CCIT Report #650 November 2007

A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel

Tie Liu and Shlomo Shamai (Shitz)

November 15, 2007

Abstract

The secrecy capacity of the multi-antenna wiretap channel was recently characterized independently by Khisti and Wornell [1] and Oggier and Hassibi [2] using a Sato-like argument and matrix analysis tools. This note presents an alternative characterization of the secrecy capacity of the multi-antenna wiretap channel using a channel enhancement argument. This characterization is by nature information rather than matrix theoretic, and is directly built on the physical intuition regarding to the optimal transmission strategy in this communication scenario. A secure V-BLAST transmission and receiver architecture is proposed to achieve the secrecy capacity of the multi-antenna wiretap channel.

1 Introduction

Consider a multi-antenna wiretap channel with n_t transmit antennas and n_r and n_e receive antennas at the legitimate recipient and the eavesdropper, respectively:

$$\begin{array}{rcl} \mathbf{y}_r[m] & = & \mathbf{H}_r\mathbf{x}[m] + \mathbf{w}_r[m] \\ \mathbf{y}_e[m] & = & \mathbf{H}_e\mathbf{x}[m] + \mathbf{w}_e[m] \end{array} \tag{1}$$

where $\mathbf{H}_r \in \mathbb{R}^{n_r \times n_t}$ and $\mathbf{H}_e \in \mathbb{R}^{n_e \times n_t}$ are the channel gain matrices associated with the legitimate recipient and the eavesdropper. The channel gain matrices $\mathbf{H}_r$ and $\mathbf{H}_e$ are assumed to be fixed during the entire transmission and are known to all three terminals. The additive noise $\mathbf{w}_r[m]$ and