Chapter 2
Secure Communications over Wireless Networks

Md. Zahurul Islam Sarkar
Queen's University Belfast, UK

ABSTRACT

Nakagami-m fading channel is chosen to analyze the secrecy capacity for fading channels since the Nakagami-m distribution can model fading conditions, which are more or less severe than that of Rayleigh and has the advantage of including Rayleigh as a special case. At first, secrecy capacity is defined in case of full channel state information (CSI) at the transmitter, where transmitter has access to both the main channel and eavesdropper channel gains. Secondly, secrecy capacity is defined with only main channel CSI at the transmitter. Then, optimal power allocation at the transmitter that achieves the secrecy capacity is derived for both the cases. Moreover, secrecy capacity is defined under open-loop transmission scheme, and the exact closed form analytical expression for the lower bound of ergodic secrecy capacity is derived for Nakagami-m fading single-input multiple-output (SIMO) channel. In addition, secrecy capacity is defined for the AWGN channel in order to realize the information-theoretic security of wireless channels with no fading. Finally, analytical expressions for the probability of non-zero secrecy capacity and secure outage probability are derived in order to investigate the secure outage performance of fading channels.

1. INTRODUCTION

This chapter is concerned with the study of secrecy capacity and secure outage performance for the wireless channels, focusing on the recent research of secure communications where a legitimate user communicates with a legitimate receiver in the presence of an eavesdropper. Perfect secrecy is achieved when the transmitter and the legitimate receiver can communicate at some positive rate, while insuring that eavesdropper gets zero bits of information. Specifically, two different channels, such as fading and additive white Gaussian noise (AWGN) channels are considered for the study. The open nature of wireless communication network makes it susceptible to eavesdropping and fraud. As a result, the privacy and security

DOI: 10.4018/978-1-4666-1797-1.ch002

in wireless communication networks have taken on an increasingly important role, as these networks are used to transmit personal information. Moreover, the problems of cryptography and secrecy systems furnish an interesting application of communication theory. Traditionally, channel fading has been viewed as a source of unreliability of communication. Therefore, the natural problem of great interest is, how we can achieve high data rates with reliability in spite of the harsh wireless channel subject to the fading, limited power and bandwidth resources. Since the goal of this work is to achieve reliable communication at the maximum possible data rate, the relevant information-theoretic measure is secrecy capacity (i.e. the maximum transmission rate at which the eavesdropper is unable to decode any information) of the channel. The probability of non-zero secrecy capacity and secure outage probability are the measures of secure outage performance for the relevant channel model. Moreover, security issues arising in wireless communication networks include *confidentiality*, integrity, authentication and nonrepudiation. Confidentiality is the measure of reliability which guarantees that legitimate receiver successfully receives the intended information from the source node, while eavesdroppers are unable to decode any information from the intended information. Integrity guarantees that original information sent by the source node is not modified by the eavesdroppers during its transmission. Authentication ensures that a recipient of information i.e. legitimate receiver is able to identify the sender of received information i.e. the source of original information from which the information has been sent. Nonrepudiation ensures that a sender of information is not able to deny having transmitted that information and the recipient is not able to deny having received the information.

1.1 Information-Theoretic Analysis of Cryptosystem

The conception of *information-theoretic security* was first introduced by Shannon (Shannon, 1949) to characterize fundamental limits of secure communications over wireless channels. Shannon considers a scenario as shown in Figure 1 where transmitter end contains two information sources such as a message source and a key source. The message source produces a message W which is enciphered to a cryptogram E by a key K shared by the transmitter and receiver. The cryptogram E is sent to the receiving end by a possible interceptible means and the key K is produced by a key source which is transmitted to the receiving end by a messenger. The key must be transmitted by non-interceptible means from transmitter to the receiving point. Sometimes it must be memorized.

Figure 1. Schematic diagram of a cryptosystem