International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:4, 2015

Security over OFDM Fading Channels with Friendly Jammer

Munnujahan Ara

Abstract—In this paper, we investigate the effect of friendly jamming power allocation strategies on the achievable average secrecy rate over a bank of parallel fading wiretap channels. We investigate the achievable average secrecy rate in parallel fading wiretap channels subject to Rayleigh and Rician fading. The achievable average secrecy rate, due to the presence of a line-of-sight component in the jammer channel is also evaluated. Moreover, we study the detrimental effect of correlation across the parallel sub-channels, and evaluate the corresponding decrease in the achievable average secrecy rate for the various fading configurations. We also investigate the tradeoff between the transmission power and the jamming power for a fixed total power budget. Our results, which are applicable to current orthogonal frequency division multiplexing (OFDM) communications systems, shed further light on the achievable average secrecy rates over a bank of parallel fading channels in the presence of friendly jammers.

Keywords—Fading parallel channels, Wire-tap channel, OFDM, Secrecy capacity, Power allocation.

I. Introduction

SECURITY and privacy remain issues of paramount importance in wireless communications systems. In contrast to their wire-line counterparts, wireless networks are inherently more susceptible to eavesdropping attacks, due to their broadcast nature, so appropriate countermeasures need to be devised in order to address these issues. It turns out that the emergence of physical-layer based wireless security [1], [2] provides mechanisms to guarantee both reliable communication between two legitimate parties as well as secure communication in the presence of eavesdroppers.

Physical layer security aims to guarantee information-theoretic security, which is widely accepted as the strictest notion of security [3]. The roots of physical-layer security trace back to seminal works by Wyner [4] and Csiszár and Körner [5]. In particular, Wyner [4] characterized the achievable rate-equivocation region for the wiretap channel, in which two legitimate nodes attempt to transmit a secret message in the presence of an eavesdropper. Wyner [4] also characterized the secrecy capacity as the maximum achievable transmission rate that guarantees reliable decoding at the legitimate receiver and perfect equivocation at the eavesdropper. Csiszár and Körner [5] have extended the analysis to the case of a non-degraded broadcast channel. The secrecy capacity has since been computed for various communications scenarios (e.g., see [1], [2], [6], [7], [8], [9]).

Munnujahan Ara is with the Mathematics Department, Khulna University, Khulna-9208, Bangladesh, e-mail: munnujahan@gmail.com.

In general, secrecy rates can be enhanced by increasing the quality, e.g., the signal-to-noise ratio, of the channel between the legitimate parties, or by decreasing the quality of the eavesdropper channel. This can be effectively done by deploying friendly jammers that add interference in a controlled way to the communication channels. The effect of jammers on the level of security of wireless channels and networks has been studied in a myriad of works (e.g., [10], [11], [12], [13], [14]). For example, in [10], the authors investigate the design of optimal jamming configurations and the relationship between jamming coverage, jamming efficiency and the probability of secrecy outage, in order to characterize the security level of a network in which a transmitter and a legitimate receiver try to communicate in the presence of an eavesdropper. [11] studies a cooperative jamming approach to increase the security of a wiretap fading channel via distributed relays. In [12] the authors consider a multiple-input single-output (MISO) wiretap scenario where a group of friendly jammers independently transmit noise in the null space of the jammer-legitimate receiver channel in order to maximize the secrecy rate subject to probability of outage and power constraints. The authors of [13] use a game theoretic approach in order to characterize the interaction between the source, that transmits the useful data, and friendly jammers, that assist the source by introducing interference in the eavesdropper channel in order to increase the secrecy capacity of the wiretap channel. In [14], the secrecy capacity of two nodes communicating in the presence of eavesdroppers, placed anywhere in a confined region, is investigated when friendly jammers, with different levels of channel state information, help the legitimate parties by causing interference to possible eavesdroppers.

Orthogonal frequency division multiplexing (OFDM) in wireless communication has been used to allow high data transmission rate in multipath channels ([15], [16], [17]). Recently OFDM is also used to investigate physical layer security ([18], [19]). In [20], the authors show that the secrecy capacity increases with the increase in the number of independent parallel sub-channels.

In this paper, it is assumed that two legitimate parties (Alice and Bob) communicate in the presence of a friendly jammer and an eavesdropper (Eve) over Rayleigh or Rician fading channels. It is also assumed that the eavesdropper is passive whereas the jammer injects interference in the eavesdropper channel in the form of additive noise. We consider transmissions over a bank of parallel fading channels

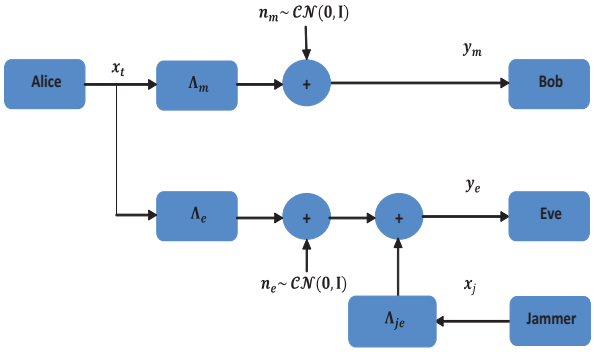

Fig. 1. Parallel Gaussian wiretap channel model with a friendly jammer.

so that the results are also applicable to OFDM systems. By assuming that the friendly jammer adopts particular power allocation policies, the goal of the work is to evaluate average secrecy rates that can be achieved over Rayleigh or Rician fading scenario, with independent or correlated sub-channels.

This paper is organized as follows: In Section II, we present the system model and the problem formulation. Section III presents a brief description of the gain in secrecy rate as result of the presence of a friendly jammer jammer for both cases when sub-channels are independent and correlated. In Section IV, numerical results describe the tradeoff between transmitter and jamming power under a total power constraint. In Section V, we summarize the main contributions of this paper.

II. Problem Formulation

We consider communications over a bank of parallel fading channels where a legitimate user, Alice, tries to communicate with another legitimate user, Bob, in the presence of an eavesdropper and a friendly jammer that interferes only with the eavesdropper channel[1] (see Fig. 1). Note that this scenario arises in systems where Alice, Bob, Eve and the jammer adopt OFDM modulation and demodulation.

We assume that Alice wishes to convey to Bob the vector of symbols $\mathbf{x}_t(l) \in \mathbb{C}^n$ at time l, where n represents the number of parallel sub-channels. The output of the main channel at time l is represented as:

$$\mathbf{y}_m(l) = \mathbf{\Lambda}_m(l)\mathbf{x}_t(l) + \mathbf{n}_m(l) \in \mathbb{C}^n \quad (1)$$

and the output of the eavesdropper channel at time l is represented as:

$$\mathbf{y}_e(l) = \mathbf{\Lambda}_e(l)\mathbf{x}_t(l) + \mathbf{n}_e(l) + \mathbf{\Lambda}_{je}(l)\mathbf{x}_j(l) \in \mathbb{C}^n, \quad (2)$$

where $\mathbf{n}_m(l) \in \mathbb{C}^n$ and $\mathbf{n}_e(l) \in \mathbb{C}^n$ are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian random vectors with zero mean and identity covariance matrix and:

$$\mathbf{\Lambda}_m(l) = \mathrm{diag}\left(\lambda_{m_1}(l), \lambda_{m_2}(l), \ldots, \lambda_{m_n}(l)\right) \in \mathbb{C}^{n\times n} \quad (3)$$

$$\mathbf{\Lambda}_e(l) = \mathrm{diag}\left(\lambda_{e_1}(l), \lambda_{e_2}(l), \ldots, \lambda_{e_n}(l)\right) \in \mathbb{C}^{n\times n} \quad (4)$$

$$\mathbf{\Lambda}_{je}(l) = \mathrm{diag}\left(\lambda_{je_1}(l), \lambda_{je_2}(l), \ldots, \lambda_{je_n}(l)\right) \in \mathbb{C}^{n\times n} \quad (5)$$

are diagonal matrices that contain the complex gains of the parallel sub-channels of the main, eavesdropper and jammer channels, respectively.

We take the main sub-channels, the eavesdropper sub-channels and the jammer sub-channels to be quasi-static fading, so that $\mathbf{\Lambda}_m(l), \mathbf{\Lambda}_e(l)$ and $\mathbf{\Lambda}_{je}(l)$ remain fixed during the entire transmission frame $l = 1, 2, ..., M$. Therefore, we omit the time index l for simplicity of notation. We also take the sub-channel fading coefficients in the main, eavesdropper and jammer channels to be particular realizations of Rayleigh or Rician channels.

The objective of this work is to evaluate an achievable average secrecy rate over a bank of parallel fading channels in the presence of friendly jamming under the different fading regimes. We assume that the transmitter and the friendly jammer send independent zero-mean Gaussian symbols over the different sub-channels, so that $\mathbf{\Sigma}_x = \mathbf{E}[\mathbf{x}_t\mathbf{x}_t^\dagger] = \mathrm{diag}(\sigma_{x_1}, \ldots, \sigma_{x_n})$ and $\mathbf{\Sigma}_j = \mathbf{E}[\mathbf{x}_j\mathbf{x}_j^\dagger] = \mathrm{diag}(\sigma_{j_1}, \ldots, \sigma_{j_n})$ where σ_{x_i} is the power of the data-bearing signal transmitted on the i-th sub-channel and σ_{j_i} is the power of the jamming signal introduced on the i-th sub-channel, and we assume that the transmitter and the jammer satisfy the power constraints $\sum_{i=1}^n \sigma_{x_i} \leq P$ and $\sum_{i=1}^n \sigma_{j_i} \leq P_j$, respectively. An achievable average secrecy rate in this scenario is given by[2]:

$$\bar{R}_s = \mathbf{E}\left[\max_{\sigma_{j_i}} R_s(\sigma_{j_1} \ldots \sigma_{j_n})\right], \quad (6)$$

where the expectation is with respect to the fading statistics of the sub-channels and[3]:

$$R_s(\sigma_{j_1} \ldots \sigma_{j_n}) = \sum_{i=1}^{n}\left[\log\left(1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right) - \log\left(1+\frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2}\right)\right]^+ \quad (7)$$

with $[z]^+ = \max(0, z)$.

We note in passing that the friendly jammer power allocation policy that maximizes the achievable secrecy rate

[1]Note that this represents a simplification of typical wireless communications systems where, due to the characteristics of wireless propagation, the jammer would introduce interference in both the main and the eavesdropper channels. This applies to scenarios where, with the intent of impairing the communication between the transmitter and eavesdropper, the jammer positions himself to be much closer to the eavesdropper than to the legitimate receiver (e.g., [13]).

[2]Note that this jamming strategy is not necessarily optimal but it is convenient [21]. It is well known that, in some cases, further secrecy gains are possible by using structured codewords instead of unstructured Gaussian noise (see [22], [23]).

[3]Throughout the paper, logarithms are to base 2.

in (7) for fixed channel realizations has been solved in [24] under a total jammer power constraint. In particular, we have posed the optimization problem:

$$\max_{\sigma_{j_i}, i=1,..,n} R_s(\sigma_{j_1} \dots \sigma_{j_n}) \tag{8}$$

subject to the constraints $\sum_{i=1}^{n} \sigma_{j_i} \leq P_j$ and $\sigma_{j_i} \geq 0, i = 1, \dots, n$. This work capitalizes on such a characterization of the optimal jammer power allocation policy to study the achievable average secrecy rate in (6) under different fading scenarios.

III. Effect of a Friendly Jammer on the Achievable Average Secrecy Rate

In this section we characterize the achievable average secrecy rate in the scenarios where:

1) The jammer sub-channels are Rayleigh, such that λ_{je_i} are zero-mean complex Gaussian variables, i.e., $\lambda_{je_i} \sim \mathcal{CN}(0, \tau_{je}), i = 1, \dots, n$, where $\tau_{je} = \mathbf{E}[|\lambda_{je_i}|^2]$ is the average power gain of the various jammer sub-channels;

2) The jammer sub-channels are Rician, so that $\lambda_{je_i} \sim \mathcal{CN}\left(\sqrt{\frac{K\tau_{je}}{1+K}}, \frac{\tau_{je}}{1+K}\right), i = 1, ..., n$, where $\tau_{je} = \mathbf{E}[|\lambda_{je_i}|^2]$ is the average power gain of the various jammer sub-channels and the Rician factor K defines the ratio between the LOS (line-of-sight) component power and the scattering component power.

The main and the eavesdropper sub-channels are all assumed to be Rayleigh so that:

$$\lambda_{m_i} \sim \mathcal{CN}(0, \tau_m), \ i = 1, \dots, n \tag{9}$$

where $\tau_m = \mathbf{E}[|\lambda_{m_i}|^2]$ and:

$$\lambda_{e_i} \sim \mathcal{CN}(0, \tau_e), \ i = 1, \dots, n \tag{10}$$

where $\tau_e = \mathbf{E}[|\lambda_{e_i}|^2]$.

We also characterize the achievable average secrecy rate in scenarios where:

1) The fading across the sub-channels is independent, so that the complex Gaussian random variables corresponding to gains of different main, eavesdropper and jammer sub-channels are independent;

2) The fading across the sub-channels is correlated, so that the complex Gaussian random variables corresponding to gains of different main, eavesdropper and jammer sub-channels are correlated.

A. Sub-channels Correlation

We model correlation across sub-channels by considering OFDM transmissions where the duration of the CP is a fraction μ of the OFDM symbol duration nT_s, over a frequency selective (dispersive) channel with exponentially decaying PDP, where, a block is modeled with n serial data symbols, each of duration T_s. We denote by $h(mT_s), \ m = 0, 1, \dots, L-1$, the time domain CIR of the time dispersive (frequency selective) channel. We assume that - by proper system design - the length of LT_s of the CIR is $LT_s \leq \mu n T_s$, the OFDM system becomes equivalent to n flat fading parallel channels with gains that are given by the n-size Fourier transform of the samples of the CIR, that is the channel frequency response [25], namely:

$$g(kF) = \frac{1}{\sqrt{n}} \sum_{m=0}^{L-1} h(mT_s) e^{-j2\pi m T_s k F}$$
$$= \frac{1}{\sqrt{n}} \sum_{m=0}^{L-1} h(mT_s) e^{-j2\pi mk/n}, \qquad k = 0, \dots, n-1. \tag{11}$$

where the channel frequency F equals to k/n cycles per sample.

Note that, we have used the multiplying factor $\frac{1}{\sqrt{n}}$ so that $h(mT_s)$ and $g(kF)$ have the same energy.

Consider the fact that the CIR is a random quantity and, in particularl, each value $h(mT_s)$ for $m = 0, \dots, L-1$ is a complex random variable that is associated with a particular reflection of the transmitted signal. Assume that the different random variables $h(mT_s)$ are independent, complex Gaussian random variables with zero mean and different variances, $\mathbb{E}[|h(mT_s)|^2] = PDP(m), \quad m = 0, \dots, L-1$. We call the function $PDP(m)$ the power delay profile of the channel.

Then, the statistical power of the independent gains corresponding to the L different paths in the CIR is given by [26]:

$$PDP(m) = \beta e^{-\frac{m}{\alpha}}, m = 0, \dots, L-1, \tag{12}$$

where, $\alpha, \beta > 0$ determine the decay rate and average power gain of the channel respectively.

By expressing the relationship between the CIR $h(mT_s)$ and the frequency response $g(kF)$ in matrix form, it is possible to determine the correlation among the sub-channel gains $g(kF)$ in terms of PDP. In particular, we collect the samples of the CIR in $n \times 1$ column vector as:

$$\mathbf{h} = \begin{bmatrix} h(0) \\ h(T_s) \\ \vdots \\ h((L-1)T_s) \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{13}$$

and the samples of the channel frequency response in the $n \times 1$ column vector as:

$$\mathbf{g} = \begin{bmatrix} g(0) \\ g(F) \\ \vdots \\ \vdots \\ g((n-1)F) \end{bmatrix} \tag{14}$$

The relationship between $\mathbf{g}$ and $\mathbf{h}$ can now be expressed as follows

$$\mathbf{g} = \mathbf{F}\mathbf{h} \tag{15}$$

in which, $\mathbf{F}$ is n-size Fourier matrix whose entry in the k-th row, m-th column is $[F]_{km} = \frac{1}{\sqrt{n}} e^{-j2\pi(k-1)(m-1)/n}$. Then the covariance matrix of the sub-channel gains will be simply given by:

$$\mathbf{\Sigma}_g = \mathbb{E}[\mathbf{g}\mathbf{g}^\dagger] = \mathbf{F}\mathbf{\Sigma}_\mathbf{h}\mathbf{F}^\dagger, \tag{16}$$

where

$$\mathbf{\Sigma}_h = \mathbb{E}[\mathbf{h}\mathbf{h}^\dagger] = \mathrm{diag}(PDP(0), \ldots, PDP(L-1), 0, \ldots, 0) \tag{17}$$

So it is possible to retrieve directly from (16) the correlation between any two sub-channel gains.

In the following sections we will analyze the effect of friendly jamming under Rayleigh and Rician fading. We consider a 64×64 parallel fading wiretap channel with $\mu = \frac{1}{4}$, $L = 13$, $\alpha = 2$ and β is chosen according to the average power gain of the channel. Therefore, the duration of the CP which is equal to 16 T_s is larger than the duration of the CIR which is equal to 13 T_s, so that ISI and ICI do not arise.

B. Achievable Average Secrecy Rates Over Rayleigh Fading

Fig. 2 shows the value of the achieved average secrecy rate vs. the transmitter available power P when the various sub-channels are subject to independent Rayleigh fading. In particular, we set $P_j = 5$ and the average power gains of the main, eavesdropper and jammer channels to be the same, i.e., $\tau_m = \tau_e = \tau_{je} = 1$. We consider four different jammer power allocation strategies. We analyze the scenario where the transmitter adopts the power allocation scheme that achieves the secrecy capacity without the presence of a friendly jammer, for each sub-channels realizations [8], and i) the jammer optimizes its power allocation strategy according to the particular transmitter power allocation policy by solving the optimization problem in (8) for each channel realizations; or ii) the jammer distributes its power equally across all the sub-channels; or iii) the jammer does not inject power into the eavesdropper channel. We also analyze the scenario where iv) the jammer and the transmitter jointly optimize their power allocation policies in order to maximize the secrecy rate for each sub-channels realizations. We can clearly observe the increase in the achievable average secrecy rates due to the presence of the friendly jammer.

Fig. 3 shows the average secrecy rate obtained over independent and correlated Rayleigh fading channels vs.

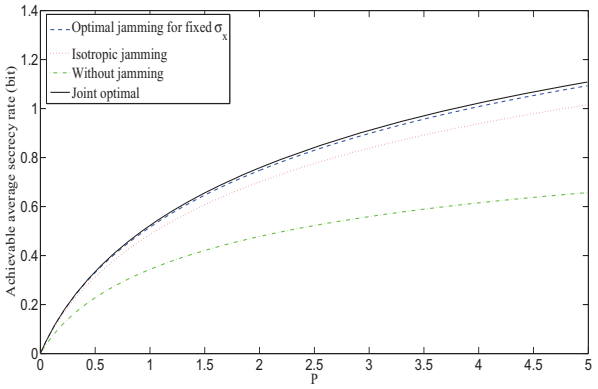

Fig. 2. Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$, when the transmitter, eavesdropper and jammer channel are subject to independent Rayleigh fading for the different power allocation strategies. $\tau_m = \tau_e = \tau_{je} = 1$.

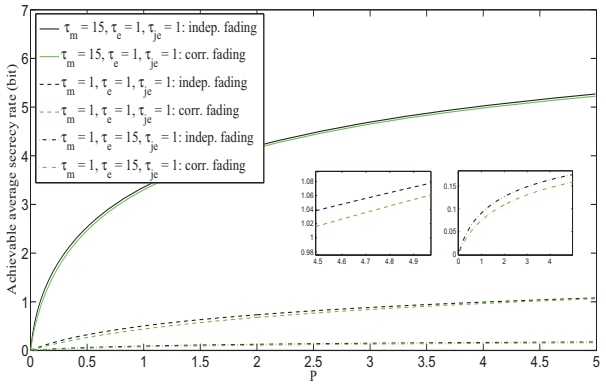

Fig. 3. Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$, when the transmitter, eavesdropper and jammer channels are subject to independent or correlated Rayleigh fading for different average power gains.

the transmitter available power P. We also set $P_j = 5$ and consider the case when the jammer optimizes its power allocation strategy according to the fixed transmitter power allocation policy. We consider three different channel configurations, corresponding to different relations between the average power gain of the main, eavesdropper and jammer channels: i) the transmitter average power gain is 15 times larger than the eavesdropper and the jammer average power gains, i.e., $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; ii) the transmitter, eavesdropper and jammer average power gains are same, i.e., $\tau_m = \tau_e = \tau_{je} = 1$; and iii) the eavesdropper average power gain is 15 times larger than the transmitter and the jammer average power gain, i.e., $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

We observe, in Fig. 3, that the achieved average secrecy rate obtained with correlated sub-channels is less than the achieved average secrecy rate for the case of independent sub-channels. This fact can be explained by noting that independent sub-channels provide a higher level of diversity to be exploited to guarantee favorable channel realizations for the legitimate receiver. It turns out that the relative loss due

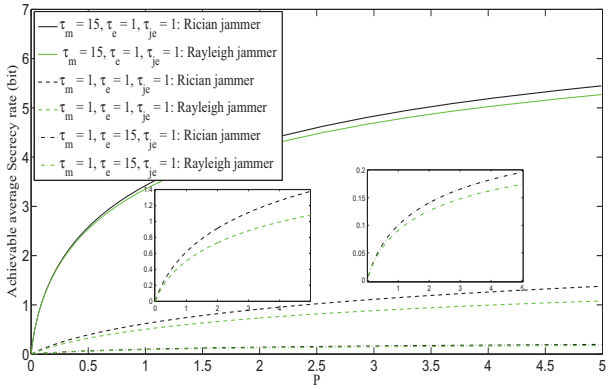

Fig. 4. Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$, when the transmitter and eavesdropper channels are subject to independent Rayleigh fading and jammer channel is subject to independent Rayleigh or Rician fading for different average power gains.

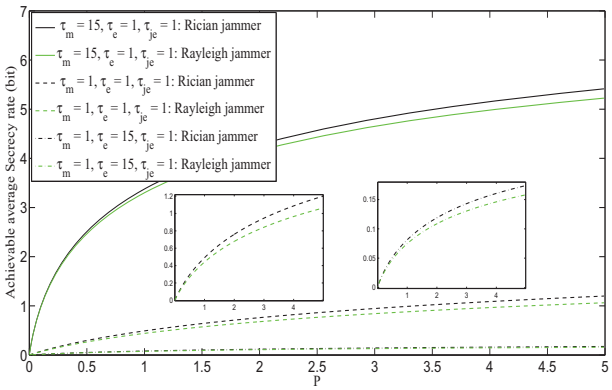

Fig. 5. Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$, when the transmitter and eavesdropper channels are subject to correlated Rayleigh fading and jammer channel is subject to correlated Rayleigh or Rician fading for different average power gains.

to the presence of sub-channels correlation is higher when the eavesdropper channel average power gain is much better than the main channel average power gain (see zooms in Fig. 3).

C. Achievable Average Secrecy Rates Over Rician Fading

In this subsection, we consider the gain in the achievable secrecy rates due to the presence of a line-of-sight channel for the jammer, for both the cases when sub-channels are independent and correlated. Fig. 4 and Fig. 5 show the value of the achieved average secrecy rate vs. the transmitter available power P when the various sub-channels are subject to independent or correlated fading, the main and eavesdropper sub-channels are subject to Rayleigh fading, and the jammer sub-channels are subject to Rayleigh or Rician fading. We also set $P_j = 5$ and consider the case where the jammer optimizes its power allocation strategy, according to the particular transmitter power allocation policy, by solving the optimization problem in (8) for each sub-channels realizations. We also consider the previous channel configurations corresponding to the different relations between the average power gain of the main, eavesdropper and jammer channel: i) $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; ii) $\tau_m = \tau_e = \tau_{je} = 1$; and iii) $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

Fig. 4 depicts the case in which sub-channels are independent, whereas in Fig. 5 sub-channels are correlated. In both cases, it is clear that the gain of the achievable secrecy rates is higher when the friendly jammer channel is Rician than when the friendly jammer channel is Rayleigh. This result relates to the fact that the jammer can benefit from the LOS component present in the Rician fading model to impair the eavesdropper in a more efficient manner. It is also clear that the relative loss due to the presence of sub-channels correlation is higher when the eavesdropper channel average power gain is much better than the main channel average power gain (see zooms in Fig. 4 and Fig. 5).

IV. Fixed Total Budget Power

It is also interesting to analyze the scenario where there is a fixed power budget to be distributed between the transmitter and the jammer. This could have various implications for wireless network operators that intend to use jammers to augment the security of their network, but yet have a certain budget power to be shared between the transmitter (e.g. a base station) and the deployed jammers.

We analyze numerical results for the case of Rayleigh and Rician fading with independent sub-channels[4], with a total power budget of 5 to be distributed between the transmitter and the jammer (i.e., $P_j = 5 - P$). We restrict the analysis to the case where the transmitter uses the power allocation policy that maximizes the instantaneous secrecy capacity for each sub-channels realizations (see [8]) whereas the jammer uses the power allocation policy embodied in the optimization problem in (8) also for each sub-channels realizations.

The fraction of power devoted to data transmission and the one for jamming are determined in order to maximize the achievable average secrecy rate. This way, we want to provide some insight on which amount of the total available power should be devoted to the friendly jammer for the different channel scenarios under consideration.

Fig. 6, Fig. 7, Fig. 8 and Fig. 9 show the optimal value of the power that should be allocated to the transmitter considering different relations between the average power gain of the main and eavesdropper sub-channels, for various average power gains of the jammer sub-channels: in Fig. 6 and Fig. 7, the average power gains of the main and the eavesdropper sub-channels are equal, i.e., $\tau_m = \tau_e$; whereas in Fig. 8 and Fig. 9, the average power gains of the main sub-channels are 15 times higher than those of the eavesdropper channel, i.e., $\tau_m = 15\ \tau_e$. For both cases the main and the eavesdropper

[4]Numerical results with correlated sub-channels show the same trends that are observed in the case of independent Rayleigh and Rician fading.

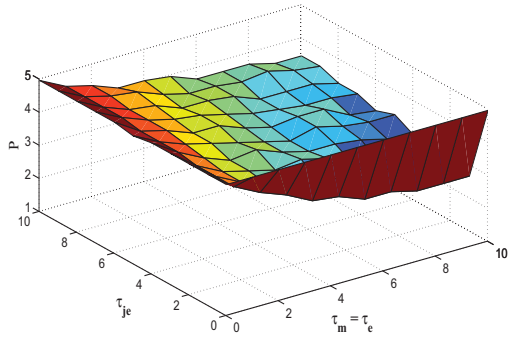

Fig. 6. Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper channels are Rayleigh and the jammer channel is also Rayleigh for $\tau_m = \tau_e$. Total power budget of $P + P_j = 5$

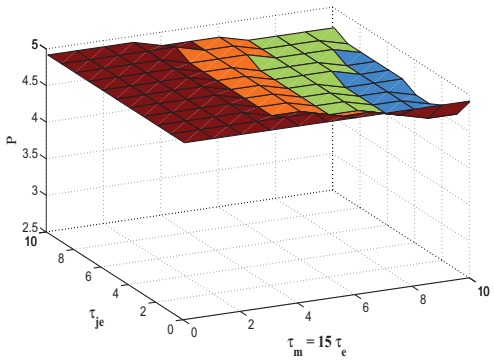

Fig. 8. Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper are Rayleigh and the jammer channel is also Rayleigh for $\tau_m = 15\ \tau_e$. Total power budget of $P + P_j = 5$

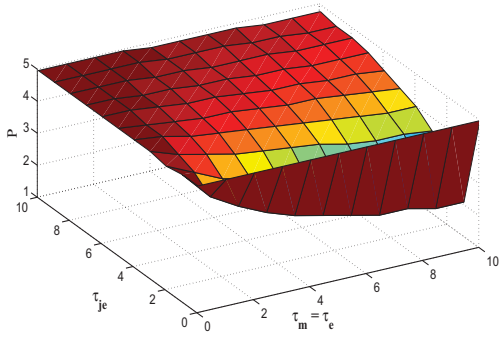

Fig. 7. Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper channels are Rayleigh and jammer channel is Rician for $\tau_m = \tau_e$. Total power budget of $P + P_j = 5$

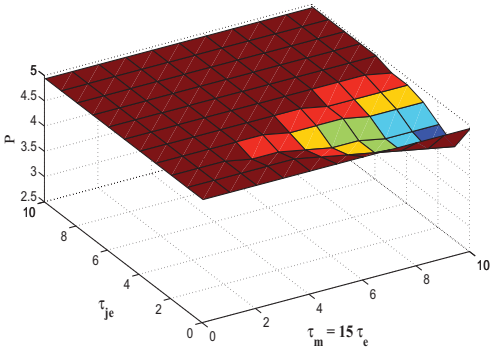

Fig. 9. Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper are Rayleigh and the jammer channel is Rician for $\tau_m = 15\ \tau_e$. Total power budget of $P + P_j = 5$

sub-channels are subject to Rayleigh fading, and the jammer sub-channels are subject to either Rayleigh or Rician fading . We also consider the case where the average power gains of the eavesdropper sub-channels are 15 times higher than those of the main sub-channels, i.e., $\tau_e = 15\ \tau_m$. But since in this case, higher fraction of the available power of the jammer is allocated to the eavesdropper channel to decrease the eavesdropper channel quality, the secrecy rate is not sufficiently increase and for this reason, we did not put any figure related this case.

V. Conclusion

We have studied the performance of transmitter / jammer power allocation strategies for secure communication over a bank of parallel, quasi-static fading channels in the presence of an eavesdropper and a friendly jammer. We characterized the effect of the optimal jammer power allocation policy, for any fixed transmitter power allocation policy over Rayleigh or Rician fading scenarios. The results demonstrate the increase in the average achievable secrecy rate obtained with friendly jamming. The achieved average secrecy rate is higher for independent sub-channels than when sub-channels are correlated. On the other hand, higher secrecy rates can be achieved when the channel from the friendly jammer to the eavesdropper is Rician with respect to the case of Rayleigh fading. We have also highlighted the loss due to correlation among the sub-channels in different fading scenarios: correlation has the most detrimental effect when the eavesdropper enjoys better channel conditions than the legitimate parties. We also investigated the distribution of power between the transmitter and the jammer, when there is a fixed total power budget. Overall, these results showcase the efficacy of friendly jamming for OFDM type of communications systems in various operating regimes.

Acknowledgment

The author would like to thank Miguel Rodrigues, University College London, for his helpful comments and suggestions of this work.

References

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[2] Y. Liang, H. V. Poor and S. Shamai (Shitz), *Information theoretic security*. Dordrecht, The Netherlands: Now Publishers, 2009.
[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.
[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.
[5] I. Csiszr and J. Krner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–349, May 1978.
[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[7] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[8] P. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
[10] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.
[11] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
[12] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *Proc. of IEEE Statistical Signal Processing Workshop (SSP), 2012 IEEE*, Aug. 2012, pp. 389–392.
[13] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, 2009.
[14] Pinto, P.C. and Barros, J. and Win, M.Z., "Wireless physical-layer security: The case of colluding eavesdroppers," *in Proc. of IEEE International Symposium on Information Theory (ISIT), Seoul, Korea, 2009*, pp. 2442–2446, Jun.28-Jul.3 2009.
[15] J. A. C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come," *IEEE Communications Magazine*, vol. 28, no. 5, pp. 5–14, May 1990.
[16] W. Y. Zou and W. Yiyan, "COFDM: an overview," *IEEE Transactions on Broadcasting*, vol. 41, no. 1, pp. 1–8, Mar. 1995.
[17] Ramjee Prasad, *OFDM for wireless communication system*. Bosto, London: Artech House, Inc., 2004.
[18] N. Romero-Zurita, M. Ghogho and D. McLernon1, "Physical Layer Security of MIMO Frequency Selective Channels by Beamforming and Noise Generation," *19th European Signal Processing Conference, Barcelona, Spain*, 2011.
[19] F. Renna, N. Laurenti and Poor, H.V., "Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.
[20] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," *44th Annual Allerton Conference on Communication, Control, and Computing. Monticello, Illinois*, Sept.27-29 2006.
[21] S. Shafiee and S. Ulukus, "Correlated jamming in multiple access channel," *in Proc. Conference in Information Science and Systems (CISS), The Johns Hopkins University*, Mar.16-18. 2005.
[22] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transaction on Information Theory*, vol. 54, no.9, pp. 4005–4019, 2008.
[23] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," *in Proc. of IEEE International Symposium on Information Theory (ISIT), Toronto, Canada*, pp. 389–393, Jul. 2008.
[24] M. Ara, H. Reboredo, F. Renna, and M. R. D. Rodrigues, "Power allocation strategies for OFDM Gaussian wiretap channels with a friendly jammer," *in Proc. of IEEE International Conference on Communications (ICC), Budapest, Hungrary*, Jun. 2-5 2013.
[25] G. L. Stber, *Principles of Mobile Communications*. 2nd. ed. Kluwer Academic Publisher, 2002.
[26] Andrea Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

Munnujahan Ara received her Ph.D. degree in Telecommunications Engineering from the University of Porto (MAP-Tele), Portugal in 2013. She is cuurently an Asistant Professor, Mathematics Department, Khulna University, Khulna, Bangladesh. She was a research visitor at University College London (UCL), UK in 2012. Between 2009 to 2013, she was a researcher at the Institute of Telecommunications (IT), Porto, Portugal.