Chapter 6
Secret Communication Under Channel Uncertainty*

Yingbin Liang, H. Vincent Poor and Shlomo Shamai (Shitz)

6.1 Introduction

A basic measure of secrecy for communications was provided by Shannon via the information theoretic entropy rate in [1]. Based on this measure, secure communication over noisy communication channels was studied by Wyner within the wire-tap channel model in [2]. In this channel, a transmitter exploits the difference between the channel randomness to its legitimate receiver and to an eavesdropper, and employs a stochastic encoding scheme to benefit the legitimate receiver while guaranteeing no information leakage to the eavesdropper. Compared to the prevalent cryptographic approaches to achieve secure communication, such an information theoretic approach does not need “keys” to encrypt and decrypt the source messages.

Alternatively, information theory also provides approaches to achieve secret key agreement for remote terminals by exploiting source and/or channel randomness available at these terminals. Such a common secret key can hence be used for secure communication via cryptographic secret-key algorithms. In this case, information theory helps key management (including key generation and distribution). We refer the reader to [3–19] and references therein for this topic, whereas the focus of this chapter is on the wire-tap channel.

Compared to contemporary cryptosystems, the information theoretic approaches to guarantee security have the advantages of either eliminating the key management issue entirely or exploiting powerful coding techniques in the physical layer to achieve key agreement, thereby resulting in significantly lower complexity and savings in resources. Furthermore, physical layer security approaches achieve provable

Y. Liang (✉)
Department of Electrical Engineering
University of Hawaii, Honolulu
HI 96822, USA
e-mail: yingbinl@hawaii.edu

security that is robust to eavesdroppers possessing unlimited computational resources, knowledge of the communication strategy employed including coding and decoding algorithms, and access to communication systems either through perfect or noisy channels.

The recent emergence and increasing ubiquity of wireless networks, and in particular of networks with minimal infrastructure, have spurred considerable interest in the information theoretic security in very recent times (see, e.g., [20–58] and the reference therein). In particular, the promise of this potentially very powerful approach for use in mobile and other wireless networks has been brought to the attention of the wireless networking community. However, to fully exploit information theoretic security in wireless networks, one major challenge is to design secure communication strategies for the time-varying channel, which is an important intrinsic characteristic of wireless communications. This chapter focuses on this topic.

A number of models can be used to describe various wireless communication scenarios. One common property of these models is that the channel may take multiple states, while channel state information (CSI) may or may not be available at the transmitter, the receiver, or the eavesdropper. The parallel wire-tap channel and the ergodic fading wire-tap channel are models that capture the situation in which there are no delay constraints. Alternatively, the block fading wire-tap channel is useful for studying outage performance when there are delay constraints. The compound wire-tap channel assumes that the channels to the legitimate receiver and to the eavesdropper take a number of states, and secure communication must be guaranteed no matter which state occurs. The compound channel does not allow coding across different states, and guarantees robust performance under delay constraints. To draw the connection between robustness and outage performance, robustness requires zero-outage probability. Another useful model is the wire-tap channel with side information which models the situation in which the channel state is non-causally known at the transmitter only, and this information helps improve the secrecy performance. This chapter reviews recent progress on characterizing the secrecy of these channel models, and discusses some interesting open problems in this area.

6.2 Wire-Tap Channel Model

In this section, we introduce the wire-tap channel model, and review results on the secrecy capacity of this channel. We will further discuss the Gaussian, the multi-input multi-output (MIMO), and the parallel wire-tap channels, which serve as basic information-theoretic models for the fading wire-tap channel.

6.2.1 Discrete Memoryless Wire-Tap Channel

The wire-tap channel was first introduced and studied by Wyner in [2]. This channel includes a transmitter that wishes to transmit a source sequence (a message $W$) to a legitimate receiver and wishes to keep this message as secret as possible from an