

MASTER'S THESIS

Towards practical location systems with privacy protection

Chen, Zhuo

Date of Award:
2015

[Link to publication](#)

General rights

Copyright and intellectual property rights for the publications made accessible in HKBU Scholars are retained by the authors and/or other copyright owners. In addition to the restrictions prescribed by the Copyright Ordinance of Hong Kong, all users and readers must also observe the following terms of use:

- Users may download and print one copy of any publication from HKBU Scholars for the purpose of private study or research
- Users cannot further distribute the material or use it for any profit-making activity or commercial gain
- To share publications in HKBU Scholars with others, users are welcome to freely distribute the permanent URL assigned to the publication

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

Declaration	i
Abstract	ii
Acknowledgements	iv
Contents	v
List of Tables	x
List of Figures	xi
Notation	xiii
1 Introduction	1
1.1 Background and Motivation	2
1.2 Approach	5
1.3 Contributions	6

1.4	Outline of the Thesis	7
2	Privacy Protection in Mobile Geo-social Services	8
2.1	Introduction	8
2.2	Geo-fence Services	9
2.2.1	Geo-fence	9
2.2.2	Geo-fence Social Networks	10
2.3	Preliminary: Location Anonymity in Mobile Geo-social Services	11
2.3.1	Proximity Detection	12
2.3.2	Static Proximity Detection with Location Anonymity . .	13
2.3.3	Dynamic Proximity Monitoring with Location Anonymity	15
2.4	Proximity Detection for Practical Mobile Geo-social Services . .	17
2.4.1	Privacy Guarantee in Proximity Detection	17
2.4.2	Geo-fence Social Networks with Privacy Protection . . .	17
2.4.3	Real-time Location Sharing with Privacy Protection . . .	18
2.5	Implementing Practical Mobile Geo-social Systems with Pri- vacy Protection	20
2.5.1	Helloc System Overview and Features	20
2.5.2	User Feedback	22
2.5.3	System Architecture	23
2.5.4	Geographic Coordinate System Conversion	23

2.5.5	Energy-Saving Message Pushing	25
2.6	SDK for Mobile Geo-social Systems with Privacy Protection . . .	28
2.6.1	Front-End SDK	28
2.6.2	Back-End SDK	30
3	Preliminary: Bluetooth and Bluetooth Low Energy	32
3.1	Introduction	32
3.2	Bluetooth Low Energy	33
3.2.1	Advantages of BLE	34
3.3	Bluetooth Address	35
3.4	Privacy Feature	37
3.5	Resolvable Address Revisited	38
3.5.1	Random Address Hash function ah	40
3.5.2	Security function e	41
4	Privacy-Preserving Large-Scale Location Monitoring Using BLE	42
4.1	Introduction	42
4.2	Related Work	44
4.3	System Objective and Model	46
4.3.1	System Model and Security Goal	47
4.3.2	Location Area Model	48
4.4	Implementation of Location Monitoring	50

4.4.1	Monitoring Hosts	50
4.4.2	Detailed Procedures	50
4.5	Implementation of Privacy Features	52
4.5.1	Baseline Privacy Features	52
	4.5.1.1 Implementation of Resolvable Private Address Resolution with IRKs	53
4.5.2	Baseline Privacy over Large Population	55
4.5.3	Opt-In and Opt-Out Support	58
4.5.4	k-Anonymity Metric Support	60
4.5.5	Granularity Metric Support	61
4.5.6	Security Analysis and Discussion	62
4.6	“Track Me Profile” (TMP)	64
4.6.1	A Generic Privacy Profile Extending BLE Privacy Feature	64
4.6.2	Roles and Requirement	65
4.6.3	Tracking Interfacing Service	67
4.6.4	Tracking Runtime Service	67
4.7	System Evaluation	68
4.7.1	Performance Evaluation	68
4.7.2	Monitoring Accuracy	69
4.7.3	User Experience Study	70
4.7.4	Application Potential	72

5 Conclusion	74
5.1 Summary	74
5.2 Future work	75
Appendix A Implementation of “Track Me Profile”	76
A.1 Implementation of Basic Privacy Profile	76
A.2 Implementation of Tracking Interfacing Service	81
A.3 Implementation of Tracking Runtime Service	84
Bibliography	86
CURRICULUM VITAE	91