Review of the book
"Security in Wireless Mesh Networks"
Edited by Yan Zhang, Jun Zheng and Honglin Hu
CRC Press, Taylor & Francis Groups 2008
ISBN 978-0-8493-8250-5

Gloria Tuquerres
2011-05-31

1 What the book is about

The book provides a comprehensive guide to security-related issues in wireless mesh networks with focus on system architectures. The book is published under Auerbach Publications / CRC Press series on Wireless Networks and Mobile Communications. The book is made up of fifteen chapters.

Chapter 1 (Wireless Mesh Networks, WMNs) is an introduction to the wireless mesh network concept including its architecture based on their applications. Some key research issues in the different layer of the protocols stack and a survey of industrial and academic testbeds are described.

Chapter 2 (Mesh Networking) describes the fundamentals of mesh networking in wireless PANs, LANs, MANs and WANs. For each infrastructure it presents routing protocols, network management, QoS provision, mainly for MAC and physical layers. Also it includes the industrial standards and the issues on design of scalable, low-cost and easily deployable mesh networks.

Chapter 3 (Attacks and Security Mechanisms) presents the security vulnerabilities due to multi-hop wireless networks. The attacks and solutions at the physical, MAC and network layers, with focus on the Multi-Radio Multi-Channel WMN. Illustrations of security model and of attacks are included.

Chapter 4 (Intrusion Detection in WMNs) reviews passive intrusion detection and surveyed intrusion detection systems for WMNs. The focus is on real-time monitoring and analysis of network traffic activity including issues on detection accuracy.

Chapter 5 (Security Routing in WMNs) presents a survey of security issues on wireless and ad hoc networks. With emphasis on separation of concerns and security requirements, design of secure routing protocols are included. Operations of the mobile nodes and messages formats of the digital signatures are described in the protocols description.

Chapter 6 (Hop Integrity in WMNs) described a protocol suite at network layer for ensuring hop integrity avoiding denial-of-services attacks due to message insertion or message replay. A specification using Abstract Protocol Notation and verification with state transition diagrams are covered in the description of the protocol suite.

Chapter 7 (Privacy Preservation in WMNs) covers a modeling of privacy and a routing algorithm based on Information Theory for achieving a balance between network performance and traffic privacy preservation. Also, a validation of the algorithm using simulations for a scenario with two colluding malicious observers is included.

Chapter 8 (Authentication, Trust and Privacy in WMNs) addresses security requirements and the mechanisms from the perspective of deployment WMNs. The focus is on security challenges due to mobility of nodes and management of the number of connections to provide link protection, authentication, and intrusion detection and prevention. A description of the mechanisms and protocols for authentication of nodes, trusted relations of the users and the protection of user data are included.

Chapter 9 (Non-Interactive Key Establishment in WMNs) presents a non-interactive key agreement and progression scheme based on the self-certificated key cryptosystem. The scheme consists of two protocols described in the signaling of on-demand ad hoc routing scenario. The security analysis of this application is included.

Chapter 10 (Key Management in WMNs) presents an analysis of vulnerability in key management systems due to mobility and then proposes a system to enhance the encoding of public keys and signatures and the detection of duplicated addresses.

Chapter 11 (Security in Wireless PAN Mesh Networks) presents the security architecture for Bluetooth and ZigBee technologies. The difference between the security protocols defined on the IEEE 802.15.4 standard to these two technologies is described. The vulnerabilities in the security architecture is also included.

Chapter 12 (Security in Wireless LAN Mesh Networks) presents a set of security technology definitions for link and network layers proposed by the IEEE 802.11 TGs for WLAN mesh network. Then, attacks to the key infrastructure mesh protocols are also described.

Chapter 13 (Security in IEEE 802.15.4 Cluster-Based Networks) addresses the security functions and security primitives defined for wireless sensors networks in the IEEE 802.15.4. Key management protocols for these networks and key exchange protocols for ZigBee technology are also described. Confidentiality, authentication and integrity of data as well as replay protection for providing secure communication are the issues analyzed.

Chapter 14 (Security in Wireless Sensor Networks) presents a survey of attacks and countermeasures including a description of the communication architecture and the nodes constraint characteristics in the WSNs. Cryptographic primitives, key management, secure routing, secure data aggregation and intrusion detection are also surveyed.

Chapter 15 (Key Management in Wireless Sensor Networks) presents security issues on key management techniques. After describing applications scenarios in sensor networks showing their specific characteristics, key management schemes are described in terms of key distribution techniques.

2 What is the book like (style)?

The book is divided into three parts and comprises of fifteen chapters as detailed in the previous section. Part I introduces the definition of Wireless Mesh Networks in two chapters. Part II includes seven chapters for describing security protocols and techniques. Part III consists of five chapters in which security standards, applications and enabling technologies are covered.

Each chapter begins with a list of topics and an introduction that gives an overview of the key topics covered in the chapter. Most of the chapters include a related work section that gives the motivation and background on the subject treated in the chapter. Illustrations of network structures, state diagrams, and security protocols and algorithms, many of them derived from testbed or specifications of the standards, are found throughout the text. An abundant number of references are found at the end of each chapter. Furthermore, each chapter includes a section with conclusions and open issues of the subject treated.

3 Would you recommend this book?

This book is a comprehensible reference on wireless mesh networks and network security domain. It encompasses the structures, transmission methods, transport formats, and security measures proposed for the research community and the wireless network industrial standards to provide integrity, availability, authentication, and confidentiality for transmission over these networks. It will be suitable for researchers and practitioners in the field and for graduated students looking for a research topic on network security. I strongly recommend this book as a handbook of security technologies for wireless networks.

The reviewer is a R&D engineer in network security with specialization in electronics and communication protocols