INTRODUCTION

Location-based services employ GPS, WLAN, Cellular network technologies to obtain location information of the mobile terminal, and to provide location-based services to the mobile terminal through the wireless network [1]. Due to the development of Internet technology, the well-known dominant mOSNs such as Facebook, YouTube, Twitter have been growing rapidly in both of size and popularity. In these traditional online social networks, users can conveniently exchange information, and share blog, video, images, etc.

When mOSNs and location-based services are integrated together, many location-based services such as near friends' query, "check-in", and simple location sharing can be provided by mOSNs. For example, users can get some preferential service through "check-in" services. In addition, users can query their friends and strangers which close to the current position and obtain their location information. After Facebook integrated with location-based services, they attract a large number of users from starting operations, and the number of users is still growing rapidly [2].

Location-based service (LBS) is one of the most important components in mOSNs, which provides services to users based on the geographical position of the mobile device. With mobility and ever-present Internet connectivity of the world, a great amount of users take the advantage of LBS to query information based on their location. In LBS, users can query the near hospitals, supermarkets, bars and so on, which provides users much convenience.

As LBSs and mOSNs grow in popularity, many new services are spawned, such as friends and travel routes recommendation. However, there are also some challenges need to be solved. Location information is one of the most sensitive privacies to users, and thus it is very valuable. For example, if mOSNs collect users' much location information, they may provide it to third parties since the commercial purpose, which will leak users' location privacy. In addition, much sensitive information can be inferred from location information, when more sophisticated analysis is employed. For example, attackers may deduce that the user's physical health from the data of in hospital. Also, attackers may infer that a user is a drunkard, if the user frequently query the nearest bars.

It is important that keep personal location information from being obtained by malicious attackers. Location privacy includes published time of location information, the spatial location and location service request content. Especially, spatial location is most concerned issue of location privacy in mOSNs. Users' geographical location information mainly relate to the spatial location, which is one of the main concern of this paper.

In mOSNs, the query from friend or stranger in the user-specified range is a typical application of location sharing services. Location-based social networking systems with location sharing services rely on a central server that can obtain all users' detail movement profile, which raises privacy concerns [3-5]. If users' location privacy is not well protected, users are likely