Levente Buttyán
and Jean-Pierre Hubaux

Security and Cooperation in Wireless Networks

Thwarting
Malicious and
Selfish Behavior
in the Age of
Ubiquitous
Computing

CAMBRIDGE

SECURITY AND COOPERATION IN WIRELESS NETWORKS

Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing

LEVENTE BUTTYÁN
Budapest University of Technology and Economics (BME), Hungary

JEAN-PIERRE HUBAUX
Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521873710

First published 2008

Printed in the United Kingdom at the University Press, Cambridge

A catalog record for this publication is available from the British Library

ISBN 978-0-521-87371-0 hardback

SECURITY AND COOPERATION IN WIRELESS NETWORKS

Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing

As wireless networking becomes almost ubiquitous, it is important to anticipate potential malicious and selfish misdeeds. This self-contained text is the first to provide a scholarly description of security and non-cooperative behavior in wireless networks.

The major networking trends are analyzed and their implications explained in terms of security and cooperation. Key problems such as cheating with identities, illegitimate access to confidential data, attacks against privacy, and "stealing of bandwidth" are described along with the existing security techniques and putative methods of protection for the future. The fundamental questions of security: user and device identification; establishment of security associations; secure and cooperative routing in multi-hop networks; fair bandwidth distribution; privacy protection, and so on, are approached from a theoretical perspective and supported by real-world examples including ad hoc, mesh, vehicular, sensor, and RFID networks. The important relationships between trust, security, and cooperation are also discussed.

End of chapter homework problems test the reader and open new directions of thought; and two tutorials in the appendices, on cryptographic protocols and game theory, provide a review of the background material required to grasp the core concepts.

Ideal for senior undergraduates and graduate students of electrical engineering and computer science, this book will also be an invaluable resource on thwarting malicious and selfish behavior for researchers and practitioners in the wireless industry.

Supplementary material for this title, including lecture slides and instructor-only solutions, are available online at http://www.cambridge.org/9780521873710 and http://secowinet.epfl.ch.

LEVENTE BUTTYÁN is an Associate Professor in the Department of Telecommunications, Budapest University of Technology and Economics (BME), Hungary.

JEAN-PIERRE HUBAUX is a Professor at the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland.

To Zsombi, Benci, and Boti
To Catherine, Sylvie, Nathalie, and Emilie

Preface

We have entered the era of wireless networks. By now, the number of wireless phones has superseded that of wired ones. Wireless LANs are routinely used by millions of nomadic users. Wireless devices have become commonplace in offices, private homes, factories, and hospitals. And technologists promise us a world of ubiquitous computing, in which myriads of tiny, untethered sensors and actuators will communicate with each other, promptly taking care of our various needs and wishes.

In addition to this pervasiveness, we are witnessing a change of paradigm: initially, wireless devices had limited or no programmability and were managed (and secured) in a highly centralized fashion. Today, high-tier wireless end-systems are full-fledged personal computers and take an increasingly active role in the networking mechanisms. In the extreme case of multi-hop ad hoc networks, the end-systems *are* the network.

Unfortunately, this evolution is creating new vulnerabilities. Even existing wireless networks (and especially wireless LANs) exhibit a number of security weaknesses, some of which have been painstakingly fixed *a posteriori*. It is now clear that the security solutions devised for wired networks cannot be used as such to protect the wireless ones. An additional problem is that the frenzy to commercialize quickly new products and new services is in contradiction with the design of a well-thought (and possibly standardized) security architecture.

This textbook aims at preventing ubiquitous computing from becoming a pervasive nightmare. It contains a thorough description of existing and envisioned mechanisms devised to thwart misdeeds against wireless networks. Indeed, we believe that the protection of wireless networks now requires more attention and a more systematic *a priori* approach.

In addition to the usual security concerns of networking, we need to address selfish behavior. The reason is that each wireless communication makes use of a fraction of the spectrum that has been and will remain a scarce resource. Moreover, most wireless devices are battery-powered, and for them energy is scarce as well. Consequently, the behavior of a wireless device can affect the service enjoyed by a another, neighboring device. Likewise, the behavior of a wireless network can affect the performance of another wireless network, especially if both networks operate in the same frequency band. These are the reasons we mention "cooperation" in the title of this book; wherever appropriate, we will make use of game theory in order to formalize the problems.

We believe this textbook to be the first of its kind regarding the treatment of security and cooperation in wireless networks. Owing to the constant evolution of the field, one of the major challenges of writing such a book is ensuring that it will have a reasonably long shelf life (and that the material learned from this book has long lasting value). The strategy we have adopted is to focus on the principles and to keep examples as generic as possible.

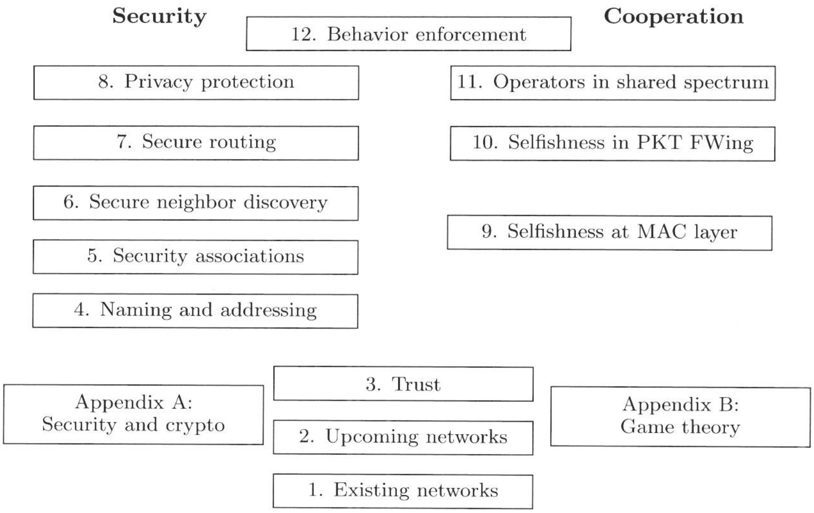
What this book is not

This book covers a substantial amount of material, but it obviously does not aim at covering everything. In particular, it is not an introduction to security or cryptography, nor is it a tutorial on game theory (but we do provide an appendix on each of these topics for the convenience of the reader). It is not an introduction to wireless networks. It is not a book on wired networks security. It is not a handbook on jamming and anti-jamming techniques. It is also not a book on wireless security standards (the reader is referred to the numerous books recently published on this topic). Finally, the book is not about the computing aspects of security, such as the protection against viruses.

What this book is about

The book provides a thorough analysis of the major trends in wireless networks and explains the implications in terms of security and cooperation. It provides a detailed description of the problems and a precise explanation of mainstream solutions wherever they exist, and of potential solutions otherwise. The structure of the book is captured by the following figure.

The twelve chapters are organized in three parts. Part I is an **introduction**, providing some background information. Chapter 1 describes how existing wireless networks are secured. Chapter 2 contains a description of upcoming wireless networks, such as mesh, vehicular, sensor and RFID networks. It identifies general trends, such as increasing decentralization and growing programmability of the devices and discusses their implications in terms of security and cooperation. Chapter 3 is devoted to the difficult issue of trust in wireless networks; it explains the



relationships between trust, security, and cooperation, and discusses the adversary model.

Part II describes the techniques aiming at thwarting **malicious behavior**;[1] as such, it makes use primarily of security techniques. Chapter 4 addresses the problem of naming and addressing; it explains how the Sybil and the replication attacks can be thwarted in such networks. Chapter 5 explains how security associations can be set up between wireless devices, notably by exploiting their physical proximity. Chapter 6 addresses secure neighbor discovery and explains the wormhole attack along with techniques to thwart it. Chapter 7 provides techniques to secure the fundamental operation of routing in wireless multi-hop networks. Finally, Chapter 8 addresses the crucial issue of privacy in upcoming wireless networks.

Part III focuses on the techniques intended to prevent **selfish behavior**;[2] therefore, it heavily relies on game theory. Chapter 9 focuses on the MAC layer. It first explains the techniques by which a WiFi selfish user can increase its share of the bandwidth, at the expense of well-behaved users; then it provides a detailed study of selfish behavior in pure ad hoc networks. Chapter 10 discusses the problem of selfishness in packet forwarding, and explains why incentives to cooperate are needed. Chapter 11 addresses the difficult question of the co-existence of operators in the same part of the spectrum. Finally, Chapter 12 describes examples of protocols that encourage selfish devices to adopt a *desirable* behavior.

[1] As we will see, malicious behavior encompasses many misdeeds, including the willingness to access unauthorized information or to deliberately affect the availability of the network for other users.

[2] Selfish behavior, as we will see, means the overuse of a common resource.

Appendix A contains a detailed description of those topics of **security** and **cryptography** that are needed to understand the book. Likewise, Appendix B provides a tutorial on **game theory** for wireless networks.

In order to make the book more concrete, we make use of several running examples to illustrate the various concepts we have introduced; these examples belong to the families of upcoming networks identified in Chapter 2: personal communication networks (including community, mesh, and mobile ad hoc networks), vehicular networks, as well as sensor and RFID networks.

Some of the chapters are specific to a given protocol layer: Chapters 6 and 9 are focused on the MAC layer, whereas Chapters 7, 10, and 12 are related to the network layer.

Intended audience

This textbook is intended for Master's and Ph.D. students as well as for researchers. It should also be of interest for the practitioners who want to get a broader view of the field.

Some familiarity with networking and security principles is useful for a proper understanding of this book.

About the title

The title of this book, *Security and Cooperation in Wireless Networks*, is well suited for the security aspects. But the word "cooperation" can be misleading, because it can be confused with the notion that wireless devices cooperate with each other at the physical layer (e.g., for beamforming). The usual term in networking is "non-cooperative behavior," but it is not particularly appropriate for the title of a book.

How to use this book

This book is designed to be covered in a one-semester course. If the students have little background on security, it is appropriate to start the course by covering Appendix A. Covering Part I should then be straightforward. At the end of Part I, the students could be encouraged to read the description of the security scheme of a wireless system not covered in the book (e.g., WiMAX) and check if they can understand it.

In Part II, each chapter can be addressed relatively independently, but the proposed order should make the understanding easier.

In current engineering and computer science curricula, game theory is usually not taught. Hence, with all likelihood, it will be necessary to first cover Appendix B before tackling Part III. Each of the four chapters of that part is fairly self-contained and can therefore be studied independently of the other. However, the beginning of the first of them (Chapter 9) is particularly intuitive because it addresses the concrete reality of WiFi systems. The last chapter (Chapter 12) is especially important as it combines the concepts of security and cooperation.

In case only a few hours per week are available, another approach consists in covering Part I and Part II in one semester, and then Part III in a follow-up (maybe optional) course in the following semester. Indeed, the two first parts of the book constitute a self-contained introduction to wireless security.

Additional material

The URL of the Web site of this book is http://secowinet.epfl.ch/ available directly or through www.cambridge.org/9780521873710. Additional material, such as slide shows (in pdf or PowerPoint[3] formats) is available there.

[3] Trademark of Microsoft Inc.

Acknowledgements

We would like to thank the students, former students, and post-docs in our research groups for their invaluable contributions. In particular, many thanks to Gergely Ács, whose research influenced Chapter 7; Naouel Ben Salem, whose research in mesh networks and in protocols for behavior enforcement was very helpful for Chapters 2 and 12; Srdjan Čapkun and Mario Čagalj, whose research shaped significantly the material of Chapter 5; Mario again, as his research was also a direct source of inspiration for Chapter 9, as was also the research carried out by Maxim Raya, Imad Aad, and Alaeddine El Fawal; Maxim again, along with Panos Papadimitratos, whose research in the security of vehicular networks proved to be very useful in several of the chapters, and in particular in Chapter 2; Mark Felegyhazi, whose research greatly influenced Chapter 10 and the second part of Chapter 11, and who contributed very significantly in clarifying the concepts in Appendix B, devoted to game theory; Julien Freudiger, for the questions of Chapter 12; Tamás Holczer and Péter Schaffer, whose research shaped the first part of Chapter 11; Hossein Manshaei for his contributions to the clarification of Bianchi's model and for some of the questions of Chapter 9; and Jun Luo, Jacques Panchard, and Marcin Poturalski who provided detailed feedback on many of the chapters.

Srdjan Čapkun deserves a specific acknowledgement for having been the first to teach a class based on a very early version of this book.

Several researchers provided very useful insights and a great support to this project; this was particularly important, considering the relative novelty of the topic. In particular, we would like to express our gratitude to Tansu Alpcan, David Basin, Jean Bolot, Daniel Figueiredo, Virgil Gligor, Matthias Grossglauser, Markus Jakobsson, Phil Janson, Frank Kargl, Edward Knightly, P. R. Kumar, Jean-Yves Le Boudec, Li Erran Li, Peter Marbach, James Massey, Cristina Nita-Rotaru, Charles Perkins, Adrian Perrig, Patrick Thiran, Don Towsley, David Tse, Nitin Vaidya, Jean Walrand, Dirk Westhoff, Heather Zheng, and Sheng Zhong.

We would like to thank the Swiss National Science Foundation for funding the National Competence Center in Research Mobile Information and Communication Systems (NCCR/MICS, sometimes nicknamed the "Terminodes project"); many of the ideas developed in this book have matured in the framework of this research program. We are indebted to those of our colleagues who have spent long hours to run the center, in particular Martin Vetterli, Thomas Gross, Karl Aberer, and Lothar Thiele. Martin deserves a special note: without his extreme dedication and visionary capabilities, the NCCR/MICS would not have taken off and, as a consequence, this book would have never existed.

We are indebted to Rafik Chaabouni who was instrumental in the formatting of the book and demonstrated a remarkable knowledge of LaTeX idiosyncrasies, and to Thomas Thurnherr who edited several figures. We would like also to extend our gratitude to Holly Cogliati who provided us with many recommendations to improve our English expressions.

Anna Littlewood and Phil Meyler, both from Cambridge University Press, deserve our gratitude for having assisted the whole editorial process; Phil selected the cover figure and helped us formulating the title of the book in the most concise way.

LB is indebted to JPH for initiating the writing of this book. Without the enthusiasm and dedication of JPH, this book would not exist today. LB is also grateful to his colleagues, István Vajda and Boldizsár Bencsáth, and to his students, Gergely Ács, László Csik, László Dóra, Tamás Holczer, Péter Schaffer, and Ta Vinh Thong for taking care of the various ongoing projects of the CrySyS Lab while he was absent due to the writing of this book, and for reading and commenting on the manuscript at various stages of the writing. Special thanks go to István Vajda for the many useful discussions on provable security. Finally, LB is infinitely grateful to his wife Zita for an endless list of things.

JPH is grateful to his dean, Willy Zwaenepoel, for his comments (and warnings) about this project. He would also like to thank Victor Bahl for having suggested to him the idea of writing a textbook on wireless security a few years ago. Last but not least, JPH is also indebted to David Messerschmitt for hosting him as a visiting scholar at the EECS department of the University of California, Berkeley, several years ago. Many of the questions addressed in this book have their seed in the discussions with David as well as with Michael Katz and Sergio Verdù.

Contents

Preface *page* xi

Acknowledgements xvi

Part I Introduction 1

1 The security of existing wireless networks 3

1.1 Vulnerabilities of wireless networks 4

1.2 Security requirements 6

1.3 How existing wireless networks are secured 7

1.4 Summary 31

1.5 To probe further 31

1.6 Questions 32

2 Upcoming wireless networks and new challenges 33

2.1 Introduction 33

2.2 Upcoming wireless networks 34

2.3 Trends and security challenges in wireless networks 68

2.4 Summary 69

2.5 To probe further 69

2.6 Questions 72

3 Trust assumptions and adversary models 74

3.1 About trust 74

3.2 Trust in the era of ubiquitous computing 76

3.3 Adversary 77

3.4 Summary 80

3.5 To probe further 80

3.6 Questions 81

Part II Thwarting malicious behavior 83

4 Naming and addressing 85

4.1 The future of naming and addressing in the Internet 85

4.2 Attacks against naming and addressing 91

4.3 Protection techniques 94
4.4 Summary 101
4.5 To probe further 101
4.6 Questions 102
5 Establishment of security associations 103
5.1 Key establishment in sensor networks 104
5.2 Exploiting physical contact 117
5.3 Exploiting mobility 118
5.4 Exploiting the properties of vicinity and of the radio link 128
5.5 Revocation 134
5.6 Summary 136
5.7 To probe further 137
5.8 Questions 140
6 Securing neighbor discovery 141
6.1 The wormhole attack 142
6.2 Wormhole detection mechanisms 146
6.3 Summary 167
6.4 To probe further 167
6.5 Questions 168
7 Secure routing in multi-hop wireless networks 169
7.1 Routing protocols for mobile ad hoc networks 169
7.2 Attacks on ad hoc network routing protocols 182
7.3 Securing ad hoc network routing protocols 191
7.4 Provable security for ad hoc network routing protocols 217
7.5 Secure routing in sensor networks 226
7.6 Summary 234
7.7 To probe further 235
7.8 Questions 236
8 Privacy protection 237
8.1 Important privacy related notions and metrics 240
8.2 Privacy in RFID systems 243
8.3 Location privacy in vehicular networks 254
8.4 Privacy preserving routing in ad hoc networks 260
8.5 Summary 267
8.6 To probe further 268
8.7 Questions 270
Part III Thwarting selfish behavior 273
9 Selfish behavior at the MAC layer of CSMA/CA 275
9.1 Operating principles of IEEE 802.11 276
9.2 Detecting selfish behavior in hotspots 280

9.3 Selfish behavior in pure ad hoc networks 301
9.4 Summary 327
9.5 To probe further 328
9.6 Questions 329
10 Selfishness in packet forwarding 331
10.1 Game theoretic model of packet forwarding 332
10.2 Meta-model 335
10.3 Analytical results 338
10.4 Simulation results 343
10.5 Summary 347
10.6 To probe further 348
10.7 Questions 348
11 Wireless operators in a shared spectrum 350
11.1 Multi-domain sensor networks 350
11.2 Border games in cellular operators 361
11.3 Summary 376
11.4 To probe further 376
11.5 Questions 377
12 Secure protocols for behavior enforcement 379
12.1 System model 379
12.2 Cooperation-optimal protocol 381
12.3 Protocol for the routing stage 383
12.4 Protocol for packet forwarding 387
12.5 Discussion 389
12.6 Summary 390
12.7 To probe further 390
12.8 Questions 391
Appendix A Introduction to cryptographic algorithms and protocols 393
A1 Introduction 393
A2 Encryption 394
A3 Hash functions 407
A4 Message authentication codes 409
A5 Digital signatures 411
A6 Session key establishment protocols 412
A7 Pseudo-random number generators 417
A8 Advanced authentication techniques 418
A9 To probe further 422
A10 Questions 422
Appendix B A tutorial on game theory for wireless networks 423
B1 Introduction 423

B2 Static games 427
B3 Dynamic games 437
B4 Repeated games 444
B5 Discussion 451
B6 Summary 454
B7 To probe further 454
B8 Questions 455
References 458
Index 479

Part I

Introduction