Preface

Wireless networks have been seen unprecedented growth in the past few years. Wireless technologies provide users with a variety of benefits like portability, flexibility, increased productivity, and lower installation costs. Various wireless technologies, from wireless local area network (WLAN) and Bluetooth to WiMAX and third generation (3G) have been developed. Each of these technologies has its own unique applications and characteristics. For example, a WLAN can provide the wireless users with high bandwidth data communication in a restricted and dense area (hotpot). Ad hoc networks, like those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. WiMAX can provide high-speed, high bandwidth efficiency, and high-capacity multimedia services for residential as well as enterprise applications.

However, any wireless technology is inherently risky. It has the same risks as the wired networks as well as new risks brought by the wireless connectivity. There have been many reports of security weaknesses and problems related to different wireless technologies, which make wireless security quite a hot research topic recently, both in the academia and industry.

Wireless security is a very broad area as there are so many different wireless technologies existing. Each wireless technology has its own architecture, algorithms, and protocols. Different wireless technologies have their own application areas and different security concerns, requirements, and solutions. To this end, we want to bring up the *Handbook of Research on Wireless Security* to serve as a single comprehensive reference in the field of wireless security.

In this book, the basic concepts, terms, protocols, systems, architectures, and case studies in the wireless security are provided. It identifies the fundamental problems, key challenges, and future directions in designing secure wireless systems. It covers a wide spectrum of topics in a variety of wireless networks, including attacks, secure routing, encryption, decryption, confidentiality, integrity, key management, identity management, and also security protocols in standards.

The chapters of this book are authoritatively contributed by a group of internationally renowned experts on wireless security. They are organized in four sections:

- Section I: Security Fundamentals
- Section II: Security in 3G/B3G/4G
- Section III: Security in Ad Hoc and Sensor Networks
- Section IV: Security in Wireless PAN/LAN/MAN

Section I introduces the basic concepts and fundamental mechanisms of wireless security. This section is able to provide the necessary background for readers and introduce all the fundamental issues on wireless security without previous knowledge on this area. Section II discusses all the security aspects in 3G/B3G/4G. It is well known that 3G mobile systems offer mobile users content rich services, wireless broadband access to Internet, and worldwide roaming. Future 4G mobile communication networks are expected to provide all IP-based services for heterogeneous wireless access technologies, assisted by mobile IP to provide seamless Internet access for mobile users. However the broadcast nature of the wireless communication and increased popularity of wireless devices introduce serious security vulnerabilities. A variety of security issues regarding 3G/B3g/4G will be introduced and addressed with effective solutions (e.g., identity management, confidentiality and integrity mechanisms, evaluation of the current 3G/B3G/4G security protocols, analysis of the impact of security deployment upon the network performance, etc.). Section III explores the security in ad hoc and sensor networks. In recent years, tremendous technological advances have been made in the areas of wireless ad hoc and sensor networks. Such networks have a significant impact on a variety of applications including scientific, military, medical, industrial, office, home, and personal domains. However, these networks introduce new security challenges due to their dynamic topology, severe resource constraints, and absence of a trusted infrastructure. Many aspects of security issues regarding the ad hoc and sensor networks will be covered, including key management, cryptographic protocols, authentication and access control, intrusion detection and tolerance, secure location services, privacy and anonymity, secure routing, resilience against different types of attacks, and so forth. Section IV exploits the security problems in wireless PAN/LAN/MAN. Nowadays we have continuously growing markets for the wireless PANs, wireless LANs, and wireless MANs, but there is a big black hole in the security of this kind of network. Diverse aspects of the security issues on these types of networks will be introduced. For instance, the threats and vulnerabilities in wireless LANs, access control in wireless LANs, evaluating security mechanisms in wireless PANs, the protocols and mechanisms to enhance the security of wireless LANs/MANs, security issues in WiMAX, and so forth are discussed. Practical examples will also be introduced to enhance the understanding.

This book can serve as an essential and useful reference for undergraduate and graduate students, educators, scientists, researchers, engineers, and research strategists in the field of wireless security.

We hope that by reading this book the reader can not only learn the basic concepts of wireless security but also get a good insight into some of the key research works in securing the wireless networks. Our goal is to provide an informed and detailed snapshot of this fast moving field. If you have any feedback or suggestion, please contact the editors.

Yan Zhang, Jun Zheng, and Miao Ma