Decentralized Privacy Protection Strategies for Location-based Services

Chih-Chun Chen
Dept. of Computer Science and Information Engineering, National Chung Cheng University, Taiwan
ccc100m@cs.ccu.edu.tw

Yu-Ling Hsueh
Dept. of Computer Science and Information Engineering, National Chung Cheng University, Taiwan
hsueh@cs.ccu.edu.tw

ABSTRACT

The rapid development of the integration of cloud computing and location-based services have drawn so much attention currently. With the increasing number of users who own smart phones, significant amount of data that describe user surrounding information and interests have become widely available. However, significant attentions have been raised on the privacy issues. The existing approaches mainly focus on a centralized approach which brings tremendous security concerns. To prevent a centralized query processor from being attached by malicious hackers, we propose a decentralized approach to protect the sensitive location information of users who request for location-based services. Our system provides an approximate computing and an exact computing mechanism for different scenarios and requirements.

1. INTRODUCTION

In recent years, a dramatic growth of the location-based services has reduced the cost of sharing and obtaining information exchanges about individuals and yet it raises a lot of attentions on the privacy issues, which include the sensitive geographical locations of users and personal identity information. The existing approaches [1, 3] for continuous queries still have unresolved issues about location privacy. These work [2] mainly focuses on a centralized approach that adopts a query processor (also termed as a LBS provider) which brings a lot of security concerns, because a single LBS provider is very likely to be hacked by malicious users. In some cases, a LBS provider can be regarded as a malicious observer. In this work, we propose a decentralized privacy protection mechanism with k-anonymity and dummy techniques to further improve the security robustness by utilizing multiple LBS providers, each of which has been assigned a partial cloaked region which contains k users including the actual query user.

2. DECENTRALIZED PRIVACY PROTECTION

For the system assumptions, we assume that there are clients that issue search requests to a dispatcher, which obfuscates a user location to several cloaked regions. For designing the obfuscation mechanisms, we construct a grid on the cloaked region. Subsequently, we convert each grid cell of the cloaked region into a Hilbert value by using the Hilbert curve. After the transformation, we use the Hilbert values as index keys to determine multiple groups of subregions and each group of subregions are sent to a specified service provider. A dispatcher must verify that each of cloaked regions contains adequate privacy protection, which is configured by a user on a privacy profile. The concept of the decentralized obfuscation is shown in Figure 1. Next, each service provider searches for a candidate data set to retrieve the query results. Finally, the dispatcher filters and transmits the search results to users. The data owner provides public data sets stored in database repositories.

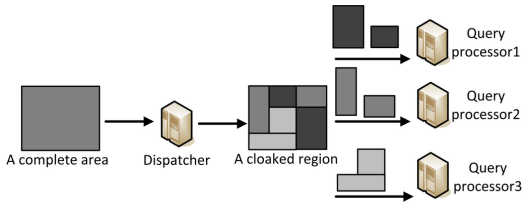

Figure 1: The concept of decentralized obfuscation.

In this work, we emphasize on four enhanced location privacy protection strategies. First, we propose a novel decentralized mechanism for a strong privacy protection. Because multiple LBS providers are adopted in our system and each service provider only obtains a partial cloaked region sending from a user, the level of the privacy protection is improved. Furthermore, such an distributed architecture enables a robust and scalable system, which is able to process big data. Second, we design a obfuscation method to generate a cloaked region to blur a user's actual position. The cloaked region is then divided into several subregions which are dispatched to the multiple LBS providers for inquiring the search results of continuous queries. Third, our system supports an approximate computing that efficiently obtains search results from the LBSs and an exact computing that retrieves the search results without losing accuracy. The trade-off analysis between efficiency and accuracy is studied. Fourth, we design an integrity check for the correctness of the search results for the query user.

Acknowledgments

This research has been funded in part by the National Science Council under the Grants NSC101-2221-E-194-054 and NCS102-2221-E-194-030-MY2.

3. REFERENCES

[1] H. Lee, B.-S. Oh, H.-I. Kim, and J.-W. Chang. Grid-based cloaking area creation scheme supporting continuous location-based services. In *SAC*, pages 537–543, 2012.

[2] K. Shin, X. Ju, Z. Chen, and X. Hu. Privacy protection for users of location-based services. In *Wireless Communications, IEEE*, pages 30–39, 2012.

[3] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux. Unraveling an old cloak: k-anonymity for location privacy. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, WPES '10, pages 115–118, New York, NY, USA, 2010. ACM.