SPRINGER BRIEFS IN COMPUTER SCIENCE

Xiaohui Liang
Rongxing Lu
Xiaodong Lin
Xuemin (Sherman) Shen

Security and Privacy in Mobile Social Networks

Springer

SpringerBriefs in Computer Science

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

Springer

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

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

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

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

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-1-4614-8856-9 ISBN 978-1-4614-8857-6 (eBook)
DOI 10.1007/978-1-4614-8857-6
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013947689

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 — Xiaohui Liang
Waterloo, ON, Canada — Rongxing Lu
Oshawa, ON, Canada — Xiaodong Lin
Waterloo, ON, Canada — Xuemin (Sherman) Shen

Contents

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

X. Liang et al., *Security and Privacy in Mobile Social Networks*, SpringerBriefs in Computer Science, DOI 10.1007/978-1-4614-8857-6_1, © The Author(s) 2013

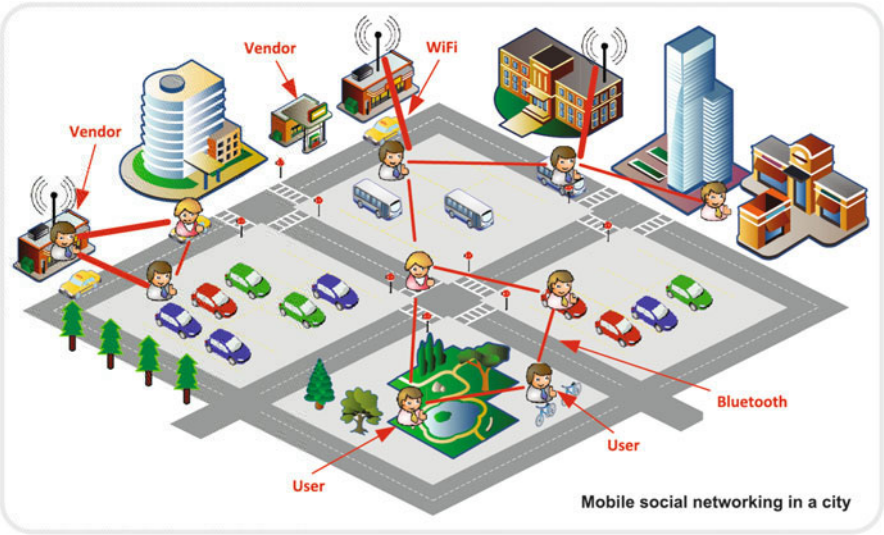

Fig. 1.1 Mobile social network

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