A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security

Theofilos Chrysikos, Tasos Dagiuklas, and Stavros Kotsopoulos

Wireless Telecommunications Laboratory
Department of Electrical & Computer Engineering
University of Patras – 26500 Greece
{txrysiko,ntan,kotsop}@ece.upatras.gr

Abstract. This paper provides a closed-form expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security. This is accomplished on the basis of an approximation of the exponential function via a first-order Taylor series. The error of this method is calculated for two different channel cases, and the resulting precision confirms the correctness of this approach. Thus, the Outage Secrecy Capacity can be calculated for a given Outage Probability and for a given propagation environment (path loss exponent, average main channel SNR), allowing us to estimate with increased precision the boundaries of secure communications.

Keywords: Wireless Information-Theoretic Security; quasi-static Rayleigh fading; Outage Secrecy Capacity; Taylor approximation; path loss exponent.

1 Introduction

Security remains an issue of utmost importance in wireless communications. For all the advances and breakthrough progress in both industry and academia, security still provides a fertile ground for extensive research and innovative solutions. It is imperative to begin with a brief overview of background work in the field of wireless security from an information-theoretic standpoint.

1.1 Background Work

Based on Shannon's definition of *perfect secrecy* [1], innovative research was carried out in the latter half of the 1970s, investigating the impact of the wireless channel on the boundaries of secure communications [2]-[4]. Both the main and the wiretap channel were considered to be Gaussian. This proved to be the first major setback in the ongoing research, due to the limitation that the average SNR of the main (legitimate) channel had to be greater than the average SNR of the wiretap channel (eavesdropper's channel) so that secure communication over the wireless interface would be guaranteed. To make matters worse, the lack of channel coding schemes at the time prevented researchers from coming up with a flexible and reliable solution to the situation at hand. Information-theoretic solutions for wireless security were seemingly brought to a quick ending, and the interest of public research was drawn towards

Q. Gu, W. Zang, and M. Yu (Eds.): SEWCN 2009, LNICST 42, pp. 3–12, 2010.

higher layer, more sophisticated schemes that paved the way for the transition from "weak" to "strong" secrecy, incorporating cryptography schemes [5]-[8].

Recent work, however, has re-approached the issue of physical layer-based security for wireless communication under a new light by developing the concept of Wireless Information-Theoretic Security.

1.2 Wireless Information-Theoretic Security

In [9],[10] Bloch, Barros, Rodrigues and McLaughlin suggest that the wireless communication between a transmitter and a (legitimate) receiver in the presence of a malicious user (eavesdropper) can be secure even when the SNR of the main channel is lower than the SNR of the eavesdropper. This is possible when quasi-static Rayleigh fading channels are considered, instead of the classic Gaussian scenario.

The outage probability for a given Secrecy Rate $R_s > 0$ (defined as the probability that the Secrecy Capacity will be smaller than a non-zero secrecy rate) is calculated as an expression of the average main and wiretap channel SNR, $\overline{\gamma}_M$ and $\overline{\gamma}_W$ respectively:

$$P_{out}\left(C_s < R_s\right) = P_{out}(R_s) = 1 - \frac{\overline{\gamma}_M}{\overline{\gamma}_M + 2^{R_s}\overline{\gamma}_W} e^{\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right)} \tag{1}$$

The practical implementation of this information-theoretic scheme can be achieved via the use of LDPC channel coding as shown in [11],[12].

1.3 Impact of the Propagation Environment

In [9],[10] the intrinsic characteristics of the propagation environment were examined by assigning a value of n=3 to the path loss exponent [13]. Thus the Outage Probability is calculated by:

$$P_{out}\left(C_s < R_s\right) = P_{out}\left(R_s\right) = 1 - \frac{e^{\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right)}}{1 + 2^{R_s}\left(\frac{d_M}{d_W}\right)^n} \tag{2}$$

This however does not correspond to realistic cases where the path loss exponent can assume a wide range of values [14], from n=1.8 (indoor LOS cases) up to n=3.8 and even n=4 (indoor complex NLOS topology, outdoor urban shadowed dense area). In [15], the impact of this channel-dependent variation of path loss exponent on the non-zero probability of Secrecy Capacity and the Outage Probability was examined.

In all published works so far, however, another important parameter, the Outage Secrecy Capacity, has not been properly and thoroughly investigated.