PHYSICAL LAYER SECURITY OF MIMO FREQUENCY SELECTIVE CHANNELS BY BEAMFORMING AND NOISE GENERATION

Nabil Romero-Zurita[1], *Mounir Ghogho*[1,2] *and Des McLernon*[1]

[1] School of Electronic and Electrical Engineering, University of Leeds, LS2 9JT, Leeds, UK
[2] International University of Rabat, Morocco
email: {el08lnrz, m.ghogho, d.c.mclernon}@leeds.ac.uk

ABSTRACT

This paper addresses physical layer security in MIMO communications over frequency selective wireless channels in the presence of passive eavesdroppers, i.e. the associated channels are unknown to the legitimate transmitter. Signalling is based on orthogonal frequency division multiplexing (OFDM). Spatial beamforming is performed to improve the quality of the legitimate link. With the aim of confusing the eavesdroppers, a fraction of the available power is allocated to transmit artificial noise. Frequency diversity is shown to significantly improve secrecy. A probabilistic analysis of secrecy is presented.

1. INTRODUCTION

The broadcast nature of wireless networks introduces many types of security vulnerabilities; one of them is eavesdropping, that occurs when a non-authorized party hears a secret conversation between two nodes in the network. The way to deal with eavesdroppers in wireless communications is currently based on computationally demanding cryptographic algorithms implemented in upper layers of the communication model. As an alternative to these complex cryptographic techniques, recently, physical layer security has received increasing interest due to the possibility of exploiting the spatio-temporal variations of the wireless channel. The first works carried out in this field established the principles of information-theoretic security [1], and proved that a secret conversation between two parties can be held when the transmission rate is below the Secrecy Capacity [2]. This secrecy capacity is given by the difference between the capacity of the legitimate link and the link between the transmitter and the eavesdropper. Thus, in AWGN channels, secrecy capacity is a function of the SNRs of the links, and it can be greater than zero when the quality of the main channel is better than that of the eavesdropper [3]. Secrecy capacity of fading channels is studied in [4] and [5] where it is stated that due to fading, it is still possible to achieve secrecy even if the average SNR of the eavesdropper channel is better than that of the legitimate channel. Secrecy for multiple antennas systems was studied in [6]. In [7] and [8], beamforming was shown to be the optimal strategy for secrecy in MISO systems. The inclusion of artificial noise as a way to confuse eavesdroppers was introduced in [9]. In most of the above mentioned works, the location of the eavesdropper is considered to be known. However, this is not a practical assumption in the case of purely passive eavesdropping. As an alternative to this scenario, in [10], an approach that uses beamforming and artificial noise generation is introduced to increment secrecy when the eavesdroppers' locations and channels are random and unknown. Stochastic geometry was used to probabilistically characterize secrecy. Also in [10], the idea that frequency selectivity can improve secrecy was mentioned. In this paper, we investigate this idea further and present a quantitative analysis of the secrecy improvement resulting from frequency selectivity. Unlike [10] where no power allocation scheme was specified, here we first use water-filling to distribute power across the subcarriers and then, for each carrier, transmit information using the minimum required power to achieve a specified signal-to-noise ratio and allocate the rest of the power to the artificial noise. The effects of increasing the number of antennas and subcarriers on secrecy are studied via simulations.

2. NETWORK AND SIGNAL MODELS

In this section, we present the eavesdropping problem over frequency selective channels. Following the well known cryptographic model, the nodes in the system are named Alice, Bob and Eve for the transmitter, intended receiver, and eavesdropper respectively. First, the system model is described and then beamforming and noise generation techniques are explained. Then, power distribution over the subcarriers and between information and artificial noise are described. Finally, a probabilistic analysis is introduced to assess the contribution of frequency selectivity to secrecy.

2.1 System Model

We consider OFDM signalling. Alice, Bob and Eve are equipped with N_t, N_r and N_e antennas, respectively. The MIMO frequency selective channels between Alice and Bob and between Alice and Eve, $\mathbf{H}$ and $\mathbf{H}_e$, consist of L multipath taps modelled as independent, zero-mean complex $(N_r \times N_t)$ and $(N_e \times N_t)$ matrices respectively with variance σ_l^2, for $l = 0, \cdots, L-1$. We assume that $\mathbf{H}$ is perfectly known to Alice. However, Alice has no knowledge of the Eve's channel, $\mathbf{H}_e$. The general system is depicted in figure 1.

Let $\mathbf{s}_{(m)}$ denote the signal transmitted over the mth subcarrier, $m \in [0, 1, \cdots, N-1]$. It is well known that one of the important properties of OFDM is to transform a frequency selective multipath channel with L taps to an equivalent system of N parallel frequency flat fading channels. The signals received by Bob and Eve on the mth subcarrier, $\mathbf{u}_{(m)}$ and $\mathbf{v}_{(m)}$, are respectively given by:

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

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

where $\mathbf{H}_{(m)}$ and $\mathbf{H}_{e(m)}$ are the frequency-domain channel matrices corresponding to the mth subcarrier, $\mathbf{n}_{(m)}$ and $\mathbf{n}_{e(m)}$

© EURASIP, 2011 - ISSN 2076-1465

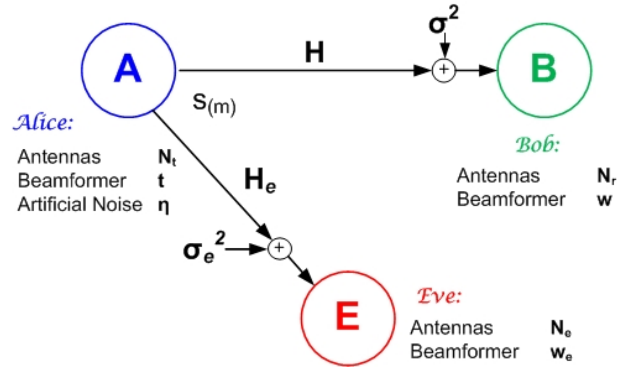

Figure 1: System Model. Wireless transmission between transmitter and intended receiver in the presence of an eavesdropper over MIMO Frequency Selective Channels.

are mutually independent, zero-mean, complex, Gaussian noise vectors with covariance matrices $\sigma^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$ with $\mathbf{I}$ denoting the identity matrix with the appropriate dimensions. Let $\mathbf{C}_{s(m)} = \mathbb{E}\{\mathbf{s}_{(m)}\mathbf{s}_{(m)}^H\}$ denote the covariance matrix of $\mathbf{s}_{(m)}$. The power allocated to the mth subcarrier is $\rho_{(m)}$ =Tr$\{\mathbf{C}_{s(m)}\}$. We assume a total power constraint i.e. $\sum_{m=0}^{N-1}\rho_{(m)} = P$. Further, a fraction $\varepsilon_{(m)} \in [0,1)$ of the power allocated to each subcarrier is used to transmit an artificial noise. The transmitted signal $\mathbf{s}_{(m)}$ is modelled as follows:

$$\mathbf{s}_{(m)} = \sqrt{\rho_{(m)}}\left(\sqrt{1-\varepsilon_{(m)}}\mathbf{t}_{(m)}d_{(m)} + \sqrt{\varepsilon_{(m)}}\eta_{(m)}\right) \qquad (3)$$

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

2.2 Beamforming, Noise Generation and Power Allocation

Beamforming is the optimum transmit strategy for maximizing the secrecy capacity in multiple antennas systems [7], so the aim of beamforming and transmitting artificial noise is to increase the secrecy of the system by incrementing the SNR difference between Bob and Eve. Hence, the strategy to follow, as mentioned in [10], is to maximise the SNR at Bob and transmit noise in all the directions except towards Bob. Thus, Alice chooses the beamforming vector $\mathbf{t}_{(m)}$ as the principal eigenvector $\mathbf{t}_{1(m)}$ corresponding to the largest eigenvalue of $\mathbf{H}_{(m)}^H\mathbf{H}_{(m)}$. The artificial noise $\eta_{(m)}$ must be orthogonal to the beamforming vector to guarantee that it does not affect Bob's reception, i.e., $\mathbf{t}_{1(m)}^H\eta_{(m)} = 0$. With this objective, the artificial noise vector is obtained by the linear combination of the remaining $N_t - 1$ eigenvectors not including $\mathbf{t}_{1(m)}$. The power is distributed uniformly among these eigenvectors. Hence, the artificial noise covariance is defined by:

$$\mathbf{C}_{\eta(m)} = \frac{\varepsilon_{(m)}\rho_{(m)}}{N_t - 1}\sum_{i,j=2}^{N_t-1}\mathbf{t}_{i(m)}\mathbf{t}_{j(m)}^H \qquad (4)$$

where $\mathbf{t}_{i(m)}$ is the ith eigenvector of $\mathbf{H}_{(m)}^H\mathbf{H}_{(m)}$.

For the power allocation, the total power is distributed among the N subcarriers using the water filling technique as explained in [11]. The aim of using water filling is to maximise the capacity between Alice and Bob [12] and, as a result, to improve the system's secrecy. In other words, water filling allow us to allocate power in an opportunistic fashion to the best subcarriers to increment the secrecy of the system. The power distribution using water filling is obtained as:

$$\rho_{(m)} = \max\left(0, \frac{1}{\hat{N}}\left(\hat{P} + \sum_{i=1}^{N}\frac{1}{\gamma_{(i)}}\right) - \frac{1}{\gamma_{(i)}}\right) \qquad (5)$$

$$\sum_{m=1}^{N}\rho_{(m)} = \hat{P} = \frac{PN}{N+\mu}. \qquad (6)$$

In (5), $\hat{N}$ is the number of subcarriers which have $\rho_{(m)} \neq 0$ after the initial power allocation. $\hat{P}$ is calculated in (6), and it is the available power once the transmission of the cyclic prefix of length μ is considered. Finally, $\gamma_{(i)}$ is the channel's power to noise ratio given by:

$$\gamma_{(i)} = \frac{||\mathbf{H}_{(i)}||_F^2}{N_tN_r\sigma^2}; i = 0, \cdots, N-1. \qquad (7)$$

Once the powers $\{\rho_{(m)}\}$, have been determined, $(1-\varepsilon_{(m)})\rho_{(m)}$ is used to transmit the information signal and $\varepsilon_{(m)}\rho_{(m)}$ is allocated to broadcast artificial noise. The parameter $\varepsilon_{(m)}$ is defined such that the target SNR at Bob required to reliably decode the transmitted information on the mth subcarrier, $\overline{\text{SNR}}$, is achieved. This value could be related to a minimum quality of service requirement of the system; indeed, we consider the security condition that system is in outage for transmissions below this value. Once that the required SNR is guaranteeed at Bob and with the aim of increasing the secrecy of the system, defined as the SNR difference between Bob an Eve, noise is broadcasted exploiting the additional power that could be available at the transmitter. Extending this consideration to the multicarrier scenario, we assume that the minimum target SNR is the same for all subcarriers. Extensions to the case of different minimum target SNRs are straightforward. Hence, for the mth subcarrier, $\varepsilon_{(m)}$ is obtained as

$$\varepsilon_{(m)} = 1 - \frac{\overline{\text{SNR}}\sigma^2}{\rho_{(m)}\nu_{1(m)}} \qquad (8)$$

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

Beamforming vectors at Bob and Eve are determined by considering that both aim to maximise the received SNR. At Bob, the corresponding beamforming vector is set to $\mathbf{w}_{(m)}$ =$\mathbf{H}_{(m)}\mathbf{t}_{1(m)}$. To calculate the beamforming vector at Eve, we assume the unlikely worst scenario where Eve knows $\varepsilon_{(m)}$, $\mathbf{t}_{1(m)}$, and $\mathbf{C}_{\eta(m)}$. Therefore, Eve sets the beamforming vector as:

$$\mathbf{w}_{e(m)} = \left(\mathbf{H}_{e(m)}\mathbf{C}_{\eta(m)}\mathbf{H}_{e(m)}^H + \sigma_{e(m)}^2\mathbf{I}\right)^{-1}\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}. \qquad (9)$$

Finally, Bob's and Eve's SNR at the mth subcarrier are given by:

$$\text{SNR}_{(m)} = \left(1-\varepsilon_{(m)}\right)\rho_{(m)}\mathbf{t}_{1(m)}^H\mathbf{H}_{(m)}^H\left[\sigma_{(m)}^2\mathbf{I}\right]^{-1}\mathbf{H}_{(m)}\mathbf{t}_{1(m)} \qquad (10)$$

$$\mathrm{SNR}_{e(m)} =$$

$$\left(1-\varepsilon_{(m)}\right)\rho_{(m)}\mathbf{t}_{1(m)}^{H}\mathbf{H}_{e(m)}^{H}\left[\mathbf{H}_{e(m)}\mathbf{C}_{\eta(m)}\mathbf{H}_{e(m)}^{H}+\sigma_{e(m)}^{2}\mathbf{I}\right]^{-1}..$$
$$..\mathbf{H}_{e(m)}\mathbf{t}_{1(m)}. \quad (11)$$

It is worth pointing out that in the above scheme more artificial noise is transmitted over the best subcarriers and therefore transmissions over these subcarriers are more likely to be secure than the other subcarriers.

2.3 Probability of Secure Communication

Since the CSI of the eavesdropper is unknown, Alice cannot determine the exact value of the secrecy capacity. In this scenario, we refer to the probability of achieving a secure communication between Alice and Bob on the mth subcarrier as the probability that the quality of mth channel between Alice and Bob is better than that between Alice and Eve. This is expressed by:

$$\mathbb{P}\left[\mathrm{SNR}_{(m)} > \mathrm{SNR}_{e(m)}\right], m \in [0,1,\cdots,N-1]. \quad (12)$$

Another approach is to consider the probability of secrecy of the system as the likelihood that information on the main link can be transmitted secretly at a certain rate C. Allocating some power to transmit an artificial noise improves the probability of secrecy at the expense of reducing the capacity of the legitimate link. As explained in [9], there are two reasons for the loss in the secret capacity in a system broadcasting artificial noise. First, only a part of the available power is used to transmit the information signal; second, the eavesdropper gains a certain amount of the transmitted information. Another way to understand this penalty in the capacity of the system is that only a fraction of the available power is allocated to information transmission to guarantee a level of SNR at Bob, so the total capacity of the main link is limited for this design consideration. Bearing this in mind, the probability that the system reaches a secrecy data rate C on the mth subcarrier is given by:

$$\mathbb{P}\left[\log\left(1+\mathrm{SNR}_{(m)}\right) - \log\left(1+\mathrm{SNR}_{e(m)}\right) > C\right],$$
$$m \in [0,1,\cdots,N-1] \quad (13)$$

where in (13), the logarithms are in base 2.

3. SIMULATION RESULTS

In this section we present some results that show secrecy performance of the system using the difference of Bob's and Eve's SNRs. For the simulations, quasi-static frequency selective channels with L taps, each with variance $\sigma_l^2 = 1/L$, are considered. The noise power is assumed to be the same for Bob and Eve, i.e. $\sigma^2 = \sigma_e^2 = 1$. 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. With the aim of understanding the performance of the system for different levels of requirements, the value of the target SNR at Bob is varied. Considering the case of a power constrained system, noise is transmitted when there is enough power to achieve the required minimum target SNR at Bob. In the case where it is still not possible to achieve the required SNR even with the total available power, then the system is said to be in outage. The SNRs are evaluated and averaged over the total number of subcarriers.

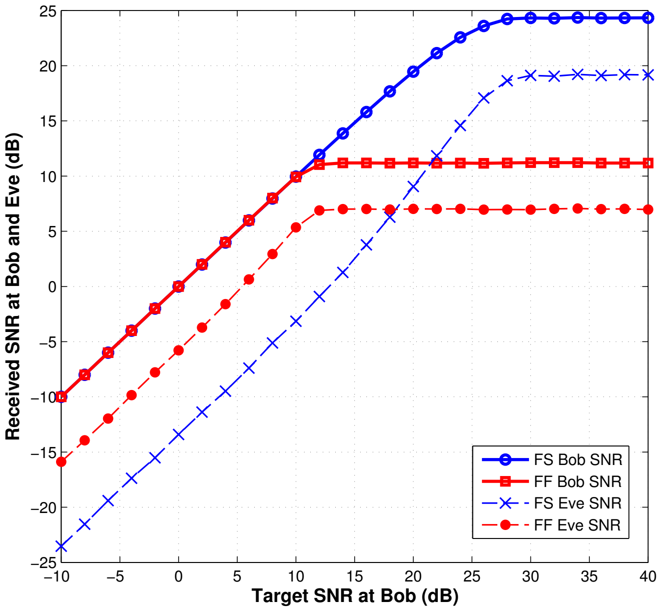

Figure 2: Secrecy on Frequency Selective Channels. System Performance. Comparison between FSC and FFC. Received SNR at Bob and Eve vs. Target SNR for $N = 8$.

3.1 System Performance

Figure 2 displays the system performance when $N = 8$, $N_t = N_r = N_e = 5$ and $L = 4$. For comparison, the result for a flat fading channel, i.e. $L = 1$, is depicted as well. It can be observed that the SNR difference between Bob and Eve in the frequency selective scenario is larger than that in the flat fading case. In most of the cases, Bob fulfils the designated target value of SNR while Eve has a lower SNR. If we consider that it is necessary to have that minimum target SNR at the receiver to decode the information, it can be inferred that Eve is not able to retrieve the information. A remarkable point to consider is that as the system demands higher SNR values, the remaining power for noise 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 SNR at Bob cannot achieved the target minimum SNR. It is clear that from the moment that this point is reached, there is no power available for noise transmission; nevertheless, a gap between Bob's SNR and Eve's still remains due to the gain introduced by beamforming.

In figure 3, the impact of increasing the number of OFDM subcarriers on system secrecy is shown. For this scenario, we consider the same number of antennas as above, i.e. $N_t = N_r = N_e = 5$. Secrecy improvement due to increasing the number of OFDM subcarriers is reflected in two factors: the maximum target SNR that Bob can achieve, and the increase of the gap between Bob's and Eve's performance. This behaviour is due to the increased diversity obtained by higher number of subcarriers and the opportunistic power allocation over the channel's fading realizations.

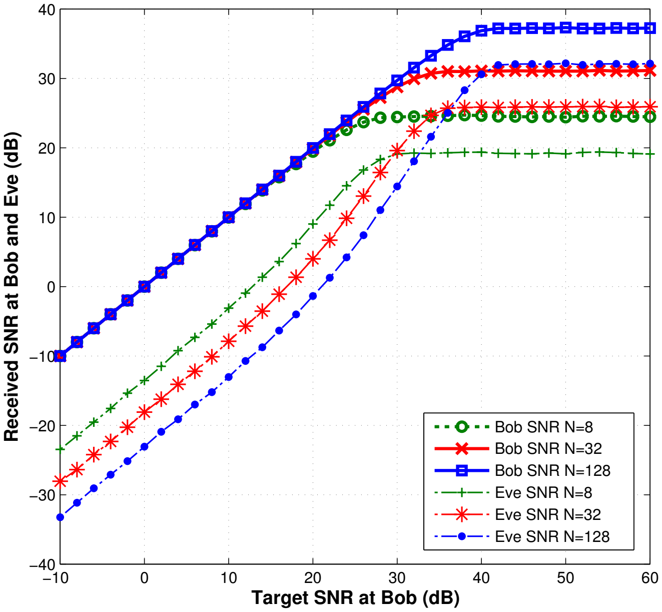

Figure 3: Secrecy on Frequency Selective Channels. System Performance. Received SNR at Bob and Eve vs. Target SNR for different values of the number of OFDM subcarriers $N = 8, 32, 128$ when $N_t = N_r = N_e = 5$.

The effect of adding antennas at Eve is analyzed in figure 4 where it is shown that this undermines the secrecy of the system. As a result of the increase in the number of antennas at Eve, its SNR improves due to the extra spatial diversity available. In the plot, it can be observed that there is a value where Eve outperforms Bob; nevertheless, considering the high number of antennas necessary to reach this point, this scenario might not be considered practical.

3.2 Probability of Secrecy

In order to study the probability of achieving a secret communication with a specific data rate C, the approach described in subsection 2.3 is considered. Using the same simulation setup as above, we have run 10.000 trials to count the number of occurrences when secrecy transmission between Alice and Bob is reached based on the condition given by (13). Here, the data rate C, that defines if the system is secure, is progressively increased. For the ease of the analysis, we calculate the probability that the averaged data rate between Alice and Bob over the subcarriers served by the water filling algorithm is larger that a target data rate C.

Three scenarios defined by the target SNR at Bob, $\overline{\text{SNR}} = 7, 14, 21$ dB are considered in figure 5. For each case, the probability of achieving secrecy with a given data rate C is analyzed when $N = 8, 32, 64, 128$ subcarriers. The improvement in secrecy due to the increase of the number of subcarriers can be seen clearly in all of the illustrated cases. As expected, and according to the design considerations required for the secrecy of the system, the maximum data rate that the system can achieve is limited by the maximum capacity corresponding to the target SNR specified for Bob. It is interesting to see that when the system becomes more demanding, which means that it requires a larger target SNR at Bob, the

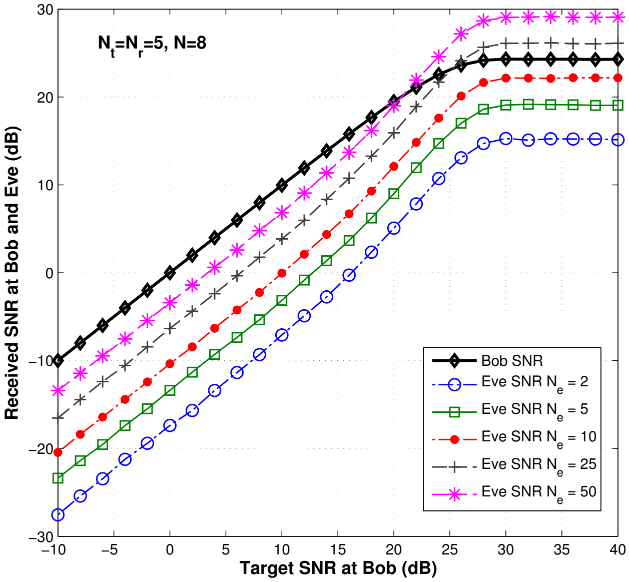

Figure 4: Secrecy on Frequency Selective Channels. System Performance. Received SNR at Bob and Eve vs. Target SNR for different values of the number of antennas at Eve $N_e = 2, 5, 10, 25, 50$ when $N_t = N_r = 5$ and $N = 8$.

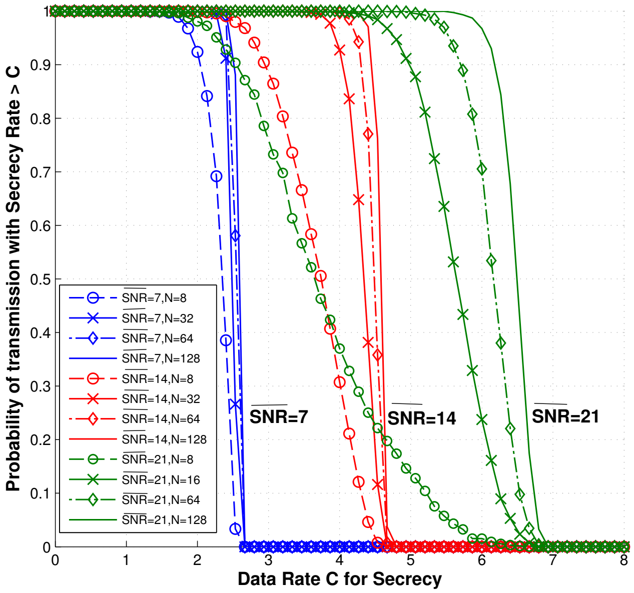

Figure 5: Secrecy on Frequency Selective Channels. Probability of Secure Communication with Data Rate greater than C vs. Target Data Rate C. The SNR at Bob is $\overline{\text{SNR}} = 7, 14, 21$ and $N = 8, 32, 64, 128$

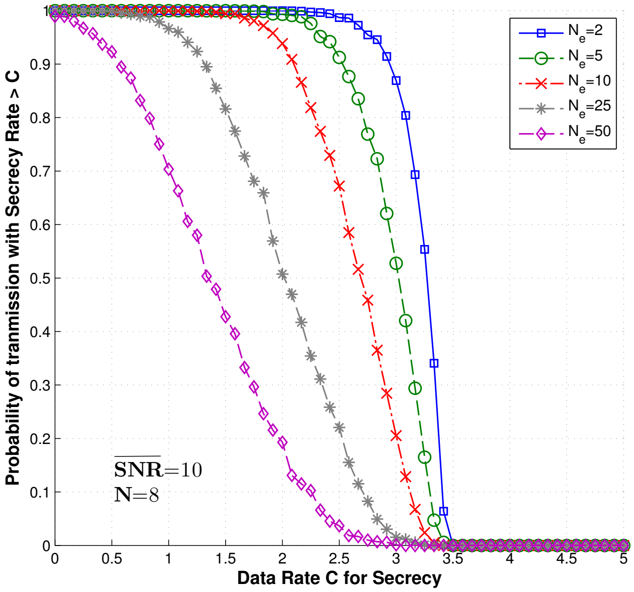

Figure 6: Secrecy on Frequency Selective Channels. Effect of Increasing antennas at Eavesdropper. Probability of Secure Communication with Data Rate greater than C vs. Target Data Rate C. SNR at Bob $\overline{\text{SNR}} = 10$, $N = 8$ and antennas at Eve are $N_e = 2, 5, 10, 25, 50$

probability of achieving a given secrecy rate in the system with few subcarriers is lower.

In figure 6, the probability that the system transmits securely with a data rate C is shown when $\overline{\text{SNR}} = 10$ and $N = 10$. The number of antennas at Eve are $N_e = 2, 5, 10, 25, 50$. From the figure, it can be inferred that adding antennas at the eavesdropper decreases the probability of achieving a secure communication between Alice and Bob transmitting at data rate C for the worst scenario when at Eve is available all the information about the transmission strategy as explained in section 2.2.

4. CONCLUSIONS

In this work, secure communication between a transmitter and a receiver in the presence of a passive eavesdropper over MIMO frequency selective channels is considered. The objective to improve the secrecy of the communication, defined as SNR difference between the receiver and the eavesdropper, is achieved by using beamforming and transmitting artificial noise to confuse the eavesdropper. Water filling is used to distribute power between subcarriers. Then, for each subcarrier, a fraction of the power is allocated to transmit an artificial noise. This fraction is determined such that the SNR at the legitimate receiver achieves a specified target SNR. Based on the results exposed, it has been demonstrated that frequency selectivity contributes positively to the secrecy of the system through frequency diversity and opportunistic power distribution. On the other hand, augmenting the number of antennas at the eavesdropper undermines secrecy.

REFERENCES

[1] A. D. Wyner, “The Wire-Tap Channel”, *Bell System Technical Journal*, vol. 54, pp. 1355-1387, 1975.

[2] I. Csiszar, I. and J. Korner, “Broadcast channels with confidential messages”. *Information Theory, IEEE Transactions on*, vol. 24(3), pp. 339-348, 1978.

[3] S. Leung-Yan-Cheong and M. Hellman, “ The Gaussian wire-tap channel.”, *Information Theory, IEEE Transactions on*, vol 24(4), pp. 451-456, 1978.

[4] J. Barros and M. R. D. Rodrigues, “Secrecy Capacity of Wireless Channels,” in *Information Theory, 2006 IEEE International Symposium on*, July 9-14. 2006, pp. 356-360.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLauglin, “Wireless Information-Theoretic Security”. *Information Theory, IEEE Transactions on*, vol 54(6), pp. 2515-2534, 2008.

[6] A. Khisti, G. Wornell, A. Wiesel, Y. Eldar, “On the Gaussian MIMO Wiretap Channel, ” in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, 2007, pp. 2471-2475

[7] S. Shafiee and S. Ulukus. “Achievable Rates in Gaussian MISO Channels with Secrecy Constraints, ” in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, June 24-29, 2007, pp. 2466-2470

[8] A. Khisti, G. W. Wornell, “Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel”, *Information Theory, IEEE Transactions on*, vol. 56(7), pp. 3088-3104.

[9] S. Goel and R. Negi, “Guaranteeing Secrecy using Artificial Noise.”, *Wireless Communications, IEEE Transactions on*, vol. 7(6), pp. 2180-2189, 2008.

[10] M. Ghogho and 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*, Kyoto, Japan, June 5, 2011.

[11] C. Oestges, *MIMO wireless communications: from real-world propagation to space-time code design*. Oxford: Academic, 2007.

[12] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.