Review of the book

"Security of Self-Organizing Networks"

Edited by Al Sakib Khan Pathan

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-1-4398-1919-7

S. V. Nagaraj
RMK Engineering College

2011-08-07

1 Summary of the review

Mobile Ad Hoc Networks (MANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs) and Vehicular Ad Hoc Networks (VANETs) are important types of self-organizing networks. Such networks are becoming very important and ubiquitous in many real-life applications. This review is about a book that focuses on the security of self-organizing networks. The book looks at various security issues concerning self-organizing networks and possible solutions. The book is made up of twenty three chapters that have been written in the form of tutorials.

2 Summary of the book

The book is a collection of articles concerning the security of self-organizing networks. It discusses the security aspects of Mobile Ad Hoc Networks (MANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs) and Vehicular Ad Hoc Networks (VANETs). The book looks at important security issues in such networks and proposes some solutions. The chapters in the book have been written in the form of self-contained tutorials.

The book is made up of four parts comprising twenty three chapters.

The first part focuses on general topics. Security issues concerning wireless and self-organizing networks are introduced here. This part has five chapters.

Chapter 1 (Secure device association: trends and issues) studies the trends and issues concerning association of devices in wireless networks in a secure fashion. This chapter studies various types of attacks and device association methods. A comparative analysis of such methods is also carried out.

Chapter 2 (Securing route and path integrity in multihop wireless networks) studies protocols for securing routing and path selection in multihop wireless networks. Among the attacks studied, the wormhole attack is identified as the most serious one.

Chapter 3 (Handling security threats to the RFID system of EPC networks) analyzes threats to the RFID system of the EPC architecture. The EPC architecture is a service-oriented architecture defined by EPCGlobal Inc. An evaluation of threats is conducted along with a survey of RFID security defenses.

Chapter 4 (Security of anomaly detection algorithms: towards self-learning networks) discusses the problem of network anomaly in a network and presents possible solutions. Various methods for anomaly detection are studied including recent methods that employ machine learning.

Chapter 5 (Reputation and trust-based systems for wireless self-organizing networks) looks at the concept of trust in wireless self-organizing networks. This chapter studies reputation and trust-based systems and looks at examples of reputation and trust-based models.

The second part of the book deals with the security of mobile ad hoc networks and vehicular ad hoc networks. This part contains seven chapters.

Chapter 6 (Security threats in mobile ad hoc networks) looks at attacks on MANETS and countermeasures to such attacks.

Chapter 7 (Key management in mobile ad hoc networks) looks at the challenges in key management in MANETs. Various scenarios demand different types of solutions for key management. For example, an ad hoc network in a battlefield demands more security when compared to that of a classroom.

Chapter 8 (Combating against security attacks against mobile ad hoc networks (MANETs)) studies network layer attacks and transport layer attacks on MANETs. Case studies and open issues are also discussed.

Chapter 9 (Classification of attacks on wireless mobile ad hoc networks and vehicular ad hoc networks: a survey) studies and classifies attacks on MANETs and VANETs at the physical layer, the MAC layer, the network layer, the transport layer, and the application layer.

Chapter 10 (Security in vehicular ad hoc networks) reviews the security needs in VANETs, the challenges, the adversaries, and the attacks.

Chapter 11 (Towards a robust trust model for ensuring security and privacy in VANETs) looks at trust models for VANETs. The data centric trust management model is highlighted. Development of trust management languages is said to be challenging.

Chapter 12 (Sybil attack in VANETs: detection and prevention) looks at VANET architecture, attacks on VANETs, Sybil attack, trust establishment, and methods for detecting a Sybil attack.

The third part of the book studies wireless sensor network security. This part has nine chapters.

Chapter 13 (Key management schemes of wireless sensor networks: a survey) studies the security requirements of key management schemes in WSNs. A study of possible security threats in such networks is also conducted.

Chapter 14 (Key management techniques for wireless sensor networks: practical and theoretical considerations) looks at key establishment, key distribution, key pre-distribution, and advanced concepts for key management and trust in WSNs. This chapter contains material from another chapter by the authors which appeared earlier in another book.

Chapter 15 (Bio-inspired intrusion detection for wireless sensor networks) looks at the application of artificial and natural immune systems for intrusion detection in WSNs.

Chapter 16 (Biological inspired autonomously secure mechanism for wireless sensor networks) studies the application of ant colony optimization based routing methods in WSNs. Different types of attacks in WSNs and ways of detecting them are also looked at.

Chapter 17 (Controlled link establishment attack on key pre-distribution schemes for distributed sensor networks and countermeasures) looks at controlled link establishment attacks and countermeasures. The authors also look at the drawbacks of the countermeasures.

Chapter 18 (Proactive key variation owing to dynamic clustering (PERIODIC) in sensor networks) studies a key renewal scheme that varies the keys employed for communication. Periodic key variation is employed by the authors.

Chapter 19 (Secure routing architectures using cross-layer information for attack avoidance (with case study on wormhole attacks)) looks at sensor network security issues, ways of defending WSNs, wormhole attacks, and progress in current research.

Chapter 20 (Reputation-based trust systems in wireless sensor networks) looks at current reputation-based trust systems, and classifies and compares them.

Chapter 21 (Major works on the necessity and implementations of PKC in WSNs: a beginner's note) studies the challenges in implementing public key cryptography in WSNs. A survey of notable implementations of public key cryptography in WSNs is presented.

The fourth part of the book studies wireless mesh network security. This part consists of two chapters.

Chapter 22 (Secure access control and authentication in wireless mesh networks) looks at access control and authentication mechanisms in wireless mesh networks. Attacks on such networks are also studied.

Chapter 23 (Misbehavior detection in wireless mesh networks) surveys ways of detecting misbehaving clients in wireless mesh networks.

The book includes a helpful index.

3 What is the book like (style)?

The book includes the contributions of over fifty researchers from several countries. The book is quite readable and therefore suitable for teaching master's and doctoral level students. The questions and sample answers at the end of each chapter will help the readers to assess their learning. The book includes adequate material to reinforce learning. The inclusion of the biographies of the authors at the end of chapters is welcomed and the style of presentation followed in the book is appreciated. There are numerous references to the literature and the inclusion of future directions for research at the end of each chapter is to be praised.

Self-organizing networks are expected to be ubiquitous in the near future. So it will be prudent to focus on their security. The authors of the individual chapters have tried to make the presentation as self-contained as possible. Despite contributions from over fifty authors, the style of presentation is uniform. The details have been presented in a manner readers will find beneficial. There are many books on the market that cover topics discussed in the book, however, this book is quite unique due to the elegant style of presentation followed. However, I wish to state that more information about WMNs could have been provided and exercises should have been included. I could not find (on the Web) supplementary materials such as slides mentioned by the editor of the book in its preface.

4 Would you recommend this book?

This book offers a good introduction to the security aspects of self-organizing networks. It will be useful for students pursuing master's and doctoral level programs. It will also be useful for researchers and industry professionals who wish to update themselves on the topics covered by this book. I strongly recommend this book as a useful reference work on the security of self-organizing networks for students, professionals, and researchers.

The reviewer is a Professor at the CSE Dept., RMK Engg. College, Kavaraipettai, Tamil Nadu, India