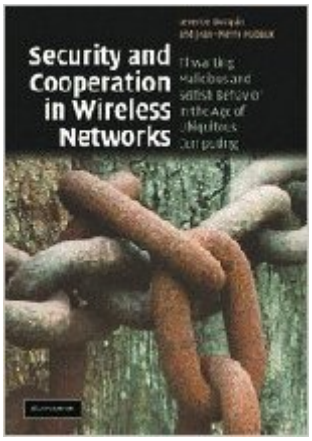
Security And Cooperation In Wireless Networks: Thwarting Malicious And Selfish Behavior In The Age Of Ubiquitous Computing



Synopsis

The current rate of deployment of wireless networks - whether cellular, LAN, Bluetooth, or sensor - is remarkable. Wireless systems are vulnerable to many kinds of attack, and the security features of fixed-line systems are not always applicable in the wireless arena. With ever-increasing amounts of data being carried on wireless networks, security has become a major concern and an area of great commercial importance. This book presents the key features of wireless networks and discusses various techniques for ensuring secure communication. In particular, techniques for dealing with hacking and other forms of attack will be dealt with, as will cooperation in multi-hop and ad hoc networks. It is suitable for senior undergraduates and graduate students of electrical engineering and computer science. Given the breadth of coverage, it will also appeal to researchers and practitioners in the wireless industry.

Book Information

Hardcover: 500 pages
Publisher: Cambridge University Press (August 1, 2007)
Language: English
ISBN-10: 0521873711
ISBN-13: 978-0521873710
Product Dimensions: 6.8 x 1.1 x 9.7 inches
Shipping Weight: 2.6 pounds (View shipping rates and policies)
Average Customer Review: 5.0 out of 5 starsÂ Â See all reviewsÂ (2 customer reviews)
Best Sellers Rank: #1,351,477 in Books (See Top 100 in Books) #133 inÂ Books > Computers & Technology > Networking & Cloud Computing > Wireless Networks #334 inÂ Books > Computers & Technology > Certification > CompTIA #1124 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

In contrast to many books available on wireless security that address mostly GSM, WLAN, and Bluetooth security, this book targets a different audience. It is an excellent survey on the ongoing security research for wireless ad-hoc networks. The previously mentioned technologies are briefly covered in the introduction, then the book discusses future forms of wireless networks that are formed spontaneously, forward traffic in a multi-hop manner, etc.As such networks have very different trust assumptions and adversary models, naturally, the security solutions differ and this is why a very active research community has created a lot of interesting security solutions.This book is

a must read for everyone who has started exploring the world of MANETs, Mesh Networks, Vehicular Networks, etc. and wonders how to provide security and prevent selfish behavior in these networks. It will safe its readers hours of literature review as the presented material has previously been cluttered over tons of conference proceedings or journal articles.The book also makes an excellent addition for any graduate class on this subject, especially as the authors provide presentation materials on the accompanying website.Last but not least, the authors are among the leading experts in this field, so they know what they are talking about. A definitive plus not found in every book ;-)

Information security has too often been addressed in an a posteriori manner, that is, when most of the system design was complete, or even after system deployment. Wireless networks are no exception in this regard. Consequently, most existing books on wireless network security describe standards and "quick fixes" to extant technologies instead of addressing the fundamental challenges for the years ahead.The book "Security and Cooperation in Wireless Networks" is unique not only because it addresses the fundamental security concepts of wireless technology but also because it anticipates new challenges, such as security of sensor, ad hoc, mesh, vehicular, and RFID networks. The authors describe possible attacks against these networks in a thorough and comprehensible way, and provide basic techniques to thwart them. An additional reason that makes this book so valuable is that it addresses not only malicious but also selfish behavior. It also includes an original tutorial to game theory and a set of detailed examples of its application to wireless networks.The clarity of this book and the comprehensive set of slides available on the book’s web site make a particularly compelling case for adopting this book as a textbook for a graduate course in computer science and engineering. "Security and Cooperation in Wireless Networks" should also be of considerable interest for researchers and practitioners.

to design, deploy, manage, and secure 802.11 wireless networks Hacking Exposed Wireless: Wireless Security Secrets & Colutions Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions Windows Vista Security: Securing Vista Against Malicious Attacks Home Security: Top 10 Home Security Strategies to Protect Your House and Family Against Criminals and Break-ins (home security monitor, home security system diy, secure home network) El gen egoista / The Selfish Gene: Las bases biologicas de nuestra conducta / The Biological Basis of Our Behavior (Ciencia / Science) (Spanish Edition) Solving Squirrel Problems: How to Keep This Ubiquitous Pest Out of Home and Garden Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Building Wireless Sensor Networks: with ZigBee, XBee, Arduino, and Processing Second Generation Mobile and Wireless Networks Localization Algorithms and Strategies for Wireless Sensor Networks RF Engineering for Wireless Networks: Hardware, Antennas, and Propagation (Communications Engineering (Paperback)) 802.11 Wireless Networks: The Definitive Guide, Second Edition 802.11 Wireless Networks: The Definitive Guide: The Definitive Guide Wireless Networks