

Wireless Networks

Series editor

Xuemin (Sherman) Shen

University of Waterloo, Waterloo, Ontario, Canada

More information about this series at <http://www.springer.com/series/14180>

Sheng Zhong • Hong Zhong • Xinyi Huang
Panlong Yang • Jin Shi • Lei Xie • Kun Wang

Security and Privacy for Next-Generation Wireless Networks



Springer

Sheng Zhong
Department of Computer Science and Tech
Nanjing University
Nanjing, China

Xinyi Huang
School of Mathematics and Computer Sci
Fujian Normal University
Fuzhou, China

Jin Shi
School of Information Management
Nanjing University
Nanjing, China

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

Hong Zhong
School of Computer Science and Tech
Anhui University
Hefei, China

Panlong Yang
College of Computer Science and Tech
University of Science and Technology of
Hefei, China

Lei Xie
Department of Computer Science and Tech
Nanjing University
Nanjing, China

ISSN 2366-1186

Wireless Networks

ISBN 978-3-030-01149-9

<https://doi.org/10.1007/978-3-030-01150-5>

ISSN 2366-1445 (electronic)

ISBN 978-3-030-01150-5 (eBook)

Library of Congress Control Number: 2018957331

© Springer Nature Switzerland AG 2019

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 Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Information technology and big data have made mobile Internet indispensable, leading to the development of a panoply of novel computing models and fueling the development of the next generation wireless networks. Breakthroughs in application technologies such as cloud computing, blockchains, and artificial intelligence have accelerated the integration of the human society and the physical world with the cyber world. The sophisticated connections between human individuals and physical devices are accurately and diversely reflected in the IoT space where the physical world and the cyber world are blended through a large-scale deployment of wireless sensor networks, the Internet of Things, and mobile crowdsourcing. Among them, new interpersonal interactions, social networks, and community collaborations, which were previously widely anticipated, have gained unprecedentedly great potentials for implementation and deployment.

In this process, on the one hand in terms of basic wireless network technologies and applications, its convenient deployment, low construction cost, strong scalability, high openness, and high flexibility bring multiple conveniences for the intelligentization, diversification and integration of our daily life; on the other hand, it is inherently open and participatory, making the control of data and communication security more complicated. Therefore, security and privacy have become a key issue as well as the primary concern for the growth of the next-generation wireless networks.

There have been an abundant number of books that introduce wireless networks which mainly make comprehensive reviews from the perspectives of technologies, principles and applications, such as wireless network security technologies, status quo and strategies of wireless network security, ZigBee wireless networks, wireless vehicle networks, wireless sensor networks, to name but a few. However, books that start from the point of view of security and privacy of wireless networks, and discuss the systems of the next-generation wireless networks and the basis of their algorithms from both the macro and micro perspectives are not so easy to find. Those books which further explore and discuss about the human-cyber-physical integration, namely, the integration of the human society, the physical

world and the cyber world, in the field of cyber security and privacy are scarcer. This book, fortunately, fills the vacant space in this research field in time. It starts at two levels, namely fundamental theories and system designs, and uses the human-cyber-physical interconnection as an entry point to explain in detail the process of integrating the human society, the physical world and the cyber world, and how to understand and solve security and privacy issues in the next-generation wireless networks.

The authors of this book are all active scholars in the field of cyber security and network systems. They have made more than significant contributions in their cutting edge research. In particular, Sheng Zhong is a leading member of the cyberspace security team of the State Key Laboratory of Novel Software Technology. He has successfully accumulated several excellent scientific research achievements in the aforementioned field, especially on the theoretical foundations. In this book, he reviews the challenges and opportunities of the next-generation wireless network security and privacy from a macro perspective, and thoroughly discusses the fundamentals of algorithm designs. Hong Zhong, Dean of the School of Computer Science and Technology at Anhui University, has always been at the forefront of network and information security research and teaching. Therefore, she has presented various innovative ideas in numerous investigative topics such as the security and privacy of self-organized vehicle networks. Xinyi Huang, Dean of the College of Mathematics and Informatics at Fujian Normal University, with a lot of experience in the research on network information security, studies security and privacy issues in mobile sensor networks in this book. Panlong Yang, from the University of Science and Technology of China, an expert of wireless networks and crowd sensing, is responsible for a chapter on security and privacy issues of mobile crowd sensing with detailed interpretations and discussions. Jin Shi, Director of the National Security Intelligence Research Group at Nanjing University, has been engaged in information security and big data analysis research for many years. He presents insights on security and privacy issues in cloud computing systems and embedded systems. Lei Xie, a promising young computer scientist from Nanjing University, writes a chapter on security and privacy issues in the integration of the cyber world and the physical world. Kun Wang from Nanjing University of Posts and Telecommunications has been engaged in extensive research on blockchain technology, energy Internet, and edge computing. In this book, he presents the latest research findings on security and privacy issues in mobile crowd computing.

The research topics covered in this book all belong to those currently hot ones. Each author has incorporated his opinions while writing the relevant chapters. This book has a nice and logical structure, uses concise language, and is fully accessible. It is a good textbook suitable for computer science, electrical engineering and other majors. It can also serve as a reference book for wireless network researchers and practitioners.

From a research point of view, all the chapters of this book are integrated into a whole; but if it is read separately, each chapter can be regarded as an independent part, and is convenient for undergraduate and graduate students interested in a particular topic to carry out targeted research and discussions. This book can

broaden readers' horizons, guide students and relevant researchers to see the development of next-generation wireless networks from a higher perspective, and explore the future trends of wireless network technology with a more acute insight in this era of rapid development. In this sense, this book is a must-read for wireless network security and privacy research. We believe that the publication of this book can play an active role in promoting the in-depth development of this research field. Hereby I recommend this book to all potential readers, and write a preface for it.

Jian Lu

Member of Chinese Academy of Sciences
President of Nanjing University
Nanjing, China

May 2018

Contents

- 1 Networking Cyber-Physical Systems: System Fundamentals of Security and Privacy for Next-Generation Wireless Networks 1**
 - 1.1 Introduction 1
 - 1.1.1 The Definition, Advantages and Classification of Wireless Network 1
 - 1.1.2 Evolution of Wireless Network Architecture: From 1G to 4G 2
 - 1.2 Next Generation Wireless Network 3
 - 1.2.1 The Construction Goal of the Next Generation Wireless Network 3
 - 1.2.2 The Architecture of the Next Generation Wireless Network 4
 - 1.2.3 Integration of Cloud Computing, Internet of Things and Next Generation Wireless Network Architecture..... 5
 - 1.3 Research on Next-Generation Wireless Network Security 8
 - 1.4 Security and Privacy Problem in Cloud Computing 10
 - 1.4.1 The Introduction of Cloud Computing 10
 - 1.4.2 Network Security of Cloud Computing 11
 - 1.4.3 Virtualization Security of Cloud Computing 12
 - 1.4.4 Data Security of Cloud Computing 14
 - 1.4.5 Cloud Computing User Privacy Security 15
 - 1.5 Security Threats in Mobile System..... 16
 - 1.5.1 Introduction 16
 - 1.5.2 LTE Architecture and the Security Issues 17
 - 1.5.3 Identity Authentication Problems in Mobile Communication Networks..... 18
 - 1.5.4 SDN Security Issues 20
 - 1.6 Security and Privacy Challenges in Embedded Systems 22
 - 1.6.1 Introduction 22
 - 1.6.2 Security of Embedded System Hardware..... 23

1.6.3	Security and Privacy of Embedded System Software	25
1.6.4	Security of Embedded Network	27
1.7	What Remains Unsolved: Future Research Trends	28
	References	29
2	Networking Cyber-Physical Systems: Algorithm Fundamentals of Security and Privacy for Next-Generation Wireless Networks	33
2.1	Challenges and Opportunities	33
2.2	Algorithms on Security Issues in Wireless Networks	34
2.3	Algorithms on Privacy Issues in Wireless Networks	37
2.4	Future Research Trends	45
	References	46
3	Connecting Physical-World to Cyber-World: Security and Privacy Issues in Pervasive Sensing	49
3.1	Connecting Physical-World to Cyber-World: Gains and Pains	49
3.2	Investigating into Security and Privacy Issues in Pervasive Sensing	50
3.3	Challenges and Opportunities	51
3.4	Security Issues in Pervasive Sensing	52
3.4.1	User Authentication	52
3.4.2	Secret Key Extraction	55
3.5	Privacy Issues in Pervasive Sensing	57
3.5.1	Sensitive Information Privacy	57
3.5.2	Location Privacy	59
3.6	What Remains Unsolved: Future Research Trends	60
	References	61
4	Connecting Human to Cyber-World: Security and Privacy Issues in Mobile Crowdsourcing Networks	65
4.1	Introduction	65
4.2	Overview of MCNs	66
4.2.1	Characteristics	66
4.2.2	Architecture	68
4.2.3	Key Components	71
4.2.4	Applications	71
4.3	Threats and Challenges in MCNs	71
4.3.1	Basic Description of Several Threats	71
4.3.2	Threat Analysis	73
4.3.3	Privacy Threats	76
4.3.4	Trust Threats	79
4.3.5	Requirements	79
4.4	Security Assuring and Privacy Preserving Solutions	81
4.4.1	Encryption	81
4.4.2	Perturbation	84
4.4.3	Data Lake	85

4.4.4	Incentives	86
4.4.5	Reputation	87
4.4.6	Location Privacy	87
4.5	Future Research Trends	90
4.5.1	Malicious Service Provider	90
4.5.2	Combination with Other Technologies	94
4.5.3	Big Data	95
4.6	Conclusion	95
	References	95
5	Connecting Things to Things in Physical-World: Security and Privacy Issues in Vehicular Ad-hoc Networks	101
5.1	Introduction of a Brand-New Network: VANET	101
5.2	Overviews of Security and Privacy	104
5.3	Methods and Strategies	108
5.4	Security Issues in VANET	114
5.4.1	Secret Key Management	114
5.4.2	Message Verification	117
5.4.3	Identity Traceability	120
5.5	Privacy Issues in VANET	123
5.5.1	Identity Traceability	124
5.5.2	Location Privacy	127
5.6	Conclusions and Future Research Directions	130
	References	131
6	Connecting Things to Things in Physical-World: Security and Privacy Issues in Mobile Sensor Networks	135
6.1	Sensor Networks	135
6.2	Challenges	136
6.3	Security Issues in Sensor Networks	138
6.3.1	Key Establishment Protocols at Higher Layers	139
6.3.2	Key Establishment Protocols at the Physical Layer	144
6.4	Privacy Issues in Sensor Networks	148
6.4.1	Localization Protocols at Higher Layers	148
6.4.2	Localization Protocols at the Physical Layer	151
6.5	Future Research Trends	153
	References	154
7	Connecting Human to Physical-World: Security and Privacy Issues in Mobile Crowdsensing	161
7.1	Overview	161
7.2	Mobile Crowdsensing Basics and How Human Are Connected to Cyber-World	161
7.2.1	Introduction of Mobile Crowd-Sensing	162
7.2.2	Task Allocation Mechanisms in Crowd-Sensing	163
7.2.3	Data Quality and Processing in Crowd-Sensing	165

7.3	Security and Privacy Issues When Using Inertial Sensors	167
7.3.1	Privacy Invasion on Different Inertial Sensors	167
7.3.2	Countermeasures.....	169
7.4	Security and Privacy Issues When Using Communication Links.....	170
7.4.1	Localization with Communication Links	170
7.4.2	Imaging with Communications Links	171
7.4.3	Recognizing Human Gesture with Communication Links....	172
7.5	Security and Privacy Issues When Using Side Channels.....	173
7.5.1	Side Channels	173
7.5.2	Coordination	173
7.5.3	Neighbor Discovery	174
7.5.4	Control Message Delivery	174
7.5.5	Smartphone Applications.....	174
7.6	Future Research Trends	175
	References	177
	Index.....	181