Chapter 3
Physical Layer Security and Its Applications: A Survey

Rajesh K. Sharma
Ilmenau University of Technology, Germany

ABSTRACT

This chapter provides a survey of physical layer security and key generation methods. This includes mainly an overview of ongoing research in physical layer security in the present and next generation communication networks. Although higher layer security mechanisms and protocols address wireless security challenges in large extent, more security vulnerabilities arise due to the increasingly pervasive existence of wireless communication devices. In this context, the focus of this chapter is mainly on physical layer security. Some security attacks in general are briefly reviewed. Models of physical layer security, information theoretic works, and key generation methods including quantization and reconciliation are discussed. Some latest developments for enhanced security like Multiple-Input Multiple-Output (MIMO) systems, reconfigurable antennas, and multiple relay systems are also presented. Finally, some existing and emerging application scenarios of physical layer security are discussed.

INTRODUCTION

Secure transmission is a concern for wireless devices and networks due to the broadcast nature of signals. As wireless devices become increasingly pervasive, they are more and more likely to serve both as targets for attack and as means for such attacks to be carried out successfully (Trappe et al., 2011). While there are a number of traditional methods for establishing secure keys using conventional secure channel or later developed public key cryptosystems and distribution systems (Diffie & Hellman, 1976), there have been numerous attempts to make various wireless

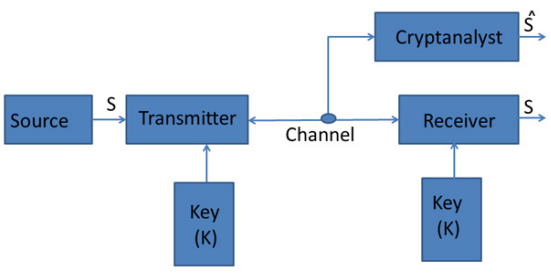
DOI: 10.4018/978-1-4666-4691-9.ch003

platforms secure by migrating traditional network security strategies to the wireless domain. In spite of these efforts, the security failures have also been continuously reported.

While conventional cryptographic security mechanisms are essential to the overall problem of securing wireless networks, they do not directly leverage the unique properties of the wireless domain to address security threats (Mathur et al., 2010). The wireless medium itself can be a powerful source of secure key that can complement and enhance traditional security mechanisms. New security paradigms which exploit physical layer properties of the wireless medium, such as the rapid spatial, spectral, and temporal decorrelation properties of the radio channel, can enhance confidentiality and authentication services (Mathur et al., 2010).

Figure 1 shows information flow in a traditional cryptographic system, where the key (K) is trans- mitted by the source to the receiver using a secure channel or an insecure public channel. In a wireless communication, the strongest notion of security is in an information theoretic sense, where the Transmitter (commonly known as Alice) and Receiver (commonly known as Bob) can share information up to the secrecy capacity, without providing any information to the Cryptanalyst (commonly known as Eve) (Massey, 1988). Although

Figure 1.Flow of information in a cryptographic system where the key (K) may be transmitted only to the legitimate receiver via a secure channel (conventional cryptography), or transmitted publicly (public cryptography) (Diffie & Hellman, 1976).



traditional systems employ private or public-key cryptography without considering the physical transmission, there is growing interest in physical layer security methods that exploit the properties of the propagation channel to strengthen existing cryptosystems (see (Bloch, Barros, Rodrigues, & McLaughlin, 2008) and references therein).

Several information-theoretic studies have been performed for secrecy in wireless communication. For example, in (Ahlswede & Csiszar, 1993), information-theoretic models of secret sharing are considered for "wiretap channel" where the concept of key-capacity has been provided and formulas and bounds to key-capacity for different models have been derived. In (Maurer, 1993) it has been proven that matching secret keys can be generated by Alice and Bob by exploiting knowledge of the physical channel and public discussion over an error-free channel. In the case of fading channels, it has been shown in (Barros & Rodrigues, 2006) that positive secrecy capacity exists without the need for a feedback channel or public discussion, and in (Bloch et al., 2008) a practical method for generating secret keys without public discussion has been developed. However, one drawback of such approaches is that both Alice and Bob require at least partial channel state information (CSI) of their own channel as well as the eavesdropper channel. The former may require a feedback channel, potentially sharing useful information with Eve, and the latter may not be obtainable in practice.

In recent years, there has been keen interest in physical layer security. There are several papers published whose contributions range from are largely theoretical to application related issues including channel properties, MIMO and Relay techniques, use of reconfiguration antennas, and new application areas like optical layer security, security in satellite communications and smart grids, etc. Some experimental works of physical layer security are also available. While many information-theoretic aspects and implementation issues of physical-layer security are still to be ex-