

BOOK REVIEWS

EDITED BY ANDRZEJ JAJSZCZYK

SECURITY FOR MOBILE NETWORKS AND PLATFORMS

SELIM AISSI, NORA DABBOUS, ANAND R. PRASAD, ARTECH HOUSE 2006, ISBN 10: 1-59693-008-x, ISBN 13: 978-1-59693-008-7, HARDCOVER, 330 PAGES

REVIEWER: MARCIN NIEMIEC

The book *Security for Mobile Networks and Platforms* presents security issues from two points of view: networks and platforms. In the first case the authors present solutions such as Internet Protocol (IP) layer and higher layer security, and security techniques in specific wireless networks. In the second case we can read about smart cards and some selected mobile platforms. The whole book is well organized and readable.

This book can be recommended for senior and graduate students in computer science or information systems. Also, mobile system architects and developers will find this book interesting and useful. Some parts of the book include basic security principles and ideas, so beginners will learn basic security issues. The simplicity, without excessive details, of these parts is an unquestionable advantage. Additionally, for wireless and mobile professionals who want to delve deeper, each chapter includes extensive bibliographic notes.

The book is organized into 16 chapters, and each chapter can be read independently. The first chapter, "Introduction," includes a lot of basic terms and is recommended for security beginners. The authors explain security basics (threats, attacks, security services) and trusted mobile platform basics (m-commerce, mobile Web services, mobile applications).

In Chapter 2, "Authentication, Authorization, and Non-Repudiation," the authors introduce authentication concepts such as challenge-response methods, and static and one-time passwords. Also, authorization strategies are presented with an example model. Finally, the authors present non-repudiation methods: digital signatures, timestamps, auditing, and some Internet Engineering Task Force (IETF) documents related to non-repudiation.

Chapter 3, "Cryptographic Techniques," presents cryptographic solutions in mobile systems: Global System for Mobile Communications (GSM), Bluetooth, and the 802.11 standard. The authors explain in detail the A5/3 algorithm and KASUMI block cipher applied in GSM; the algorithms MILENAGE, f8, and f9 defined by the Third Generation Partnership Project

(3GPP); the E1, E2, and E3 algorithms applied in Bluetooth; and the solutions implemented in 802.11 networks, from the Wired Equivalent Privacy (WEP) to the CCM protocol.

Chapter 4, "Hardware Security," consists of two parts: threats addressed by hardware protection and hardware security solutions. The second part describes architectures, protections, and applications in specific hardware solutions. They include smart cards, the trusted platform module, TrustZone technology, and wireless trusted platforms.

The content of Chapter 5, "Software Security," is software solutions. At the beginning, the authors introduce such concepts as basic elements of mobile security and communication between layers in the OSI/ISO network model. Then the authors present various protection mechanisms in mobile operation systems and the security aspects of Web services. The chapter ends with presentation of runtime security in the Java and .NET environments.

Chapter 6, "Security Certification and Evaluation," is devoted to security certification schemes and privacy aspects. The security issues discussed in this chapter are either used currently or probably will be used in the future for a mobile platform.

Chapters 7 and 8 present the security solutions in network communications. "Higher Layer Security" describes basically the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. "IP Layer Security" includes the description of IPsec, key management, Network Address Translator (NAT), virtual private network (VPN), and mobile IP. This part of the book is helpful for mobile system architects and graduate students, and allows one to acquire basic knowledge on security in IP networks.

In Chapter 9 the framework and protocols of authentication, authorization, and accounting (AAA) are presented. The chapter closes with a discussion of some practical issues such as wireless Internet service provider roaming and AAA in mobile systems.

Chapter 10 covers common IEEE 802.1x and Extensible Authentication Protocol (EAP). Several EAP methods are described in this chapter.

The next four chapters (11 to 14) describe security solutions implemented in the wireless communication network; they are presented in order of achieved range. First, wireless personal area networks (WPANs) are presented. This part considers such techniques as Blue-

tooth, Zigbee, and ultrawideband. Then the authors present such wireless local area network (WLAN) issues as security in IEEE 802.11, attacks and countermeasures, WiFi protected area (WPA), and IEEE 802.11i. Also, secure WLAN deployment methods for corporate, wireless Internet service providers, and mobile operators are given. As an example of wireless metropolitan area networks (WMANs), the authors present the IEEE 802.16 standard (WiMAX). The security issues and PKM protocols (both versions) are explained in detail. This part ends with wireless wide area networks (WWANs); GSM and 3GPP security are presented.

Chapter 15, "Future Security Challenges," provides an interesting analysis of future mobile networks and platforms from the security point of view. The authors "try to look at the crystal ball and try to materialize (...) what they see in it."

Chapter 16, "Mobile Security Threat Catalog," includes some tables with major security threats (software, hardware, and network threats), published attacks, vulnerabilities, and security protection means.

The great advantage of this book is that it collects in one volume information on software and hardware security of mobile systems. Although perhaps not all presented protocols and algorithms are described precisely enough, the book includes all of the main mobile security solutions currently applied in telecommunications. In my opinion, this book is worth recommending for people who want to have a broad look at modern mobile security.

COOPERATION IN WIRELESS NETWORKS: PRINCIPLES AND APPLICATIONS

EDITED BY: FRANK H. P. FITZEK AND MARCOS D. KATZ, SPRINGER, DORDRECHT, THE NETHERLANDS, 2006, ISBN 1-4020-4710-X, HARDCOVER, 641 PAGES

REVIEWER: SZYMON SZOTT

The wireless networking domain faces a multitude of challenges, ranging from varying channel conditions to battery limitations. It is amazing how many of these challenges can be overcome through the use of cooperative techniques. The book *Cooperation in Wireless Networks: Principles and Applications* (a set of independent texts gathered by Frank H. P. Fitzek and Marcos D. Katz) provides insight on the theory and practice of utilizing cooperation. Such combined efforts can

(Continued on page 22)

(Continued from page 20)

occur between different entities, yet their purpose is always to provide a synergy effect. The book consists of 20 chapters in which top researchers from different parts of the world display the benefits of cooperation. These include spectral and power efficiency, increased throughput, coverage, quality of service (QoS), scalability, and security. The chapters at the beginning of the book are more theoretical and discuss the principles of applying cooperation in wireless networks, whereas later chapters provide practical applications of cooperation.

The first chapter (by the editors) serves as an introduction to the topic of cooperation from the perspective of nature, social sciences, and game theory. The characteristics of cooperative behavior and guidelines for the implementation of such systems are presented. The chapter also provides the motivation for introducing cooperation into wireless environments with illustrative examples.

The second chapter (by A. Chakrabarti, A. Sabharwal, and B. Aazhang) provides a theoretical discussion on the throughput of relay channels (the basic building blocks of cooperative communication) and discusses how to construct practical codes. The authors of Chapter 3 (O. S. Shin, N. Devroye, P. Mitran, H. Ochiari, S. S. Ghassemzadeh, H. T. Kung, and V. Tarokh) present theoretical fundamentals for nodes or clusters of a wireless network, communicating on the same frequency using either cooperative or cognitive paradigms, as alternatives to competition strategies.

In Chapter 4 (by S. Cui and A. J. Goldsmith) the focus is on a cross-layer design framework, intended to increase network performance, in particular to save battery power. Interesting design examples illustrate key features of such a cross-layer design. The next chapter (by D. S. Lun, T. Ho, N. Ratnakar, M. Médard, and R. Koetter) is related to the theory of network coding (i.e., coding at the packet level) and the issues involved. Its positive impact on network performance, through efficient use of resources, decentralized operation, and increased security, is highlighted.

Chapter 6 (by J. N. Laneman) is a theoretical study of cooperative diversity, an interesting new class of spatial diversity techniques that utilize relay nodes to jointly transmit data. In the subsequent chapter (by P. Mähönen, M. Petrova, and J. Riihijärvi), the major

challenges of cooperation in ad hoc networks are outlined. Emphasis is put on awareness of 802.11 performance limitations. Future trends for ad hoc (cognitive radios, topology awareness, mesh networking) are presented.

Chapter 8 (by K. Navaie and H. Yanikomeroglu) presents a novel cooperative relaying method for multihop infrastructure-based wireless networks to increase per-user throughput. An incentive system ensures node cooperation. Simulations show that in a UMTS-type environment the throughput gain can be significant. The concept of a cognitive radio (CR) architecture is the subject of Chapter 9 (by J. Mitola III). It discusses the motivation and application of CR and provides detailed information on the architecture.

Chapter 10 (by K. Wrona and P. Mähönen) deals with the problem of encouraging cooperation and mitigating misbehavior. The stability of cooperative systems is analyzed using a game theoretical approach and through simulation. Optimizing energy usage in cellular networks is the topic of Chapter 11 (by F.H.P. Fitzek, P. Kyritsi, and M.D. Katz). The authors provide means of reducing power consumption through the cooperation of nearby nodes.

The authors of Chapter 12 (P. C. F. Eggers, P. Kyritsi, and I. Z. Kovács) have evaluated by measurements and simulation the performance of cooperative antenna systems (based on user-to-user cross links). Another possible way of cooperating in the field of antenna systems is the concept of virtual antenna arrays presented in Chapter 13 (by M. Dohler and A. H. Aghvami). Spatially adjacent nodes cooperate to form a MIMO-like system. This virtual transceiver entity can increase capacity in many different network scenarios while maintaining scalability.

Chapter 14 (by M. D. Katz and F. H. P. Fitzek) discusses the research challenges in 4G networks and argues that cooperation can be utilized to solve various problems. Cooperation is claimed to be “a promising resource-trading framework”. The next chapter (by K. Sivanesan and D. Mazzarese) analyzes upcoming IEEE 802 standards and discusses where cooperation techniques might be used. Cooperation at the terminal and network level, as well as between networks, is likely to be the key factor in achieving scalability and reliability.

The authors of Chapter 16 (M. H. Larsen, P. Popovski, and S. V. Andersen) describe how to use cooperation

within the realm of source coding. The proposed coding scheme can decrease traffic in the network, especially in terms of multimedia downloads (e.g., video on demand). Bandwidth can also be saved with the use of cooperative header compression as explained in Chapter 17 (by T. K. Madsen). This technique can be beneficial for many types of networks, from cellular to ad hoc.

The topic of energy awareness returns in Chapter 18 (by A. B. Olsen and P. Koch), this time through cooperative task computing. The goal is to distribute workload over cooperating terminals so that certain tasks are not performed redundantly. Chapter 19 (by J. C. H. Lin and A. Stefanov) discusses the application of cooperative coding in OFDM systems. It is shown through simulations that significant gain can be achieved in a variety of scenarios with different channel qualities between cooperating users. Finally, in the last chapter (by Y. Takatori) spatial channel control in multiple access point (AP)/base station (BS) scenarios is discussed. Multiple node cooperation in this method leads to a higher spectral efficiency than conventional solutions.

This book touches on a wide variety of aspects related to cooperation in wireless networks. It does a great job at presenting state-of-the-art research and gives an interesting overview of well developed ideas. All chapters have extensive and current references. However, several issues need to be pointed out. First of all, some chapters are general and describe problems within a certain field (e.g., ad hoc, 4G), while others are very specific. This leads to a different degree of understanding since no reader can be an expert in all fields. The clarity of the book could be further improved if it was divided into parts. Second, the book seems to be biased toward transmission and reception issues. In general, it concentrates on cooperation outside the realm of user choice. Furthermore, as a first edition, the book contains minor editorial errors, and some diagrams could be more legible.

However, despite these minor flaws, I can wholeheartedly recommend this useful book for postgraduate students, university researchers, and engineers working in the industry. *Cooperation in Wireless Networks* can not only give insight into this interesting field of research, but also truly inspire its readers to incorporate cooperative designs into their work.

Cooperation in Wireless Networks: Principles and
Applications

Real Egoistic Behavior is to Cooperate!

Fitzek, F.H.P.; Katz, M.D. (Eds.)

2006, LII, 641 p., Hardcover

ISBN: 978-1-4020-4710-7