

SpringerBriefs on Cyber Security Systems and Networks

Editor-in-Chief

Yang Xiang, Digital Research and Innovation Capability, Swinburne University of Technology, Hawthorn, Melbourne, VIC, Australia

Series editors

Liqun Chen, University of Surrey, Guildford, UK

Kim-Kwang Raymond Choo, University of Texas at San Antonio, San Antonio, TX, USA

Sherman S. M. Chow, Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong

Robert H. Deng, Singapore Management University, Singapore, Singapore

Dieter Gollmann, Hamburg University of Technology, Hamburg, Germany

Javier Lopez, University of Málaga, Málaga, Spain

Kui Ren, University at Buffalo, Buffalo, NY, USA

Jianying Zhou, Singapore University of Technology and Design, Singapore, Singapore

The series aims to develop and disseminate an understanding of innovations, paradigms, techniques, and technologies in the contexts of cyber security systems and networks related research and studies. It publishes thorough and cohesive overviews of state-of-the-art topics in cyber security, as well as sophisticated techniques, original research presentations and in-depth case studies in cyber systems and networks. The series also provides a single point of coverage of advanced and timely emerging topics as well as a forum for core concepts that may not have reached a level of maturity to warrant a comprehensive textbook. It addresses security, privacy, availability, and dependability issues for cyber systems and networks, and welcomes emerging technologies, such as artificial intelligence, cloud computing, cyber physical systems, and big data analytics related to cyber security research. The main focuses on the following research topics:

Fundamentals and Theories

- Cryptography for cyber security
- Theories of cyber security
- Provable security

Cyber Systems and Networks

- Cyber systems security
- Network security
- Security services
- Social networks security and privacy
- Cyber attacks and defense
- Data-driven cyber security
- Trusted computing and systems

Applications and Others

- Hardware and device security
- Cyber application security
- Human and social aspects of cyber security

More information about this series at <http://www.springer.com/series/15797>

Bo Liu · Wanlei Zhou · Tianqing Zhu
Yong Xiang · Kun Wang

Location Privacy in Mobile Applications

Bo Liu
La Trobe University
Bundoora, VIC, Australia

Wanlei Zhou
School of Software
University of Technology Sydney
Ultimo, NSW, Australia

Tianqing Zhu
School of Software
University of Technology Sydney
Ultimo, NSW, Australia

Yong Xiang
School of Information Technology
Deakin University
Burwood, VIC, Australia

Kun Wang
School of Internet of Things
Nanjing University of Posts
and Telecommunications
Nanjing, China

ISSN 2522-5561 ISSN 2522-557X (electronic)
SpringerBriefs on Cyber Security Systems and Networks
ISBN 978-981-13-1704-0 ISBN 978-981-13-1705-7 (eBook)
<https://doi.org/10.1007/978-981-13-1705-7>

Library of Congress Control Number: 2018953315

© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The Global Positioning System (GPS) module has almost become standard in mobile phones in recent years, driving the growth of location-based services (LBSs) which provide a variety of information services (such as mobile social networks, navigation, places of interest finding, sports and healthy assistant, augmented reality games) based on the location data. As all the LBS providers require the access permission to users' location data, severe privacy concerns are raised at the same time. Therefore, effective location privacy preservation is foremost for these mobile applications.

Despite the big amount of papers in this area, there lacks a systematic study to present all related components of the problem. Moreover, the gap between theory and practice is big. To overcome these obstacles, this book will provide an integrated five-element framework for location privacy research, which includes analysis of location privacy definitions, attacks and adversaries, location privacy protection methods, location privacy metrics, and location-based mobile applications. In addition, we analyze the relationships between the different elements of location privacy. For example, a particular attack is targeted to the location data in a particular application. Then, it can be prevented by a certain type of protection method. Moreover, location privacy will be studied in detail in three different applications. We will also share some insights on the possible research directions.

We believe that this study will shed light on the research issues of location privacy and promote the advance and development of future location-based mobile applications. The content will be useful for researchers, students, and engineers in this area.

Melbourne, Australia
June 2018

Bo Liu

Contents

1	Introduction	1
1.1	Background	1
1.2	Definition of Location Privacy	2
1.2.1	Location-Based Services	2
1.2.2	Representation of Location Information	3
1.2.3	The Definition of Location Privacy	5
1.2.4	Location Privacy Versus Data Privacy	6
1.3	Location Attacks and Adversaries	6
1.3.1	Location Information Obtaining Methods	7
1.3.2	Types of Adversarial Knowledge	7
1.3.3	Attack Targets	8
1.3.4	Types of Attack Methods	9
1.3.5	Emerging Trends	10
1.4	People's View About Location Privacy	10
1.4.1	Do People Really Know How Much of Their Location Information Has Been Collected or Revealed?	10
1.4.2	How Do People Care About Their Location Privacy?	11
1.5	Location-Based Services in Practical Applications	11
1.6	The Unified Location Privacy Research Framework	13
1.7	Outline and Book Overview	14
	References	14
2	Location Privacy-Preserving Mechanisms	17
2.1	Cryptographic Mechanism	17
2.2	Anonymization Mechanisms	18
2.2.1	k -Anonymity	18
2.2.2	Mix-Zone	19
2.3	Obfuscation Mechanisms	20
2.3.1	Dummy Locations	20
2.3.2	Location Obfuscation	20

2.3.3	Differential Privacy-Based Methods	21
2.4	Reducing Location Information Sharing	22
2.4.1	Caching	22
2.4.2	Game Theory	22
2.5	Comparisons and Discussions	22
2.5.1	LPPMs Versus Other Privacy Preservation Techniques	22
2.5.2	Comparisons of the Four Different Groups	24
2.6	Performance Evaluation: Location Privacy Metrics	25
2.6.1	Certainty	25
2.6.2	Correctness	26
2.6.3	Information Gain or Loss	26
2.6.4	Geo-Indistinguishability	27
2.6.5	Time	27
2.6.6	Discussion on Performance Metrics	28
	References	28
3	Location Privacy in Mobile Social Network Applications	33
3.1	Introduction	33
3.2	Sensitive Location Prediction by Users Social Network Data	34
3.2.1	Content-Based Approach	34
3.2.2	Check-In-Based Approach	34
3.2.3	Check-In Behavior of Users in Mobile Social Networks	35
3.2.4	Home Location Prediction Algorithms	36
3.2.5	The Adversary and Attack Models	36
3.2.6	Privacy Metrics	37
3.3	Protecting Important Locations in Social Networks	37
3.3.1	Community-Based Geo-Location Information Sharing Scheme	37
3.3.2	Aggregated Check-In Behavior of Users in a Community	39
3.3.3	Datasets and Evaluation Setup	39
3.3.4	Impact on Spatial Feature of the Check-Ins	40
3.3.5	Impact on Home Location Prediction Algorithms	40
3.4	Summary	42
	References	45
4	Location Privacy in Mobile Crowd Sensing Applications	47
4.1	Introduction	47
4.2	System Model and Problem Formulation	49
4.2.1	The General Mobile Crowd Sensing System	49
4.2.2	The Basic Idea of Privacy-Preserving MCS Application Framework	49

4.2.3	Location Privacy Metric	51
4.2.4	Economic Models for the MCS Application	51
4.2.5	Problem Formulation	53
4.3	Privacy-Preserving MCS Schemes Based on Economic Models	54
4.3.1	The Monopoly Model-Based Scheme (MMBS)	55
4.3.2	Cournot’s Oligopoly Model-Based Scheme (COMBS)	58
4.3.3	Privacy Analysis of Our Proposed Schemes	60
4.4	Performance Evaluation	62
4.4.1	Simulation Setup	62
4.4.2	Performance Analysis	63
4.4.3	Discussions	72
4.5	Conclusions and Future Works	74
	References	75
5	Location Privacy in Wireless Vehicular Networks	77
5.1	Introduction	77
5.2	System Model	79
5.2.1	System Model	79
5.2.2	V2R Communication Model	80
5.2.3	Privacy Threats for In-Vehicle Users and Adversary Attack Models	82
5.2.4	POI Query Probability	82
5.3	Problem Formulation and the Proposed Privacy-Enhancing Scheme	83
5.3.1	Basic Idea of Our Privacy Preservation Framework	83
5.3.2	Location Privacy Metrics	84
5.3.3	Problem Formulation	85
5.3.4	Privacy-Enhancing Scheme Based on LBS Content Broadcasting and Active Caching (LBS-CBAC)	86
5.3.5	Knowledge-Based Pre-caching for RSU Broadcasting Content	88
5.4	Performance Evaluation	88
5.4.1	Simulation Setup	88
5.4.2	Performance Analysis	90
5.4.3	Comparison of Privacy Level with k-Anonymity Methods	95
5.4.4	Further Discussions	96
5.5	Conclusions	97
	References	97

6	Future Directions and Conclusions	99
6.1	Future Directions	99
6.1.1	Location Privacy Protection Under Correlations	99
6.1.2	Location Privacy in Big Data and Deep Learning Era	99
6.1.3	Location Privacy in Autonomous Systems	100
6.2	Conclusions	100
	References	101

Acronyms

AR	Augmented reality
DP	Differential privacy
DSRC	Dedicated short-range communication
GPS	Global positioning system
LBA	Location-based application
LBS	Location-based service
LPPM	Location privacy preservation mechanism
MCS	Mobile crowd sensing
MSN	Mobile social network
OBU	On-board unit
PIR	Private information retrieval
POI	Place of interest
PSD	Personal sensing device
QoS	Quality of service
RoT	Region of Task
RSU	Roadside unit
SP	Service provider
SQL	Service quality loss
TTP	Trusted third party
V2R	Vehicle-to-roadside
V2V	Vehicle-to-vehicle
WAVE	Wireless Access for Vehicular Environments