

Xiaohui Liang
Rongxing Lu
Xiaodong Lin
Xuemin (Sherman) Shen



Security and Privacy in Mobile Social Networks



SpringerBriefs in Computer Science

Series Editors

Stan Zdonik

Peng Ning

Shashi Shekhar

Jonathan Katz

Xindong Wu

Lakhmi C. Jain

David Padua

Xuemin Shen

Borko Furht

V.S. Subrahmanian

Martial Hebert

Katsushi Ikeuchi

Bruno Siciliano

For further volumes:

<http://www.springer.com/series/10028>

Xiaohui Liang • Rongxing Lu • Xiaodong Lin
Xuemin (Sherman) Shen

Security and Privacy in Mobile Social Networks

Xiaohui Liang
Department of Electrical and Computer
Engineering
University of Waterloo
Waterloo, ON, Canada

Xiaodong Lin
Faculty of Business and Information
Technology
University of Ontario Institute
of Technology
Oshawa, ON, Canada

Rongxing Lu
School of Electrical
and Electronics Engineering
Nanyang Technological University
Singapore

Xuemin (Sherman) Shen
Department of Electrical and Computer
Engineering
University of Waterloo
Waterloo, ON, Canada

ISSN 2191-5768
ISBN 978-1-4614-8856-9
DOI 10.1007/978-1-4614-8857-6
Springer New York Heidelberg Dordrecht London

ISSN 2191-5776 (electronic)
ISBN 978-1-4614-8857-6 (eBook)

Library of Congress Control Number: 2013947689

© The Author(s) 2013

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Social networking makes wireless communication technologies sharpening tools for extending the social circle of people. It has already become an integral part of our daily lives, enabling us to contact our friends and families without geographic barriers. Recently, social networking can be further reached in a mobile environment due to the pervasive use of smartphones. Smartphones greatly increase our communication, computation, and information storage capabilities and help us stay connected with our social friends anywhere anytime. The convergence of smartphones and social networking tools give us a pervasive communication platform, named mobile social network (MSN), over which we are able to use long-ranged wireless communication techniques such as 3G and LTE to reach our online social friends, or short-ranged techniques such as Bluetooth or WiFi to explore the physically close neighbors. In MSNs, multiple communication domains coexist, and within each domain promising applications are fostered. For example, nearby friend search applications help users to find other physically close peers who have similar interests and preferences; local vendors disseminate attractive service information to nearby users and users leave service reviews to vendors. Before the practical implementation of these applications, there are still many challenging research issues, among which security and privacy are the most important ones as users are vulnerable to security attacks, easily ignore their privacy protection, and hardly have trust toward others in the MSN. In this book, we focus on three emerging research topics in MSNs, namely privacy-preserving profile matching (PPM) protocols, privacy-preserving cooperative data forwarding (PDF) protocols, and trustworthy service evaluation (TSE) systems. The PPM helps two users compare their personal profiles without disclosing the profiles. The PDF helps users forward data to their friends via multiple cooperative relay peers while preserving their identity and location privacy. The TSE enables users to locally share service reviews on the vendors such that users receive more valuable information about the services not only from vendors but also from their trusted social friends. We study the three research topics from both theoretic and practical aspects. Specifically, we introduce the system model, review the related works, and present the solutions. We further

provide the security analysis and the performance evaluation based on real-trace simulations. Lastly, we summarize our works followed by introducing the future research directions.

Waterloo, ON, Canada
Waterloo, ON, Canada
Oshawa, ON, Canada
Waterloo, ON, Canada

Xiaohui Liang
Rongxing Lu
Xiaodong Lin
Xuemin (Sherman) Shen

Contents

1	Overview	1
1.1	Mobile Social Network	1
1.1.1	Mobile Social Network	1
1.1.2	Mobile Applications	3
1.2	Characteristics of MSN	5
1.2.1	Multiple Communication Domains	5
1.2.2	Social Behavior	6
1.2.3	Social Graph	7
1.2.4	Security and Privacy	7
1.3	Research Topics in Mobile Social Network	9
1.4	Security Primitives	11
1.4.1	K Anonymity	11
1.4.2	Multiple Pseudonym Technique	11
1.4.3	Prediction Method: Autoregression	12
1.4.4	Cryptographic Techniques	13
2	Profile Matching Protocol with Anonymity Enhancing Techniques	19
2.1	Introduction	19
2.2	Network Model and Design Goal	20
2.2.1	Network Model	20
2.2.2	Design Goal	20
2.3	PPM Solutions	22
2.3.1	Approach 1: Explicit Comparison-Based Approach	24
2.3.2	Approach 2: Implicit Comparison-Based Approach	26
2.3.3	Approach 3: Implicit Predicate-Based Approach	28
2.4	Anonymity Enhancing Techniques	30
2.4.1	Anonymity Measurement	30
2.4.2	Anonymity Enhancement	32
2.5	Performance Evaluation	34
2.5.1	Simulation Setup	35
2.5.2	Simulation Results	36

2.6	Related Work	39
2.7	Conclusion and Future Directions	40
3	Cooperative Data Forwarding Strategy with Privacy Preservation	43
3.1	Introduction	43
3.2	Models and Design Goal	44
3.2.1	Network Model and Social Behavior Model	44
3.2.2	Design Goal	46
3.3	PDF Solutions	47
3.3.1	Overview of the Protocol	47
3.3.2	Phase 1: Privacy-Preserving Route-Based Authentication	48
3.3.3	Phase 2: Proximity Measurement	51
3.3.4	Phase 3: Morality-Driven Data Forwarding	53
3.3.5	Summary of Data Forwarding Strategy	57
3.4	Performance Evaluation	58
3.4.1	Simulation Settings	58
3.4.2	Simulation Results	61
3.5	Related Work	64
3.6	Conclusion and Future Directions	66
4	Recommendation-Based Trustworthy Service Evaluation	67
4.1	Introduction	67
4.2	System Model and Design Goal	69
4.2.1	System Model	69
4.2.2	Design Goal	70
4.3	TSE Solutions	71
4.3.1	Phase 1 of bTSE: Structured Reviews	72
4.3.2	Phase 2 of bTSE: Token Generation	73
4.3.3	Phase 3 of bTSE: Review Generation and Submission	76
4.3.4	SrTSE	78
4.3.5	Summary of bTSE and SrTSE	81
4.4	Security Analysis	82
4.4.1	Resilience to Review Linkability Attacks	82
4.4.2	Resilience to Review Rejection Attacks	82
4.4.3	Resilience to Review Modification Attacks	83
4.4.4	Resilience to Sybil Attacks	84
4.4.5	Numerical Results of Detecting Sybil Attack	85
4.5	Performance Evaluation	87
4.5.1	Simulation Setup	88
4.5.2	Simulation Results	89
4.6	Related Work	91
4.7	Conclusion and Future Directions	92
References	95

Chapter 1

Overview

1.1 Mobile Social Network

Social networking makes digital communication technologies sharpening tools for extending our social circle. It has already become an important integral part of our daily lives, enabling us to contact our friends and families. In the meantime, fueled by the pervasive adoption of smartphones, we have a growing tendency to access our social networks more often by smartphones than desktop computers or laptops [1]. With smartphones, we are able to check the digital personal schedules when lying in bed; read and reply to emails in the meeting room; contact friends to have a lunch together on the way to the mall; and send photos to families in the tourist areas. In other words, with smartphones, we are more capable of creating, implementing and managing of novel and efficient mobile applications. In nowadays, the pervasive use of mobile applications and the social connections fosters a promising mobile social network (MSN) where reliable, comfortable and efficient computation and communication tools are provided to improve the quality of our work and life.

1.1.1 *Mobile Social Network*

Over the past decade, smartphones evolve dramatically from appearance to functionality; they are no longer the clumsy equipments with basic calling and messaging functions but nice-looking and portable “toys” with integrated sensing functions and countless mobile applications. Hardware specifications of smartphones have been dramatically improved to the level of personal computers, along with friendly interface improvements and usability enhancements. In parallel to that, the deployment of 3G and LTE networks has considerably improved the available mobile bandwidth, enabling the provisioning of content and services powered by the cloud computing infrastructure. WiFi and Bluetooth techniques are pervasively used in mobile applications to enable users to communicate with

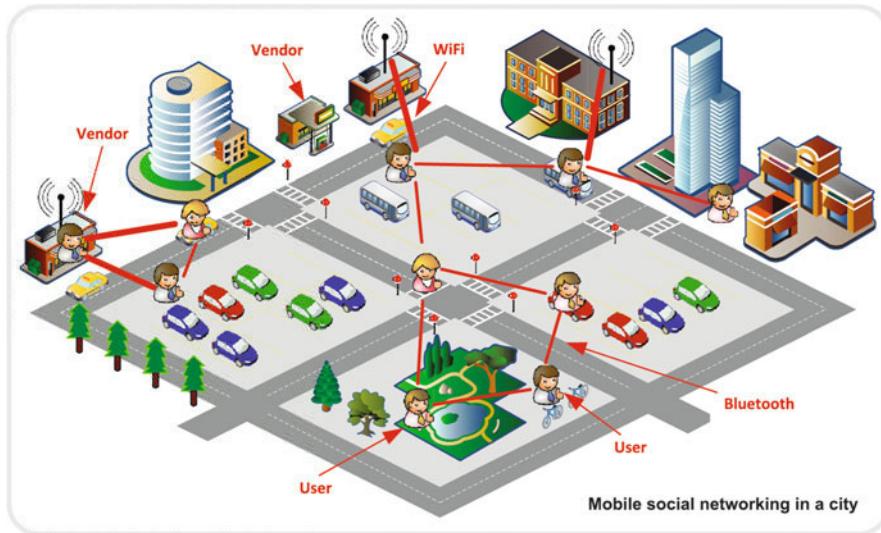


Fig. 1.1 Mobile social network

their physically-close neighbors. Due to the great potential commercial opportunity, developers and researchers design a wide range of mobile applications which can be used in different scenarios to keep up with the demand from users. As such, MSN as a pervasive communication platform to host the promising centralized/decentralized applications becomes the focus, and its research challenges and solutions are much urgent to be explored. In the following, we introduce the components of an MSN as shown in Fig. 1.1.

In the MSN, smartphones enable users to stay connected with not only the online service providers through 3G and LTE techniques, but also the physically-close peers through short-ranged wireless communication techniques, such as Bluetooth or WiFi. We consider each individual user has a unique mobility model and a personalized social behavior pattern. The reliability and efficiency of any communication protocols in the MSN are influenced by the opportunistic contacts and individual choices of users.

Vendors (a.k.a. local service providers), either mobile or static aim to provide local services to nearby users. When a vendor is mobile, it can be performed by a user who disseminates information to the encountered users in a distributed manner. When a vendor is static, it can be a local store, a restaurant, or an information center, which can be visited by the nearby users. In this case, the vendor could have more powerful and stable communication and storage devices which are placed on, in, or around their buildings.

Prior to the development of the MSN, *trusted authorities* are considered to be trusted to initialize the key materials for both vendors and users. The key materials are used to secure the local communications. Commonly-used online social systems