Preface

Along with the rapid development of wideband wireless communication networks, wireless security has become a critical concern. Traditionally, in current wired or wireless communication networks, the issue of security is viewed as a whole independent feature addressed above the physical layer and cryptographic protocols are widely used to guarantee the security of the network. And the cryptographic protocols are designed assuming the physical layer has already been established and is error free. However, this assumption is usually impractical in the case of wireless communication. Compared with wireline networks, wireless networks lack a physical boundary due to the broadcasting nature of wireless transmissions. Any receivers nearby can hear the transmissions, and can potentially listen/analyze the transmitted signals, or conduct jamming. This unique physical-layer (PHY) weakness has motivated innovative PHY security designs in addition to, and integrated with, the traditional data encryption approaches.

One of the fundamental issues for PHY security is defined as information theoretic security, i.e., the adversary's received signal gives no more information for eavesdropping than legitimate receiver. The information-theoretic secrecy was first introduced by Shannon. "Perfect Secrecy" is defined by requiring of a system that after a cryptogram is intercepted by the enemy the a posteriori probabilities of this cryptogram representing various messages be identically the same as the a priori probabilities of the same messages before the interception. It is shown that perfect secrecy is possible by two approaches. First, perfect secrecy is possible but requires, if the number of messages is finite, the same number of possible keys. Second, perfect information theoretic secrecy requires that the signal Z received by the eavesdropper does not provide any additional information about the transmitted message W. Therefore, the build-in security of PHY security is also defined as: no secret keys are required before transmission.

In information-theoretic secrecy, channel noise plays a role of randomness resource. This book gives a review of the previous outstanding works of PHY security, and then provides the recent achievements on the confidentiality and authentication for wireless communications systems by channel identification. The first chapter introduces the PHY confidentiality and authentication concept. Chapter 2 introduces a practical approach to build unconditional confidentiality for

wireless communication security by feedback and error correcting code. In wireless channels, multiple antennas can increase system robustness against fading, and also transmission rates, as well as providing valid ways to realize information-theoretic secrecy. A framework of PHY security based on space time block code (STBC) MIMO system is introduced in Chap. 3. Innovative cross-layer security designs with both PHY security and upper-layer traditional security techniques are desirable for wireless networks. In this chapter, we also present a scheme that combines cryptographic techniques implemented in higher layers with the physical layer security approach using redundant antennas of MIMO systems to provide stronger security for wireless networks. The channel responses between communication peers have been explored as a form of fingerprint with spatial and temporal uniqueness. Chapters 4 and 5 fulfill this idea and develop a new lightweight method of channel identification for Sybil attack and node clone detection in wireless sensor networks (WSNs).