# MASTER'S THESIS

## Towards practical location systems with privacy protection

Chen, Zhuo

*Date of Award:*
2015

CHEN Zhuo
Hong Kong Baptist University

Master of Philosophy
September 2015

# Towards Practical Location Systems with Privacy Protection

## Abstract

With the rapid growth of mobile, ubiquitous and wearable computing, location-based services become an indispensable part of mobile internet. These services rely on the geographical position of the mobile devices and provide location-dependent contents or services to users, such as location-based instant messaging, POI browsing, map navigation, and location-based virtual reality games. Most existing systems implement these location-based services by always storing and transmitting raw, plaintext GPS coordinates. However, location information is arguably a private asset of individual user, and the disclosure of such information could lead to severe privacy disclosure of other even more sensitive information, such as religion, sexuality, medical condition, or political affiliation.

To address this issue, researchers have proposed a series of techniques to protect user location privacy against location-based service providers. However, it is challenging to apply these theoretical and sophisticated techniques

to practical location systems because of the computational or network overhead imposed on the mobile devices as well as the complexity of the secure protocols and algorithms for application developers. In this thesis, I will study two real-life privacy-preserving location systems and show how they can be adopted by developers with little security background. The first is outdoor proximity detection that determines whether two users (or a user and an object) are within a given distance threshold. This is a fundamental service in many geo-social or map services. For example, "People nearby" in Wechat and QQ interconnect users because of their locality and/or mutual interests in some topics, such as food and movies. The second is indoor location monitoring and tracking. Wearable devices such as smart watch and bracelets continually broadcast Bluetooth Low Energy signals, which can be easily captured by monitoring devices such as WiFi routers and Bluetooth scanners. As more and more wearable devices emerge, unauthorized monitoring and tracking by adversary becomes great privacy threats not only in the cyberworld, but also in the physical world. To protect location privacy, I develop a real-life location monitoring system that is based on Bluetooth Low Energy (BLE) privacy feature that changes the device physical address periodically. To enable users to better control their privacy level while still providing monitoring and tracking service to authorized parties (e.g., for child and elderly care), I extend BLE privacy by enriching its privacy semantics with a comprehensive set of metrics, such as simple opt-in/out, k-anonymity, and granularity-based anonymity. Both systems have been posted online and evaluated in terms of accuracy and user study.

# Contents