Physical Communication 4 (2011) 313–321

Contents lists available at SciVerse ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation☆

Nabil Romero-Zurita [a,*], Mounir Ghogho [a,b], Des McLernon [a]

[a] School of Electronic and Electrical Engineering, University of Leeds, LS2 9JT, Leeds, United Kingdom
[b] International University of Rabat, Morocco

ARTICLE INFO

Article history:
Received 10 October 2011
Received in revised form 13 October 2011
Accepted 14 October 2011
Available online 26 October 2011

Keywords:
Physical layer security
Passive eavesdropping
Beamforming
Artificial noise
MIMO
OFDM

ABSTRACT

In this paper we address physical layer security in multiple-input-multiple-output (MIMO) frequency selective wireless channels in the presence of a passive eavesdropper, i.e., the associated channel is unknown to the transmitter. Signalling is based on orthogonal frequency division multiplexing (OFDM). Spatial beamforming and artificial noise broadcasting are chosen as the strategy for secure transmission. The contribution of channel frequency selectivity to improve secrecy is presented by performance and probabilistic analysis. Moreover, we investigate the capability of the eavesdropper to jeopardize the security of the system (defined as the SNR difference between the intended receiver and the eavesdropper) by mitigating the interfering effect of the artificial noise using zero forcing as a receive beamforming strategy. The results show that although zero forcing is not the optimal strategy to maximize the SNR, it offers (from the eavesdropper's perspective) a better performance than MMSE for MIMO frequency selective channels and thus threatens the overall security of the system.

1. Introduction

Eavesdropping is a well-known security vulnerability shared by all wireless networks due to their broadcast nature. It occurs when a non-authorized party hears a secret conversation between two nodes in the network. The way to partially prevent eavesdroppers' attacks is currently based on computationally demanding cryptographic algorithms implemented in the upper layers of the communication model. As an alternative to these complex cryptographic techniques, physical layer security has recently emerged as a way to augment the system security by exploiting the spatio-temporal variations of the wireless channel.

Physical layer foundations were established in seminal papers [1–3] where, from an information-theoretic perspective, it was shown that perfect secrecy can be guaranteed in AWGN channels when the quality of the transmitter-to-receiver channel is better than that of the transmitter-to-eavesdropper channel. Under this condition a non-zero secrecy data rate can be achieved. The maximum data rate at which this secret communication can be held is known as secrecy capacity and is a function of the signal-to-noise ratios (SNRs) of the links between both transmitter-to-receiver and transmitter-to-eavesdropper. In a fading channel, it was shown in [4,5] that it is still possible to achieve secrecy even if the average SNR of the eavesdropper's channel is better than that of the legitimate receiver's channel.

The system information available at the transmitter plays a critical role for guaranteeing secrecy. Indeed, secrecy capacity can be computed if the channel-state-information (CSI) of both links is available at the transmitter (i.e., transmitter-to-receiver and transmitter-to-eavesdropper). This description corresponds to the

☆ Part of this work was presented at the 19th European Signal Processing Conference (EUSIPCO 2011), Barcelona, Spain, August 2011.

* Corresponding author. Tel.: +44 7522042245; fax: +44 1133432032.
E-mail addresses: el08lnrz@leeds.ac.uk (N. Romero-Zurita), m.ghogho@leeds.ac.uk (M. Ghogho), d.c.mclernon@leeds.ac.uk (D. McLernon).

1874-4907/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.phycom.2011.10.004

active eavesdropping scenario. In the most common and practical situation, the eavesdropper's CSI is unknown at the transmitter (i.e., passive eavesdropping), so secrecy capacity cannot be determined and thus perfect secrecy cannot be guaranteed. In this context, and with the aim of defining secrecy, in [4] the concept of outage probability of secrecy is introduced as the probability that the instantaneous secrecy capacity falls below a predefined target secrecy rate. Another approach to define secrecy in a passive eavesdropping system is to use security constraints given by quality-of-service (QoS) bounds on the SNRs of the legitimate receiver and eavesdropper links based on the statistics of the CSI [6,7].

The contribution that multiple antennas offer to secrecy is studied in [8–10]. In [11,12] beamforming is shown as the optimal strategy for maximizing the secrecy capacity in multiple-input-single-output (MISO) systems. In [13,14] artificial noise (AN) is transmitted over the null space of the intended receiver's channel as a way to confuse eavesdroppers and also improve the secrecy of the system by not affecting the quality of the main link (i.e., transmitter-to-receiver). Therefore, taking advantage of the positive contributions of beamforming and AN generation to the secrecy of the passive eavesdropping system, several works have proposed techniques to allocate the available transmit power (i.e., between the information-bearing signal and AN) in order to minimize the outage probability of secrecy or to ensure a given SNR to satisfy QoS constraints.

In [15,16] the average lower bound secrecy capacity is maximized when eavesdroppers' CSI is not available at the transmitter. This leads to an equal power distribution between the information and AN. With the aim of guaranteeing a given SNR at the intended receiver, in [6] only the minimum necessary power is devoted for information transmission while the remaining available power is allocated for isotropic AN broadcasting. In [17] this security condition is used to introduce robust beamforming techniques for multiple-input-multiple-output (MIMO) systems as a way to overcome the imperfect CSI availability at the transmitter. This security definition is extended in [7] to also guarantee (on average) a given SNR at the eavesdropper. Here the authors assume either partial or complete eavesdropper's statistical CSI knowledge to transmit AN towards the eavesdropper's direction rather than in an isotropic fashion as in [6]. The power allocation is translated into a joint optimization problem solved by convex optimization and semidefinite relaxation techniques to determine the optimum beamformer and AN spatial distribution. In [18], an approach that uses beamforming and AN generation is introduced to quantify the probability of secrecy in the presence of a random network of eavesdroppers whose locations and channels are unknown. Stochastic geometry was used to probabilistically characterize secrecy.

In all the above mentioned references (i.e., [6,7,15–18]) secrecy is studied by beamforming and AN generation in flat fading channels, however, in [18] the idea that frequency selectivity can improve secrecy is mentioned. In this context, in this paper, we investigate this idea to present a novel quantitative analysis of the secrecy improvement resulting from frequency selectivity in MIMO–OFDM systems. With this aim, we first use water-filling to distribute power across the subcarriers and then for each carrier allocate the power between the information-bearing signal and AN. Three schemes are used to allocate power. First, we transmit information using the minimum required power to achieve a specified SNR and then allocate the rest of the power to the AN. Second, we distribute power equally between information and AN to finally progressively vary the power devoted to the AN in order to understand its contribution to the secrecy of the OFDM–MIMO system. Furthermore, and in contrast with [6,17,18] where minimum mean square error (MMSE) estimation is used to maximize the SNR at the eavesdropper side, here we will investigate a simple method based on zero forcing (ZF) through which the eavesdropper can minimize, even null, the interfering effect of the AN which threatens the overall security of system. The effects of increasing the number of antennas and subcarriers on secrecy are then studied via simulations.

This paper is organized as follows. Section 2 provides the general problem formulation and also the transmit and receive strategies. Here the different approaches considered for allocating power and beamforming are detailed in different subsections to then introduce the concept of probability of secrecy that will be used to characterize secrecy. In Section 3, after describing the simulation methodology used, results are presented. First we show the contribution of frequency selectivity to the secrecy of the system and then compare the performance offered for the different receive beamforming methods. In Section 4 we present a brief discussion about the practical capability and requirements for the eavesdropper to put at risk the system security. Finally, Section 5 concludes the paper.

2. System and signal models

In this section, we formulate the security problem for a MIMO system using both beamforming and AN generation as a transmit strategy. We assume that a single eavesdropper is equipped with multiple antennas. Note that this can also be viewed as multiple single antenna colluding eavesdroppers (i.e., eavesdroppers working in a cooperative fashion). Following the well known cryptographic model, the legitimate transmitter and receiver are named Alice and Bob, and the eavesdropper is referred to as Eve.

2.1. System model

We consider OFDM signalling. Alice, Bob and Eve are respectively equipped with N_t, N_r, and N_e antennas. $\mathbf{H}$ and $\mathbf{H}_e$ denote the MIMO Alice-to-Bob and Alice-to-Eve frequency selective channels of L multipath taps. The channel taps are modelled as independent, zero-mean complex $(N_r \times N_t)$ and $(N_e \times N_t)$ matrices respectively. We assume a passive eavesdropping scenario, and so $\mathbf{H}$ is perfectly known to Alice while $\mathbf{H}_e$ remains unknown to her. The system is depicted in Fig. 1.

The frequency selective multipath channel with L taps is represented by an equivalent OFDM system of N parallel frequency flat fading channels. Let $\mathbf{s}_{(m)}$ denote the beamformed signal vector transmitted by Alice over the