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

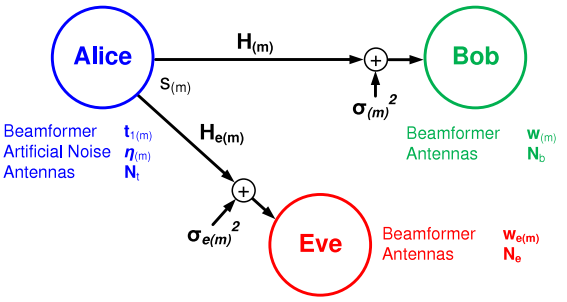

Fig. 1. System model. Wireless transmission between the transmitter and the intended receiver in the presence of an eavesdropper over MIMO–OFDM frequency selective channels. The subscript '*m*' refers to the equivalent flat-fading channel for the *m*th subcarrier.

*m*th subcarrier, $m \in [0, 1, \ldots, N-1]$. Thus, the signal vectors received by Bob and Eve on the *m*th subcarrier are respectively given by

$$\mathbf{u}_{(m)} = \mathbf{H}_{(m)}\mathbf{s}_{(m)} + \mathbf{n}_{(m)} \tag{1}$$

$$\mathbf{v}_{(m)} = \mathbf{H}_{e(m)}\mathbf{s}_{(m)} + \mathbf{n}_{e(m)} \tag{2}$$

where $\mathbf{H}_{(m)}$ and $\mathbf{H}_{e(m)}$ are the Alice-to-Bob and Alice-to-Eve frequency-domain channel matrices on the *m*th subcarrier. In addition, $\mathbf{n}_{(m)}$ and $\mathbf{n}_{e(m)}$ representing additive white Gaussian noise (AWGN) are mutually independent, zero-mean, complex, Gaussian random vectors with respective covariance matrices $\sigma^2_{(m)}\mathbf{I}$ and $\sigma^2_{e(m)}\mathbf{I}$ where $\mathbf{I}$ denotes the appropriate dimension identity matrix.

The covariance matrix of $\mathbf{s}_{(m)}$ is given by $\mathbf{C}_{s(m)} = \mathbb{E}\{\mathbf{s}_{(m)}\mathbf{s}^H_{(m)}\}$. The power allocated to the *m*th subcarrier is defined by $\rho_{(m)} = \mathrm{Tr}\{\mathbf{C}_{s(m)}\}$. We assume a total power constraint $\sum_{m=0}^{N-1}\rho_{(m)} = P$. Finally, a fraction $\epsilon_{(m)} \in [0, 1)$ of the power allocated to each subcarrier is devoted to AN generation. So the transmitted signal vector $\mathbf{s}_{(m)}$ is modelled as follows:

$$\mathbf{s}_{(m)} = \sqrt{\rho_{(m)}}\left(\sqrt{1-\epsilon_{(m)}}\mathbf{t}_{(m)}d_{(m)} + \sqrt{\epsilon_{(m)}}\boldsymbol{\eta}_{(m)}\right) \tag{3}$$

where $\mathbf{t}_{(m)}$ is a normalized $(N_t \times 1)$ beamforming vector, (i.e., $\|\mathbf{t}_{(m)}\| = 1$), $d_{(m)}$ is the transmitted scalar complex information symbol with $\mathbb{E}\{|d_{(m)}|^2\} = 1$, and $\boldsymbol{\eta}_{(m)}$ is the $(N_t \times 1)$ AN vector with covariance matrix $\mathbf{C}_{\eta(m)} = \mathbb{E}\{\boldsymbol{\eta}_{(m)}\boldsymbol{\eta}^H_{(m)}\}$.

2.2. Transmit beamforming, artificial noise generation and power allocation

We define the secrecy performance of the system by the difference between Bob's and Eve's SNRs. So with the aim of increasing the secrecy of the system, beamforming and AN are chosen as the transmit strategy. So following [18], Alice chooses the beamforming vector $\mathbf{t}_{1(m)}$ as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{H}^H_{(m)}\mathbf{H}_{(m)}$. The AN vector $\boldsymbol{\eta}_{(m)}$ is then generated by the (weighted) linear combination of the remaining $N_t - 1$ eigenvectors (each with equal power) so $\boldsymbol{\eta}_{(m)}$ will lie in the nullspace of $\mathbf{H}_{(m)}$ and orthogonality between the AN vector and the beamformer is preserved $\left(\text{i.e., } \mathbf{t}^H_{1(m)}\boldsymbol{\eta}_{(m)} = 0\right)$. That is

$$\boldsymbol{\eta}_{(m)} = \frac{1}{\sqrt{N_t - 1}}\sum_{i=2}^{N_t}\mathbf{t}_{i(m)}\eta_i \tag{4}$$

where $\mathbf{t}_{i(m)}$ is the *i*th eigenvector of $\mathbf{H}^H_{(m)}\mathbf{H}_{(m)}$ and η_i is a random, complex scalar with unit magnitude and random phase uniformly distributed, (i.e., $\eta_i = e^{j\phi_i}$ and $\phi_i \in [0, 2\pi)$). Thus we have that

$$\mathbf{C}_{\eta(m)} = \frac{1}{N_t - 1}\sum_{i=2}^{N_t}\mathbf{t}_{i(m)}\mathbf{t}^H_{i(m)}. \tag{5}$$

With the aim of incrementing the secrecy of the system by allocating more power to the best subcarriers in an opportunistic fashion, following [19] the total power P is distributed among the N subcarriers using the water-filling technique as follows:

$$\rho_{(m)} = \max\left(0, \frac{1}{\hat{N}}\left(\hat{P} + \sum_{i=1}^{N}\frac{1}{\gamma_{(i)}}\right) - \frac{1}{\gamma_{(i)}}\right) \tag{6}$$

$$\text{s.t.} \sum_{m=1}^{N}\rho_{(m)} = \hat{P} = \frac{PN}{N+\mu}. \tag{7}$$

In (6) and (7) $\hat{N}$ is the number of subcarriers which have $\rho_{(m)} \neq 0$ after the initial power allocation, and $\hat{P}$ is the available power for information once the power requested for the transmission of the cyclic prefix of length μ is considered. Finally, the channel's power to noise ratio $(\gamma_{(i)})$ is given by

$$\gamma_{(i)} = \frac{\|\mathbf{H}_{(i)}\|^2_F}{N_t N_r \sigma^2_{(m)}} \tag{8}$$

where $\|\cdot\|_F$ denotes the Frobenius norm.

Once the powers per subcarrier $\{\rho_{(m)}\}$ have been determined, $(1-\epsilon_{(m)})\rho_{(m)}$ is used to transmit the information signal and $\epsilon_{(m)}\rho_{(m)}$ is allocated to broadcast AN.

Throughout this paper we consider three different approaches for allocating the power between the information and the AN. The first one follows the idea introduced in [6] and defines the parameter $\epsilon_{(m)}$ in such way that secrecy is guaranteed based on satisfying a minimum target SNR at Bob on the *m*th subcarrier, $\overline{\mathrm{SNR}}_{(m)}$. Hence, $\epsilon_{(m)}$ is obtained as

$$\epsilon_{(m)} = 1 - \frac{\overline{\mathrm{SNR}}_{(m)}\sigma^2_{(m)}}{\rho_{(m)}\nu_{1(m)}} \tag{9}$$

where $\nu_{1(m)}$ is the largest eigenvalue of $\mathbf{H}^H_{(m)}\mathbf{H}_{(m)}$.

The second way to distribute the power is based on the results in [15]. Here the power is equally distributed between information and AN in order to maximize the ergodic secrecy capacity of the system (i.e., $\epsilon_{(m)} = 0.5\ \forall m$). Finally, and with the aim of understanding the impact of the AN over the secrecy of the system, the fraction of power committed to AN generation given by the parameter $\epsilon_{(m)}$ is progressively varied.

2.3. Receive beamforming by maximal ratio combining

At the receiver side, Bob chooses maximal ratio combining (MRC) as the multiple antennas combining

technique in order to maximize the received SNR of $y_{(m)_{\mathrm{MRC}}} = \mathbf{w}^H_{(m)_{\mathrm{MRC}}}\mathbf{u}_{(m)}$. Hence the optimum beamformer vector at the mth subcarrier is given by

$$\mathbf{w}_{(m)_{\mathrm{MRC}}} = \mathbf{H}_{(m)}\mathbf{t}_{1(m)}. \tag{10}$$

So Bob's SNR at the mth subcarrier can be calculated as follows:

$$\mathrm{SNR}_{(m)} = \left(1-\epsilon_{(m)}\right)\rho_{(m)}\mathbf{t}^H_{1(m)}\mathbf{H}^H_{(m)}\left[\sigma^2_{(m)}\mathbf{I}\right]^{-1}\mathbf{H}_{(m)}\mathbf{t}_{1(m)}. \tag{11}$$

2.4. Receive beamforming using the minimum mean square error approach

Eve attempts to recover the maximum possible information from the Alice-to-Bob transmission. So from her point of view the best multiple antenna combining method will be the one that provides the highest SNR. This condition represents the worst case for the security of the system. In this context, as in [6,17,18], Eve uses MMSE as an optimal receiver structure to maximize the SNR. In order to calculate the beamformer vector, it is assumed that Eve is somehow aware of $\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}$, the AN covariance matrix $\mathbf{C}_{\eta(m)}$ and the power $(\epsilon_{(m)}\rho_{(m)})$ allocated for the AN.

Under this assumption, Eve's MMSE beamformer at the mth subcarrier is given by

$$\mathbf{w}_{e(m)_{\mathrm{MMSE}}} = \mathbf{\Psi}\mathbf{H}_{e(m)}\mathbf{t}_{1(m)} \tag{12}$$

where

$$\mathbf{\Psi} = \left(\epsilon_{(m)}\rho_{(m)}\mathbf{H}_{e(m)}\mathbf{C}_{\eta(m)}\mathbf{H}^H_{e(m)} + \sigma^2_{e(m)}\mathbf{I}\right)^{-1}. \tag{13}$$

Bearing in mind that Eve's scalar signal at the output of the beamformer is given by $y_{e(m)_{\mathrm{MMSE}}} = \mathbf{w}^H_{e(m)_{\mathrm{MMSE}}}\mathbf{v}_{(m)}$, then Eve's SNR at the mth subcarrier is given by

$$\mathrm{SNR}_{e(m)_{\mathrm{MMSE}}} = \left(1-\epsilon_{(m)}\right)\rho_{(m)}\mathbf{t}^H_{1(m)}\mathbf{H}^H_{e(m)}\mathbf{\Psi}\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}. \tag{14}$$

2.5. Receive beamforming by zero forcing

In this subsection we address the case when Eve, through knowledge of the transmitting strategy used by Alice, is able to mitigate the interfering effect of AN. Under the same assumptions noted in the above section, (i.e., Eve knows $\mathbf{H}_{e(m)}$ and $\mathbf{t}_{1(m)}$), let us consider using ZF to calculate Eve's beamformer vector as follows:

$$\mathbf{w}_{e(m)_{\mathrm{ZF}}} = \left(\mathbf{H}^{\dagger}_{e(m)}\right)^H\mathbf{t}_{1(m)} \tag{15}$$

with $\mathbf{H}^{\dagger}_{e(m)} = \left(\mathbf{H}^H_{e(m)}\mathbf{H}_{e(m)}\right)^{-1}\mathbf{H}^H_{e(m)}$ denoting the Moore–Penrose pseudo inverse. Note (from (2) and (3)) that we have not used the traditional ZF beamformer of $\left(\left(\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}\right)^{\dagger}\right)^H$ because of the AN term $\left(\sqrt{\epsilon_{(m)}}\boldsymbol{\eta}_{(m)}\right)$ in (3) which can be mitigated by (15).

Eve's scalar signal at the output of the beamformer is given by $y_{e(m)_{\mathrm{ZF}}} = \mathbf{w}^H_{e(m)_{\mathrm{ZF}}}\mathbf{v}_{(m)}$ and can be written as

$$\begin{aligned} y_{e(m)_{\mathrm{ZF}}} &= \sqrt{1-\epsilon_{(m)}}\sqrt{\rho_{(m)}}\mathbf{t}^H_{1(m)}\mathbf{H}^{\dagger}_{e(m)}\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}d_{(m)} \\ &\quad + \sqrt{\epsilon_{(m)}}\sqrt{\rho_{(m)}}\mathbf{t}^H_{1(m)}\mathbf{H}^{\dagger}_{e(m)}\mathbf{H}_{e(m)}\boldsymbol{\eta}_{(m)} \\ &\quad + \mathbf{t}^H_{1(m)}\mathbf{H}^{\dagger}_{e(m)}\mathbf{n}_{e(m)}. \end{aligned} \tag{16}$$

Here, assuming $N_e \geq N_t$, it is straightforward to see that the second term that contains the AN $(\boldsymbol{\eta}_{(m)})$ is cancelled due to $\mathbf{H}^{\dagger}_{e(m)}\mathbf{H}_{e(m)} = \mathbf{I}$ and $\mathbf{t}^H_{1(m)}\boldsymbol{\eta}_{(m)} = 0$.

Now, Eve's SNR at the mth subcarrier can be shown to be

$$\mathrm{SNR}_{e(m)_{\mathrm{ZF}}} = \left(1-\epsilon_{(m)}\right)\rho_{(m)}\mathbf{\Theta} \tag{17}$$

where:

$$\mathbf{\Theta} = \left[\sigma^2_{e(m)}\mathbf{t}^H_{1(m)}\mathbf{H}^{\dagger}_{e(m)}\left(\mathbf{H}^{\dagger}_{e(m)}\right)^H\mathbf{t}_{1(m)}\right]^{-1}. \tag{18}$$

If $N_e < N_t$, then the AN nulling operation will not be completely successful, so, in general, Eve's SNR at the mth subcarrier can be written as

$$\begin{aligned} &\mathrm{SNR}_{e(m)_{\mathrm{ZF}}} \\ &= \frac{\left(1-\epsilon_{(m)}\right)\rho_{(m)}|\mathbf{t}^H_{1(m)}\mathbf{H}^{\dagger}_{e(m)}\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}|^2}{\mathbf{t}^H_{1(m)}\mathbf{H}^{\dagger}_{e(m)}\left[\epsilon_{(m)}\rho_{(m)}\mathbf{H}_{e(m)}\mathbf{C}_{\eta(m)}\mathbf{H}^H_{e(m)} + \sigma^2_{e(m)}\mathbf{I}\right]\left(\mathbf{H}^{\dagger}_{e(m)}\right)^H\mathbf{t}_{1(m)}}. \end{aligned} \tag{19}$$

Although this ZF detector mitigates the AN, unlike MRC it does not maximize the SNR due to the fact that the AWGN is amplified. On the other hand, the MMSE approach strikes a balance between AN cancellation and AWGN enhancement [19–21].

2.6. Probability of secure communication

As mentioned before, for the pure passive eavesdropping scenario (i.e., thus Alice is not aware of Eve's CSI) Alice cannot determine the system's secrecy capacity. Following the methodology described in [18], we refer to the probability of achieving secrecy between Alice and Bob on the mth subcarrier as the likelihood that information on the main link can be transmitted secretly at a certain rate C. This is expressed by

$$\mathbb{P}\left[\log\left(1+\mathrm{SNR}_{(m)}\right) - \log\left(1+\mathrm{SNR}_{e(m)}\right) > C\right]. \tag{20}$$

Note that in (20), the logarithms are in base 2.

3. Simulation results

In this section we present simulation results to show the contribution to secrecy of the frequency selectivity and the performance of both ZF and MMSE as beamforming receive strategies for Eve by the analysis of system performance and achieved secrecy probability. For the simulations, quasi-static frequency selective channels with L taps, each one with variance $\sigma^2_l = 1/L$, are considered. With the aim of preserving the average SNR independent of the number of subcarriers on both the frequency and time domain systems, the AWGN power is assumed to be the same for Bob's and Eve's channels s.t. $\sigma^2_{(m)} = \sigma^2_{e(m)} = 1/N$ and the total transmitted power is normalized to $P = 1$. The length of the cyclic prefix in the OFDM signalling is set to $L-1$ samples in order to avoid intercarrier interference.

3.1. Frequency selectivity contribution to secrecy

In Fig. 2, equal power distribution between the information and AN is used to depict the effect of increasing the number of OFDM subcarriers over the

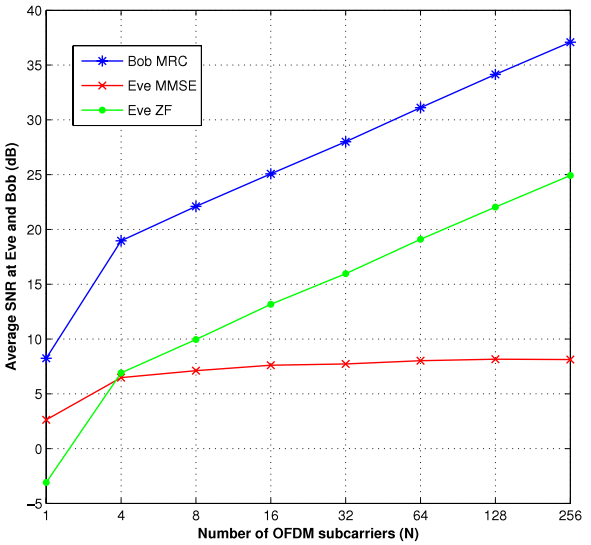

Fig. 2. System performance. Average SNR at Bob and Eve vs. number of OFDM subcarriers (N) when Eve uses MMSE and ZF, $\epsilon_{(m)} = 0.5$, $N_t = N_r = N_e = 5$ and $L = 4$.

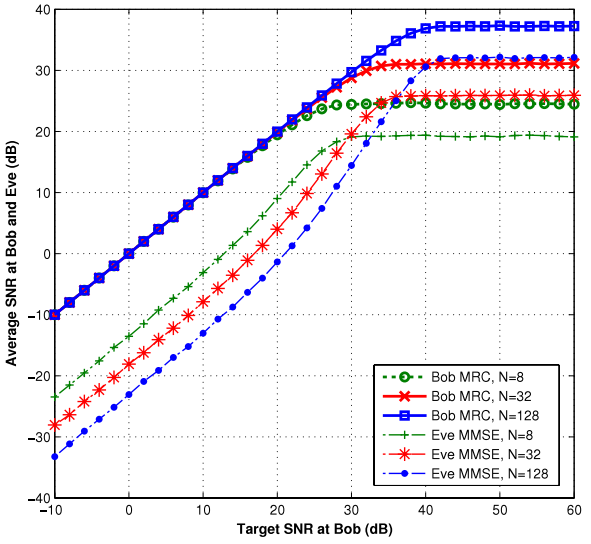

Fig. 3. System performance. Average SNR at Bob and Eve vs. target SNR for different numbers of OFDM subcarriers, $N = 8, 32, 128$, when Eve uses MMSE, $N_t = N_r = N_e = 5$ and $L = 4$.

secrecy of the system where all the nodes are equipped with the same number of antennas (i.e., $\epsilon_{(m)} = 0.5$ and $N_t = N_r = N_e$). Both receive beamforming methods, MMSE and ZF, are considered at Eve's side to obtain its SNR (i.e., respectively given by (14) and (17)). Here, the secrecy defined by the gap between Bob's and Eve's SNR increases with the number of subcarriers N when Eve is using MMSE. This gap remains constant for the ZF case due to Eve's AN cancellation capabilities explained in Section 2.5. This interesting behaviour and the fact that ZF outperforms MMSE will be analysed in detail later. For the moment we will concentrate on the case when Eve uses the MMSE approach.

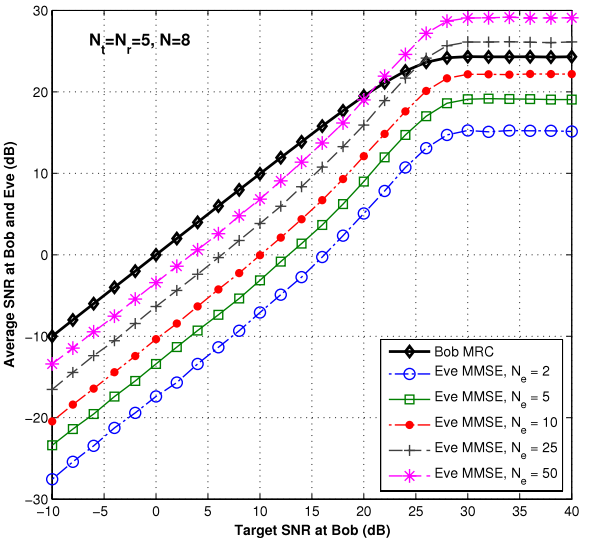

Fig. 4. System performance. Average SNR at Bob and Eve vs. target SNR for different numbers of antennas at Eve, $N_e = 2, 5, 10, 25, 50$, when Eve uses MMSE, $N_t = N_r = 5$, $N = 8$ and $L = 4$.

In Fig. 3, the impact of increasing the number of OFDM subcarriers on the system's secrecy is shown when the power is allocated between the information and AN to guarantee a target SNR (i.e., $\epsilon_{(m)}$ is calculated using (9)). Target SNR at Bob ($\overline{\text{SNR}}_{(m)}$) in (9) varies from -10 to 60 dB. All the nodes are equipped with the same number of antennas. Eve chooses MMSE as a receive beamforming strategy (i.e., as in (12)). In this approach, secrecy improvement due to the additional number of OFDM subcarriers is reflected in two factors: the increase of the gap between Bob's and Eve's SNR and the maximum target SNR that Bob can achieve with the power available. A remarkable point to consider is that as the system demands higher SNR values, the remaining power for AN transmission is lower, so the gap between Bob's and Eve's SNR decreases. In fact, there is a point on the curve where the power available at Alice is exhausted and the system cannot achieved the target minimum SNR at Bob. Once there is no power available for AN transmission the gap between Bob's and Eve's SNR still remains due to the gain introduced by beamforming.

Using the same power allocation scheme, the effect of increasing the number of antennas at Eve is analysed in Fig. 4. Here, Eve's SNR improves as the number of antennas N_e increases due to the extra spatial diversity available undermining the secrecy of the system. In the plot, it can be observed that there is a value where Eve outperforms Bob; however, the high number of antennas necessary to reach this point makes this scenario not practical.

In order to study the probability of achieving a secret communication with a data rate C, the methodology described in Section 2.6 is now considered and given a number of trials where we count the number of occurrences when secrecy between Alice and Bob is reached based on the condition given in (20). Here, the data rate C that defines if the system is secure, is progressively increased. For the ease of the analysis, we calculate the

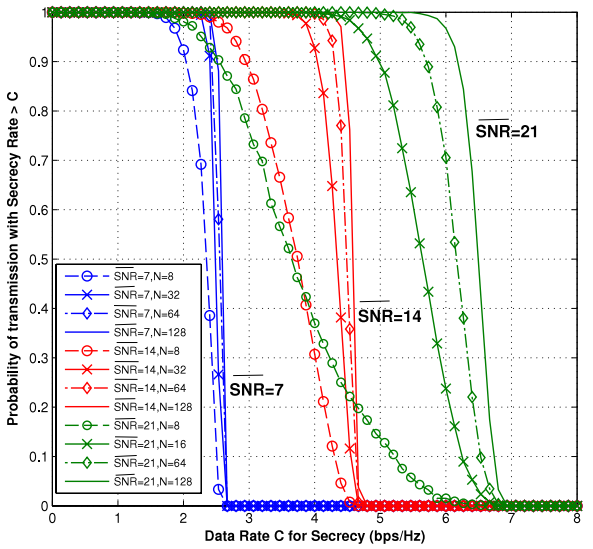

Fig. 5. Achieved probability of secure communication with data rate greater than C vs. target data rate C when Eve uses MMSE, target SNR at Bob is $\overline{\text{SNR}} = 7, 14, 21$, $N_t = N_r = N_e = 5$, $N = 8, 32, 64, 128$, and $L = 4$.

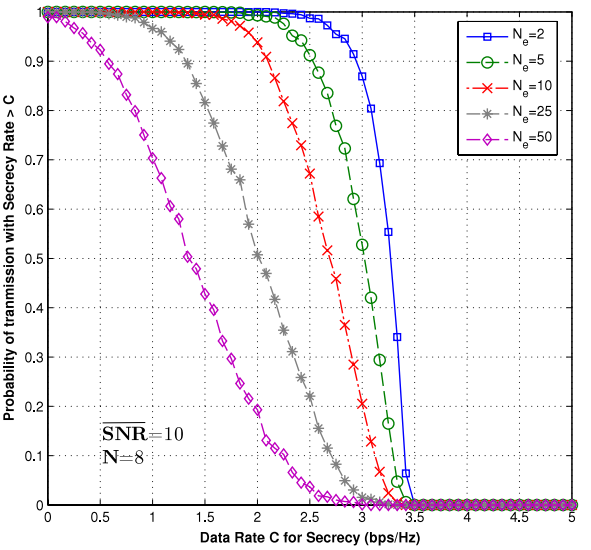

Fig. 6. Achieved probability of secure communication with data rate greater than C vs. target data rate C for different numbers of antennas at Eve $N_e = 2, 5, 10, 25, 50$ when Eve uses MMSE, target SNR at Bob $\overline{\text{SNR}} = 10$, $N_t = N_r = 5$, $N = 8$, and $L = 4$.

probability that the average data rate between Alice and Bob (over the subcarriers served by the water-filling algorithm) is larger than the target data rate C.

The improvement in secrecy due to the increase of the number of OFDM subcarriers can be clearly seen in the three cases illustrated in Fig. 5 when power is allocated to guarantee a given SNR at Bob by using (9). As expected, the maximum data rate that the system can achieve is limited by the design consideration associated to the target SNR to be satisfied at Bob. It is interesting to note that when the system becomes more demanding, (i.e., a larger target SNR at Bob is required) the probability of achieving a given secrecy rate with only a few subcarriers is lower. In Fig. 6 we investigate the relationship between the number of antennas at Eve and the probability that the system transmits securely with a data rate C. Adding antennas at the eavesdropper decreases the probability of achieving a secure communication between Alice and Bob.

3.2. Effect of artificial noise cancellation

In this subsection we analyse in detail the secrecy performance of the system when Eve is able to mitigate the effect of the AN due to the knowledge that she has about the transmit strategy used by Bob (as described in Section 2.5). In this context, we compare the performance achieved by both beamforming methods MMSE and ZF (i.e., respectively given by expressions (12) and (15)) under different AN conditions. Thus, we progressively vary the value of the fraction of the power allocated to AN ($\epsilon_{(m)}$) from zero AN power to the case when almost no power is allocated for the information (i.e., $\epsilon_{(m)} \in [0, 0.95]$). The SNR is calculated by averaging the subcarriers that have been allocated power by the water-filling algorithm (i.e., Eve's ZF and MMSE SNR are calculated using (14) and (19) respectively).

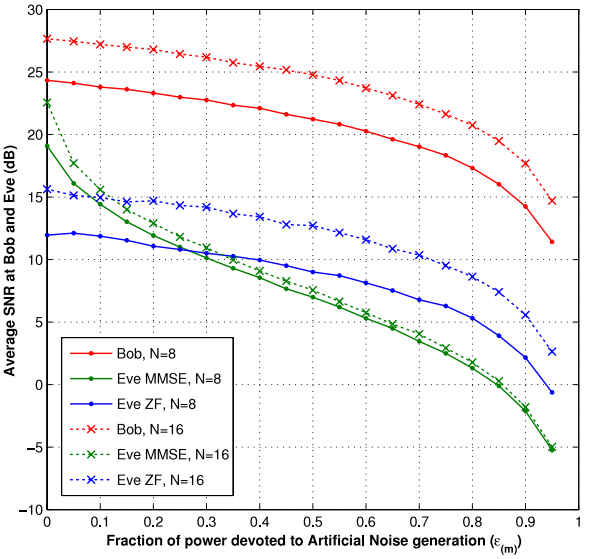

Fig. 7. System performance. Average SNR at Bob and Eve vs. fraction of power for AN generation ($\epsilon_{(m)}$) for different numbers of OFDM subcarriers ($N = 8, 16$) when Eve uses MMSE and ZF, $N_t = N_r = N_e = 5$ and $L = 4$.

In Fig. 7 the beamformers' performance is compared for frequency selective channels when all the nodes in the network are equipped with the same number of antennas. Here ZF achieves a better performance due to the effect of the AN cancellation. Indeed, for ZF the gap between Bob's and Eve's SNR remains constant for all the values of $\epsilon_{(m)}$ due to the effective AN cancellation, so it does not affect the SNR. In contrast, for MMSE the gap depends on how much power is devoted to the AN generation.

It is worth reiterating that the fact that ZF outperforms MMSE in MIMO–OFDM systems (i.e., even as explained in Section 2.4 that MMSE is the optimum strategy to

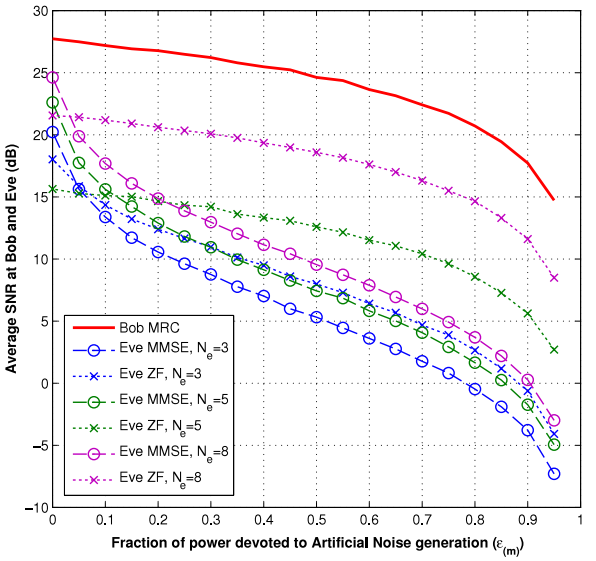

Fig. 8. System performance. Average SNR at Bob and Eve vs. fraction of power for AN generation ($\epsilon_{(m)}$) for different numbers of antennas at Eve ($N_e = 3, 5, 8$) when Eve uses MMSE and ZF, $N_t = N_r = 5$, $N = 16$, and $L = 4$.

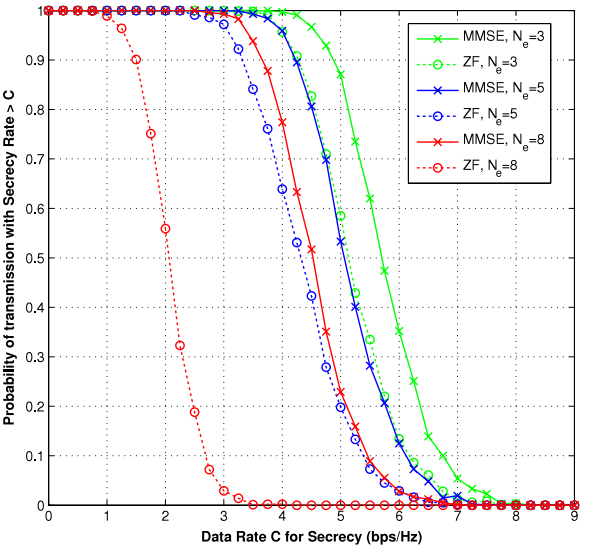

Fig. 9. Achieved probability of secure communication with data rate greater than C vs. target data rate C for different numbers of antennas at Eve ($N_e = 3, 5, 8$) when Eve uses MMSE and ZF, $N_t = N_r = 5$, $N = 16$, and $L = 4$.

maximize SNR) is based on two observations. First, ZF contributes towards a higher SNR due to the fact that the strategy (as defined in Section 2.5) effectively cancels the AN. This can be observed by comparing Eqs. (14) and (17) where the negative contribution of the AN to the SNR is nulled by ZF. Second, in (17), we should also comment that the trade-off for cancelling the AN is an AWGN enhancement, but not enough to offset the AN cancellation. The reason is based on the fact that an OFDM multicarrier system preserves the performance (given by the average SNR) by effectively distributing the power of both information and AWGN among the subcarriers. As a result, the N flat fading channel system now has low AWGN power in each subcarrier. Under this condition the AWGN enhancement penalty introduced by ZF is not relevant, so the cancellation of the AN affects positively to the achieved SNR without any backward. In addition, water-filling allocates opportunistically the power among the subcarriers leading to subcarriers with high SNR a condition that is favourable to the ZF approach.

In Fig. 8 we investigate the link between Eve's number of antennas and her AN cancellation ability. As expected, when the Alice-to-Eve channel corresponds to a square or tall matrix (i.e., $N_e \geq N_t$), Eve can effectively null the AN. However, in the case of a fat channel matrix (i.e., $N_e < N_t$), Eve (using ZF) still can partially cancel the AN; indeed, as shown in Fig. 8, Eve's SNR achieved by ZF is larger than all the cases where an MMSE strategy is used. These results are corroborated by the achieved probability of secrecy depicted in Fig. 9 where the likelihood of achieving a secret communication with secrecy rate C diminishes for all the cases when Eve uses ZF rather than MMSE.

In Fig. 10 this analysis is extended to flat fading channels. Here the results show that, as expected, the best technique to use for receive beamforming in a flat fading channel (from Eve's point of view) is MMSE rather than ZF.

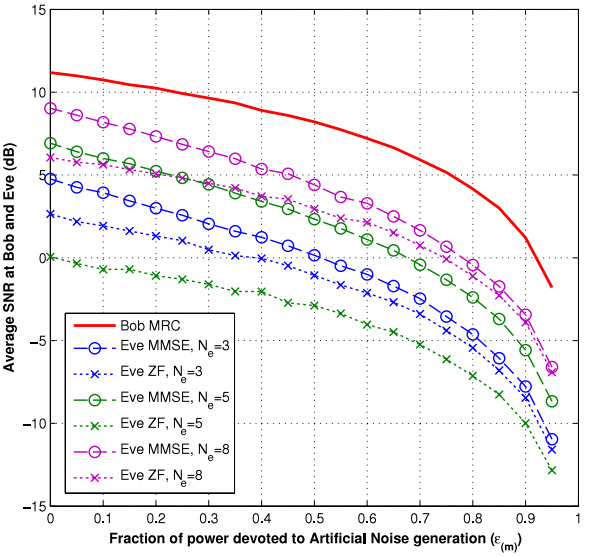

Fig. 10. System performance. Average SNR at Bob and Eve vs. fraction of power for AN generation ($\epsilon_{(m)}$) in flat fading channels for different numbers of antennas at Eve ($N_e = 3, 5, 8$) when Eve uses MMSE and ZF and $N_t = N_r = 5$.

As explained before, this improved performance is because under single carrier systems (i.e., where the information and AWGN is not distributed among subcarriers) the optimal scheme to maximize the SNR is introduced by MMSE even though ZF cancels the AN.

4. Discussion

In this section we consider briefly the eavesdropper's practical ability and requirements that it would have to fulfil to recover the information necessary to cancel the AN

broadcasted by the transmitter and then to jeopardize the security between Alice and Bob. Recapitulating Sections 2.4 and 2.5, if the eavesdropper uses MMSE as a receive beamforming strategy, the worst scenario for the secrecy of the system is when Eve is somehow aware of $\mathbf{H}_{(m)}\mathbf{t}_{1(m)}$, the AN covariance matrix $\mathbf{C}_{\eta(m)}$ and the power allocated to the AN $\epsilon_{(m)}\rho_{(m)}$. On the other hand, ZF only requires knowledge of Eve's own CSI (i.e., $\mathbf{H}_{e(m)}$) and the beamformer vector used by the transmitter $\mathbf{t}_{1(m)}$ in order to attempt to null the AN. Considering that $\mathbf{t}_{1(m)}$ is chosen as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{H}^H_{(m)}\mathbf{H}_{(m)}$, then the security of the system relies on keeping the Alice-to-Bob's CSI ($\mathbf{H}_{(m)}$) secret from Eve.

In this context, and assuming that Eve is perfectly capable of recovering her own channel, the main problem from the eavesdropper's perspective is how to recover the main channel's time domain signature $\mathbf{H}$ in order to establish the frequency domain beamformer vector $\mathbf{t}_{1(m)}$. Let us consider two scenarios where Alice acquires $\mathbf{H}$. The first one, used in FDD systems, relies on the quantized feedback sent back by Bob to Alice after he has estimated the channel. The second one exploits channel reciprocity between uplink and downlink in TDD systems so Alice and Bob estimate the channel separately by themselves. In the first case, Eve, in order to recover $\mathbf{H}$, might eavesdrop the Bob-to-Alice feedback channel to hear the channel estimated information when Bob sends the CSI back to Alice. In the second scenario, when channel reciprocity is used, the task is more complicated for Eve and will require extra complexity at her side to incorporate blind channel estimation techniques. This approach will not lead to a complete accurate CSI and so the security of the system offered by the AN generation will be still partially preserved.

5. Conclusion

In this work we investigate the contribution of frequency selectivity to the secrecy of the communication, defined as the SNR difference between the receiver and the eavesdropper, when beamforming and broadcasting artificial noise are chosen as the transmit strategy over MIMO–OFDM channels. Based on the results previously presented, frequency selectivity contributes positively to the secrecy of the system through frequency diversity and opportunistic power distribution. However, the eavesdropper's characteristics such as the number of available antennas, the knowledge that it has regarding the transmit strategy and the chosen multiple antennas methodology, all play a critical role in determining the security of the system. Indeed, if the eavesdropper has a large number of antennas, knows the main channel CSI, and uses zero forcing to mitigate the interference introduced by the artificial noise transmission, then the secrecy of the system can be put at risk.

References

[1] A. Wyner, Wire-tap channel, Bell System Technical Journal 54 (1975) 1355–1387.

[2] I. Csiszar, J. Korner, Broadcast channels with confidential messages, IEEE Transactions on Information Theory 24 (1978) 339–348.

[3] S. Leung Yan Cheong, M.E. Hellman, The Gaussian wire-tap channel, IEEE Transactions on Information Theory 24 (1978) 451–456.

[4] J. Barros, M. Rodrigues, Secrecy capacity of wireless channels, in: 2006 IEEE International Symposium on Information Theory, pp. 356–360.

[5] M. Bloch, J. Barros, M. Rodrigues, S. McLaughlin, Wireless information-theoretic security, IEEE Transactions on Information Theory 54 (2008) 2515–2534.

[6] A. Swindlehurst, Fixed SINR solutions for the MIMO wiretap channel, in: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2009, 2009, pp. 2437–2440.

[7] W.C. Liao, T.H. Chang, W.K. Ma, C.Y. Chi, QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach, IEEE Transactions on Signal Processing 59 (2011) 1202–1216.

[8] A. Khisti, G. Wornell, A. Wiesel, Y. Eldar, On the Gaussian MIMO wiretap channel, in: IEEE International Symposium on Information Theory, ISIT 2007, 2007, pp. 2471–2475.

[9] A. Khisti, G. Wornell, Secure transmission with multiple antennas II: the MIMOME wiretap channel, IEEE Transactions on Information Theory 56 (2010) 5515–5532.

[10] N. Chiurtu, B. Rimoldi, E. Telatar, On the capacity of multi-antenna Gaussian channels, in: 2001 Proceedings IEEE International Symposium on Information Theory, 2001, p. 53.

[11] S. Shafiee, S. Ulukus, Achievable rates in Gaussian MISO channels with secrecy constraints, in: IEEE International Symposium on Information Theory, ISIT 2007, pp. 2466–2470.

[12] S. Shafiee, N. Liu, S. Ulukus, Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2–2–1 channel, IEEE Transactions on Information Theory 55 (2009) 4033–4039.

[13] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Transactions on Wireless Communications 7 (2008) 2180–2189.

[14] R. Negi, S. Goel, Secret communication using artificial noise, in: 2005 IEEE 62nd Vehicular Technology Conference, VTC-2005-Fall, vol. 3, 2005, pp. 1906–1910.

[15] X. Zhou, M. McKay, Physical layer security with artificial noise: secrecy capacity and optimal power allocation, in: 3rd International Conference on Signal Processing and Communication Systems, ICSPCS 2009, 2009, pp. 1–5.

[16] X. Zhou, M. McKay, Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation, IEEE Transactions on Vehicular Technology 59 (2010) 3831–3842.

[17] A. Mukherjee, A. Swindlehurst, Robust beamforming for security in MIMO wiretap channels with imperfect CSI, IEEE Transactions on Signal Processing 59 (2011) 351–361.

[18] M. Ghogho, A. Swami, Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers, in: IEEE ICC Workshop on Physical Layer Security, 2011.

[19] C. Oestges, B. Clerckx, MIMO Wireless Communications: From Real-World Propagation to Space–Time Code Design, Academic Press, 2007.

[20] D. Tse, P. Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005.

[21] J. Andrews, A. Ghosh, R. Muhamed, Fundamentals of WiMAX Understanding Broadband Wireless Networking, Prentice Hall, 2007.

Nabil Romero-Zurita received the B.Sc. degree in electronic engineering from ESPE, Quito-Ecuador, and the M.Sc. in Modern Digital and Wireless Frequency Communications from the University of Leeds, UK where he is currently working towards the Ph.D. degree. He has industrial experience as radio frequency engineer planning and optimizing 2G and 3G cellular networks. His research areas of interest are security on physical layer, MIMO systems, cooperative communications, capacity, planning and optimization of cellular networks. Mr. Romero-Zurita has been awarded with the Excellence Scholarship in 2008, and with the four-year Fully Founded International Research Scholarship in 2010, both by the University of Leeds.

Mounir Ghogho received the M.S. degree in 1993 and the Ph.D. degree in 1997 from the National Polytechnic Institute of Toulouse, France. He was an EPSRC Research Fellow with the University of Strathclyde, Glasgow, from September 1997 to November 2001. Since December 2001, he has been a faculty member with the school of Electronic and Electrical Engineering at the University of Leeds, where he is currently a Professor. He is also currently a Professor at the International University of Rabat in Morocco. He served as an Associate Editor of the IEEE Signal Processing Letters from 2001 to 2004 and the IEEE Transactions on Signal Processing from 2005 to 2008. He also served as a member of the IEEE Signal Processing Society SPCOM Technical Committee from 2005 to 2010 and is currently a member of the IEEE Signal Processing Society SPTM Technical Committee. He was the general co-chair of the eleventh IEEE workshop on Signal Processing for Advanced Wireless Communications (SPAWC'2010), the technical co-chair of the MIMO symposium of IWCMC 2007 and IWCMC 2008, and a technical area co-chair of Eusipco 2008, Eusipco 2009 and ISCCSP'05. He is the general chair of Eusipco 2013. He was the guest co-editor of the EURASIP Journal on Wireless Communications and Networking special issue on "synchronization for wireless communications".

His research interests are in communication and sensor networks, radar imaging and signal processing. Prof. Ghogho was awarded a five-year Royal Academy of Engineering Research Fellowship in September 2000.

Des McLernon received his B.Sc. in electronic and electrical engineering and his M.Sc. in electronics, both from the Queen's University of Belfast, Northern Ireland. He then worked on radar systems with Ferranti Ltd. in Edinburgh, Scotland and later joined Imperial College, University of London, where he took his Ph.D. in signal processing. After first lecturing at South Bank University, London, UK, he moved to the School of Electronic and Electrical Engineering, at the University of Leeds, UK, where he is a Reader in Signal Processing and is the Director of Graduate Studies. His research interests are broadly within the domain of signal processing (in which area he has published 213 journals and conference papers).