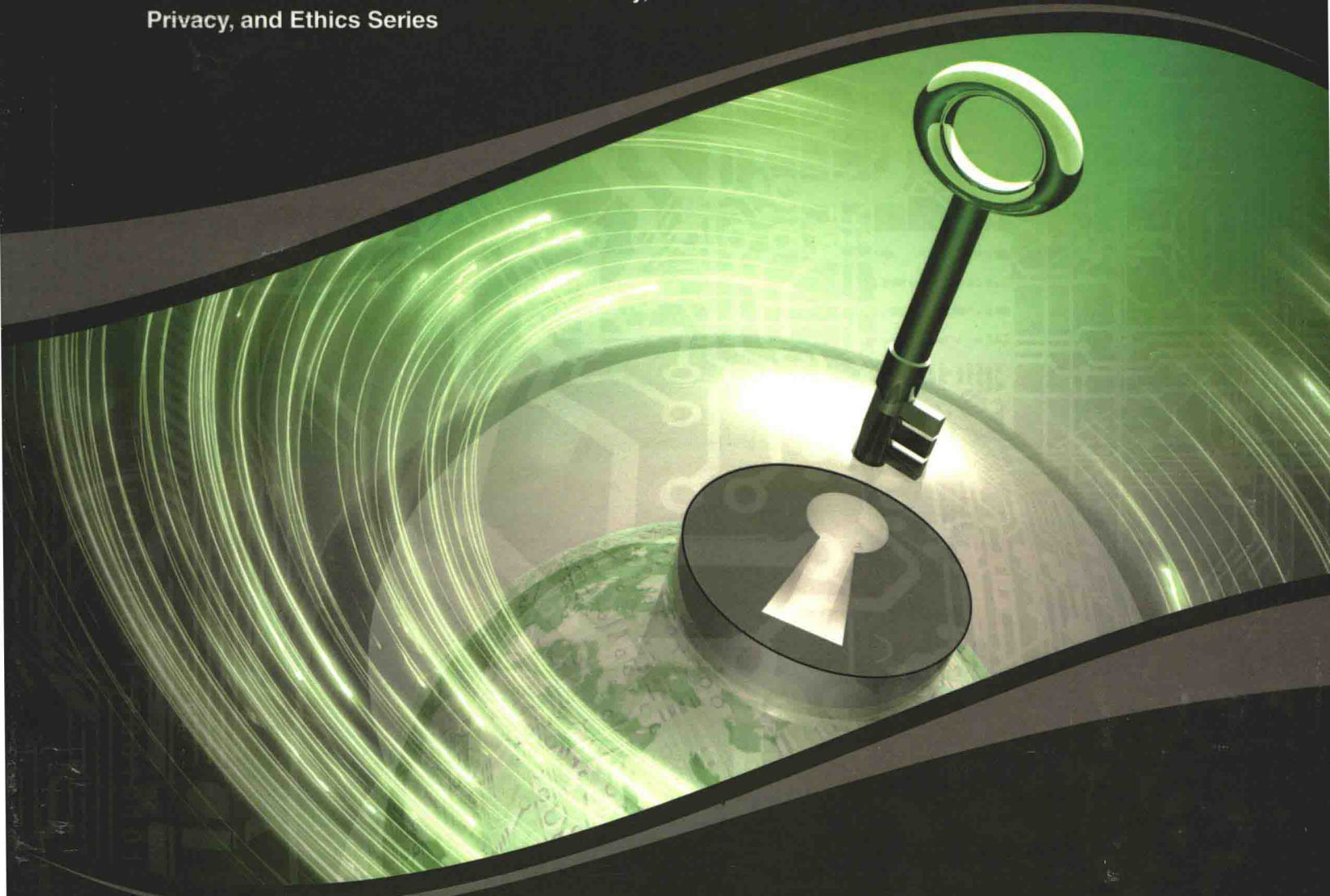
Premier Reference Source

Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications

Part of the Advances in Information Security, Privacy, and Ethics Series



Danda B. Rawat, Bhed B. Bista, and Gongjun Yan

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE

Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications

Danda B. Rawat
Georgia Southern University, USA

Bhed B. Bista
Iwate Prefectural University, Japan

Gongjun Yan
University of Southern Indiana, USA

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Editorial Director Myla Merkel
Production Manager: Jennifer Yoder
Publishing Systems Analyst: Adrienne Freeland
Development Editor: Christine Smith
Acquisitions Editor: Kayla Wolfe
Typesetter: John Crodian
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

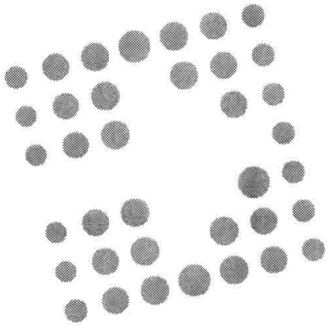
Library of Congress Cataloging-in-Publication Data

Security, privacy, trust, and resource management in mobile and wireless communications / Danda B. Rawat, Bhed B. Bista, and Gongjun Yan, editors.
pages cm
Includes bibliographical references and index.
Summary: "This book examines the current scope of theoretical and practical applications on the security of mobile and wireless communications, covering fundamental concepts of current issues, challenges, and solutions in wireless and mobile networks"-- Provided by publisher.
ISBN 978-1-4666-4691-9 (hardcover) -- ISBN 978-1-4666-4692-6 (ebook) -- ISBN 978-1-4666-4693-3 (print & perpetual access) 1. Wireless communication systems--Security measures. 2. Mobile communication systems--Security measures. 3. Computer networks--Security measures. I. Rawat, Danda B., 1977- II. Bista, Bhed B., 1967- III. Yan, Gongjun, 1976-.
TK5103.2.S444 2013
005.8--dc23

2013025029

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.



Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

ISSN: 1948-9730
EISSN: 1948-9749

Mission

In the digital age, when everything from municipal power grids to individual mobile telephone locations is all available in electronic form, the implications and protection of this data has never been more important and controversial. As digital technologies become more pervasive in everyday life and the Internet is utilized in ever increasing ways by both private and public entities, the need for more research on securing, regulating, and understanding these areas is growing.

The **Advances in Information Security, Privacy, & Ethics (AISPE) Book Series** is the source for this research, as the series provides only the most cutting-edge research on how information is utilized in the digital age.

Coverage

- Access Control
- Device Fingerprinting
- Global Privacy Concerns
- Information Security Standards
- Network Security Services
- Privacy-Enhancing Technologies
- Risk Management
- Security Information Management
- Technoethics
- Tracking Cookies

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Information Security, Privacy, and Ethics (AISPE) Book Series (ISSN 1948-9730) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-information-security-privacy-ethics/37157. Postmaster: Send all address changes to above address.

Titles in this Series

For a list of additional titles in this series, please visit: www.igi-global.com

Research Developments in Biometrics and Video Processing Techniques
Rajeev Srivastava (Indian Institute of Technology (BHU), India) S.K. Singh (Indian Institute of Technology (BHU), India) and K.K. Shukla (Indian Institute of Technology (BHU), India)
Information Science Reference • copyright 2014 • 237pp • H/C (ISBN: 9781466648685) • US $195.00 (our price)

Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications
Danda B. Rawat (Georgia Southern University, USA) Bhed B. Bista (Iwate Prefectural University, Japan) and Gongjun Yan (University of Southern Indiana, USA)
Information Science Reference • copyright 2014 • 413pp • H/C (ISBN: 9781466646919) • US $195.00 (our price)

Architectures and Protocols for Secure Information Technology Infrastructures
Antonio Ruiz-Martinez (University of Murcia, Spain) Rafael Marin-Lopez (University of Murcia, Spain) and Fernando Pereniguez-Garcia (University of Murcia, Spain)
Information Science Reference • copyright 2014 • 427pp • H/C (ISBN: 9781466645141) • US $195.00 (our price)

Theory and Practice of Cryptography Solutions for Secure Information Systems
Atilla Elçi (Aksaray University, Turkey) Josef Pieprzyk (Macquarie University, Australia) Alexander G. Chefranov (Eastern Mediterranean University, North Cyprus) Mehmet A. Orgun (Macquarie University, Australia) Huaxiong Wang (Nanyang Technological University, Singapore) and Rajan Shankaran (Macquarie University, Australia)
Information Science Reference • copyright 2013 • 351pp • H/C (ISBN: 9781466640306) • US $195.00 (our price)

IT Security Governance Innovations Theory and Research
Daniel Mellado (Spanish Tax Agency, Spain) Luis Enrique Sánchez (University of Castilla-La Mancha, Spain) Eduardo Fernández-Medina (University of Castilla – La Mancha, Spain) and Mario G. Piattini (University of Castilla - La Mancha, Spain)
Information Science Reference • copyright 2013 • 373pp • H/C (ISBN: 9781466620834) • US $195.00 (our price)

Threats, Countermeasures, and Advances in Applied Information Security
Manish Gupta (State University of New York at Buffalo, USA) John Walp (M&T Bank Corporation, USA) and Raj Sharman (State University of New York, USA)
Information Science Reference • copyright 2012 • 319pp • H/C (ISBN: 9781466609785) • US $195.00 (our price)

Investigating Cyber Law and Cyber Ethics Issues, Impacts and Practices
Alfreda Dudley (Towson University, USA) James Braman (Towson University, USA) and Giovanni Vincenti (Towson University, USA)
Information Science Reference • copyright 2012 • 343pp • H/C (ISBN: 9781613501320) • US $195.00 (our price)

www.igi-global.com

701 E. Chocolate Ave., Hershey, PA 17033
Order online at www.igi-global.com or call 717-533-8845 x100
To place a standing order for titles released in this series, contact: cust@igi-global.com
Mon-Fri 8:00 am - 5:00 pm (est) or fax 24 hours a day 717-533-8661

To Our Families

Editorial Advisory Board

Preface

After successful deployment of Wi-Fi and cellular networks in the past decade, wireless and mobile communication systems became the fastest growing sector of the communication industry, and there are different networks based on the coverage area: Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), and Wireless Wide Area Network (WWAN). The vision of being connected anywhere and anytime is no longer just an idea; it is becoming a reality because of the combination of mobile devices with wireless communication technologies. Almost all businesses that rely on wireless and mobile networks expect the same or a similar level of security, privacy, and trust as the ones that exist in wired networks to ensure the integrity and confidentiality of communications among terminals, networks, applications, and services. Many physical, capacity, and economic limitations of wireless and mobile networks represent important challenges. Yet, it is very challenging to ensure security, privacy, trust, and resource management because of the mobility of network nodes.

Although higher layer security mechanisms and protocols address wireless security challenges to a large extent, more security vulnerabilities arise due to the increasingly pervasive existence of wireless communication devices. Secure transmission is a concern for wireless devices and networks due to the broadcast nature of signals. By exploiting variations in the transmission channel, wireless devices can generate a shared secret key to provide security in the physical layer. The physical layer security concept is linked to two main desired features. The first is system reliability, which means that a message intended for a specific user should be reliably received by that user. The second is message secrecy, which means that a transmitter wants to communicate a secret message to a legitimate receiver.

With the advent of ad hoc networking technologies, mobile users could form a Mobile Ad Hoc Network (MANET) where users have an opportunity to create their own wireless network on the fly. MANETs represent a milestone in the evolution of wireless networks; however, they inherit the traditional limitations of mobile and wireless communication systems, such as allocation of bandwidth, transmitting power, coverage, etc. In MANETs, each node can directly communicate with other nodes using a direct link (i.e., single hop) or multi-hop communications. In this case, each node works as a source, a router, or a destination node. Nodes rely on the message received from other nodes, and thus, it is important to measure the trustworthiness of the received messages. As a consequence, each node needs security, privacy, and trust management schemes to protect the MANET as a whole.

Vehicular Ad Hoc Networks (VANETs) are a special form of MANETs where vehicles exchange information with each other while they travel on the road. Because of the high speed of the vehicles, VANETs have highly dynamic topologies, which result in frequent communication link breakage. In addition, vehicles' identities are linked with the identities of owners/drivers. As a consequence, it is not

secure to use Vehicle Identification Numbers (VINs) or other private information that is linked to the owner or driver. To provide security and privacy, anonymity of vehicles is commonly used to participate in communications. In this case, malicious drivers can easily mislead the communication by injecting false information when ad hoc networks do not have the capability of tracking malicious drivers. Therefore, security, privacy, and trust in VANETs are key components to realizing its full potential.

Recent advances in Micro-Electro-Mechanical Systems (MEMS) technology have made it easy to build small, inexpensive, and energy-efficient wireless nodes that make a Wireless Sensor Network (WSN) a reality. In WSN, each node is comprised of a sensing, processing, transmitting, and power unit. When sensor nodes are deployed in a remote location, they are supposed to coordinate with each other to perform a specific action. Each operation of the sensor node costs the battery life, and no one would be able to change the battery in the sensor or deploy new sensors, especially in war zones. WSN has wide range of applications including temperature sensing, pressure sensing, inventory tracking, seismic detection, mobility sensing, environment monitoring, homeland security, etc. Despite their diverse applications, WSN poses a number of unique technical challenges due to several factors, such as fault tolerance, scalability, operating environment, network topology, transmit media, power consumption, limited security implementation, etc.

In true mobile communications to provide seamless mobility, there is an intrinsic problem related to mobility in the data network that uses the IP address as the node's identifier and location within a sub network. When a mobile node moves from one network to another, the assigned IP can no longer serve as a locator for the node in the new network. Mobile IPv4 (MIPv4) and Mobile IPv6 (MIPv6) are emerging to provide macro-mobility support using IPv4 and IPv6 network protocol stacks. Mobility in this type of network is effective when the mobile nodes are one hop away from access routers. The emergence of cloud computing and its extension into the mobile domain creates the potential for a global, interconnected mobile cloud computing environment that will allow the entire mobile ecosystem to enrich their services across multiple networks.

This book is organized as follows:

- Section 1 introduces the fundamentals of mobile and wireless communications networks;
- Section 2 presents physical layer security;
- Section 3 discusses about vehicular communications and networking;
- Section 4 describes security in mobile ad hoc networks;
- Section 5 deals with trust and privacy in wireless networks;
- Section 6 discusses the wireless sensor network and its challenges;
- Section 7 describes the applications and issues of cloud and mobile communications;
- Section 8 deals with wireless network management and analysis.

In more detail:

- Section 1 includes chapters titled "Introduction to Mobile and Wireless Communications Networks" and "Security in Wireless Metropolitan Area Networks: WiMAX and LTE;"
- Section 2 includes "Physical Layer Security and Its Applications: A Survey" and "Physical Layer Security in Wireless Communication Networks;"

- Section 3 includes "Security and Connectivity Analysis in Vehicular Communication Networks," "Location Security in Vehicular Wireless Networks," "Misbehavior Detection in VANET: A Survey," and "Intrusion Detection in Vehicular Ad-Hoc Networks on Lower Layers;"
- Section 4 includes "Security Issues in Mobile Ad Hoc Networks: A Survey" and "Security and Privacy in Mobile Ad Hoc Social Networks;"
- Section 5 includes "A Multi-Parameter Trust Framework for Mobile Ad Hoc Networks," "Trust Management and Modeling Techniques in Wireless Communications," and "Privacy Protection in Vehicular Ad-Hoc Networks;"
- Section 6 includes "Security Challenges in Wireless Sensor Networks" and "Voting Median Base Algorithm for Measurement Approximation of Wireless Sensor Network Performance;"
- Section 7 includes "Mobile Cloud Computing and Its Security, Privacy, and Trust Management Challenges," "State of the Art for Near Field Communication: Security and Privacy within the Field," and "Modeling and Verification of Cooperation Incentive Mechanisms in User-Centric Wireless Communications;"
- Section 8 includes "Seamless Mobility Management: A Need for Next Generation All-IP Wireless Networks" and "900 MHz Spectrum Refarming Analysis for UMTS900 Deployment."

This book covers the fundamental concepts and current issues, challenges, and solutions in wireless and mobile networks. We hope it serves as a reference for graduate students, professors, and researchers in this emerging field.

Danda B. Rawat
Georgia Southern University, USA

Bhed B. Bista
Iwate Prefectural University, Japan

Gongjun Yan
University of Southern Indiana, USA

Acknowledgment

This book would not have been published without the contribution of several people. First and foremost, we would like to express our warm appreciation to the authors who work hard to contribute the chapters and have chosen this book as a platform to publish their research findings. Special thanks go to the contributors' universities and organizations who allowed them the valuable time and resources towards the effort of writing the chapters. We would also like to express our warm appreciation to the editorial advisory board members and reviewers who gave their valuable time to reviewing chapters and helping us select high quality chapters.

Finally, we want to thank our families who supported and encouraged us in spite of all the time this book took us away from them. Last and not least, we beg forgiveness of all we have failed to mention.

Danda B. Rawat
Georgia Southern University, USA

Bhed B. Bista
Iwate Prefectural University, Japan

Gongjun Yan
University of Southern Indiana, USA

Section 1

Fundamentals of Mobile and Wireless Communication Networks

Table of Contents

Section 3
Vehicular Communications and Networking

Section 4
Mobile Ad Hoc Networks

Section 5
Trust and Privacy in Mobile and Wireless Communications

Section 6
Wireless Sensor Networks

Section 7
Cloud and Mobile Communications

Section 8
Wireless Network Management and Analysis

Detailed Table of Contents