SpringerBriefs in Electrical and Computer Engineering

More information about this series at http://www.springer.com/series/10059

Aiqing Zhang • Liang Zhou • Lei Wang

Security-Aware Device-to-Device Communications Underlaying Cellular Networks

Springer

Aiqing Zhang
College of Telecommunications
and Information Engineering
Nanjing University of Posts
and Telecommunications
Nanjing, Jiangsu, China

Lei Wang
Key Lab of Broadband Wireless
Communication and Sensor Network
Technology
Nanjing University of Posts
and Telecommunications
Nanjing, Jiangsu, China

Liang Zhou
Key Lab of Broadband Wireless
Communication and Sensor Network
Technology
Nanjing University of Posts
and Telecommunications
Nanjing, Jiangsu, China

ISSN 2191-8112 ISSN 2191-8120 (electronic)
SpringerBriefs in Electrical and Computer Engineering
ISBN 978-3-319-32457-9 ISBN 978-3-319-32458-6 (eBook)
DOI 10.1007/978-3-319-32458-6

Library of Congress Control Number: 2016939117

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

With an explosive growth of mobile population and wireless multimedia data, it is increasingly necessary and important to off-load the busy traffic of cellular networks. As device-to-device (D2D) communication is a promising data off-loading solution in long-term evolution (LTE) networks, it has received a substantial amount of interest in communication and network research communities recently. D2D communications enable devices to communicate directly; thus, they have the advantages of improving resource utilization, enhancing user's throughput, extending battery lifetime, etc. However, due to the open nature of D2D communications, they face two substantial technical challenges when it applies to large-scale applications, that is, security and availability. The objective of this book is to present systematical mechanisms to realize system security and availability for D2D communications.

Chapter 1 gives an overview of D2D communications, including their architecture, characteristics, application scenarios, and open topics. Then, the security issues are presented from the aspects of security architectures, threat model, and security requirements. Finally, the organization of the book is depicted for a comprehensive understanding of the book.

In Chap. 2, we propose a secure data sharing protocol, which merges the advantages of public key cryptography and symmetric encryption, to achieve data security in D2D communications. Specifically, digital signature combining with mutual authentication between the evolved NodeB (eNB) and users guarantees the entity authentication, data authority and integrity, and transmission non-repudiation as well as traceability. Meanwhile, data confidentiality is achieved through symmetric encryption. The key hint transmission between the eNB and user equipments (UEs) realizes reception non-repudiation. Free-riding attack is detected by keeping a record of the data sharing behaviors for the UEs in the eNB; thus, the system availability is improved.

In Chap. 3, an overview of physical-layer security is firstly given in terms of secrecy capacity, physical-layer key agreement, and physical-layer authentication. Then a joint framework involving both the physical- and application-layer security

technologies is proposed for multimedia service over D2D communications. In this scheme, the scalable security service can be achieved without changing the current communication framework.

Furthermore, as the system availability largely depends on the cooperation degree of the users, Chap. 4 focuses on cooperation stimulation. As multimedia dominates the contents with quality of experience (QoE) as a key measurement, the cooperation stimulation mechanism is constructed for maximizing user QoE characterized by mean opinion score (MOS). In the proposed scheme, the users compute their transmitter MOS and receiver MOS and send them to the content provider (CP). Then, the CP formulates a weighted directed graph based on the network topology and connection MOS. By seeking 1-Factors for the graph, the content dissemination scheme is designed according to the 1-Factor with the maximum weight. Additionally, in order to realize cheat-proof, a debt mechanism is introduced in the scheme. Simulation results demonstrate that the proposed scheme gives due consideration to efficiency and fairness for content dissemination in D2D communications.

Finally, Chap. 5 summarizes this book and highlights the future research directions.

Nanjing, China
October 2015

Aiqing Zhang
Liang Zhou
Lei Wang

Acknowledgments

This work is partly supported by the National Natural Science Foundation of China (Grants No. 61322104, 61571240), Natural Science Foundation of Anhui Province (1608085QF138), University Natural Science Research Foundation of Anhui Province (KJ2015A105, KJ2015A092), and Key Projects of the Outstanding Young Talents Program in Universities of Anhui Province (gxyqZD2016027).

Contents