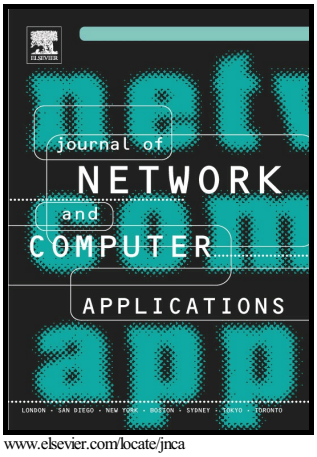
SocialHide: A Generic Distributed Framework for Location Privacy Protection

Ren-Hung Hwang, Yu-Ling Hsueh, Jang-Jiin Wu, Fu-Hui Huang



www.elsevier.com/locate/jnca

PII: S1084-8045(16)30215-6
DOI: http://dx.doi.org/10.1016/j.jnca.2016.09.009
Reference: YJNCA1721

To appear in: *Journal of Network and Computer Applications*

Received date: 1 February 2016
Revised date: 18 May 2016
Accepted date: 16 September 2016

Cite this article as: Ren-Hung Hwang, Yu-Ling Hsueh, Jang-Jiin Wu and Fu-Hu Huang, SocialHide: A Generic Distributed Framework for Location Privacy Protection, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2016.09.009

SocialHide: A Generic Distributed Framework for Location Privacy Protection

Ren-Hung Hwang, Yu-Ling Hsueh, Jang-Jiin Wu, and Fu-Hui Huang
Dept. of Computer Science & Information Engineering, National Chung Cheng University, Taiwan
{rhhwang@cs.ccu.edu.tw, hsueh@cs.ccu.edu.tw, jangjiin@gmail.com, smallq7997@gmail.com}

Abstract

Location-based services (LBS) have become one of the most popular smartphone applications, as smartphones are able to connect to the Internet and are equipped with the Global Positioning System (GPS). Since LBS queries include the query location of mobile users, it raises a privacy concern about exposing the locations of query issuers. In the literature, a centralized architecture which consists of a trusted anonymity server is widely adopted. However, this approach exhibits several apparent weaknesses, such as single point of failure, performance bottlenecks, and serious security threats. Furthermore, the anonymity server as an intermediate component between the query issuers and an LBS server is not necessarily trusted by the users. In this paper, we propose a generic distributed framework (*SocialHide* for short) based on the unique structure of Peer-to-Peer systems and the trust relationship retrieved from the social networks to support LBS queries for any approaches that utilize global user information for privacy protection purpose, such as constructing cloaked regions for location obfuscation. In *SocialHide*, a user can maintain his/her own location information and decide which friends to trust such that the protection of location privacy can be achieved without involving a third-party, trusted anonymous server. We use the K-anonymity spatial region as an application example to this novel framework. We evaluate the performance of the proposed architecture based on both a real world social network as well as a synthetic small-world social relationship dataset. Our experiment results confirm that our method achieves robust, decentralized strong privacy protection for LBS users.

Keywords: Location Privacy, Location Based Service, Distributed Anonymity Server Architecture, Peer-to-Peer, and Social Networking.