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

البحث في الإعلام العلمي و التقني
مصلحة
الإعلام العلمي
و التقني
CERIST

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

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

CAMBRIDGE
UNIVERSITY PRESS

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

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 in the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland.

Cover illustration: image courtesy of Deborah McLauchlan

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-0-521-87371-0

9 780521 873710