Wireless Secrecy Regions with Friendly Jamming

João P. Vilela, Matthieu Bloch, João Barros, Steven W. McLaughlin

***Abstract*— Inspired by recent results on information-theoretic security, we consider the transmission of confidential messages over wireless networks, in which the legitimate communication partners are aided by friendly jammers. We characterize the security level of a confined region in a quasi-static fading environment by computing the probability of secrecy outage in connection with two new measures of physical-layer security: the *jamming coverage* and the *jamming efficiency*. Our analysis for various jamming strategies based on different levels of channel state information provides insight into the design of optimal jamming configurations and shows that a single jammer is not sufficient to maximize both figures of merit simultaneously. Moreover, a single jammer requires full channel state information to provide security gains in the vicinity of the legitimate receiver.**

I. Introduction

Today's networks are secured essentially by means of encryption algorithms that are executed at the upper layers of the protocol architecture. These primitives are designed and implemented assuming data is error-free, an abstraction enabled by the use of error-correcting codes at the physical layer. In contrast, several information-theoretic results, based on Wyner's wiretap channel model [2], support the idea that there is much to be gained from coding not just for error correction but also for security at the physical layer. "Physical-layer security" has thus known a growing interest in the past few years, motivated in large part by applications to wireless communications.

A substantial body of work lays its foundation on the Gaussian wiretap channel [3], in which the channel between the legitimate partners and the eavesdropper's channel are additive white Gaussian noise (AWGN) channels. For this model, the secrecy capacity, defined as the maximum transmission rate at which the eavesdropper is unable to acquire any information, can be obtained from the signal-to-noise ratios (SNRs) of the receivers by subtracting the Shannon capacity of the eavesdropper's channel to the Shannon capacity of the legitimate receiver's channel.

This work was partly supported by the Fundação para a Ciência e Tecnologia (Portuguese Foundation for Science and Technology) under grants SFRH/BD/28056/2006 and PTDC/EIA/71362/2006. Part of this work was presented at the IEEE International Conference on Communications[1].

João P. Vilela (joaovilela@dcc.fc.up.pt) is with Instituto de Telecomunicações, Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto, rua do Campo Alegre 1021/1055, 4169-007, Porto, Portugal.
Matthieu Bloch (mbloch@ece.gatech.edu) is with the School of ECE, Georgia Institute of Technology, Atlanta, USA and GT-CNRS UMI 2958, 2-3 rue Marconi, 57070 Metz, France.
João Barros (jbarros@fe.up.pt) is with Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores, Faculdade de Engenharia, Universidade do Porto, rua Dr. Roberto Frias s/n, 4200-465, Porto, Portugal.
Steven W. McLaughlin (swm@ece.gatech.edu) is with the School of ECE, Georgia Institute of Technology, Atlanta, GA 30332–0250, USA.

Several fading models have been considered to generalize the Gaussian wiretap channel model. For quasi-static fading models, [4], [5] provide a detailed characterization in terms of the probability of outage of secrecy capacity and show that fading alone guarantees that information-theoretic security is achievable, even when the eavesdropper has a better average SNR than the legitimate receiver. For ergodic fading models, [6], [7], [8], [9] provide the secrecy capacity under different levels of channel state information (CSI) and the corresponding optimal power and rate allocation. The wiretap channel with multiple antennas is analyzed in [10], [11], [12].

Secrecy rate can be increased in two ways: (a) by improving the SNR of the legitimate receiver (e.g. by shortening the distance to the transmitter) or (b) by reducing the SNR of the eavesdropper (e.g. by adding controlled interference). Interference then emerges as a valuable resource for wireless security. From the point of view of the attacker, correlated jamming techniques are known to cause severe disruption of the communications flow by exploiting the available information on the transmitted signals [13]. However, jamming can also be used by the legitimate communication partners to increase the noise level of the eavesdropper and ensure higher secure communication rates. This idea has already appeared in the literature under the name of artificial noise [14] or cooperative jamming [15], and has been used in other contexts, such as secure relaying [16].

To develop our understanding of the benefits of jamming for secure communications in wireless networks, we make the following contributions:

- *Security measures for jamming:* we introduce the jamming coverage and the jamming efficiency as security measures;
- *Jamming strategies:* we characterize the secrecy outage probability for three jamming strategies that rely on various levels of channel state information (CSI);
- *Effect of CSI on secrecy:* we analyze how the variation of jammer location and power affects the coverage and efficiency for jamming strategies with different CSI requirement;
- *Multiple jammers:* we evaluate the effect of additional jammers on the security of the wireless system.

Our work differs from previous studies of jamming for secure communications [15], [16] because it puts forward two new aspects that were not previously accounted for:

- *CSI*: we study the effect of access to CSI and show that it has a profound impact on secrecy. In particular, CSI about the legitimate receiver's channel helps the jammer mitigate harmful interference whereas CSI about the eavesdropper's channel help the jammer identify when to impact the eavesdropper;

- *fading*: our models incorporate the effect of multipath fading. In a fading environment, there is always a non-zero probability that the jammer-eavesdropper channel is stronger than the jammer-receiver channel, irrespective of the distance. This becomes particularly relevant if CSI is available and favors the detection of jamming opportunities.

The remainder of the paper is organized as follows. In Section II, we present the system setup and we introduce the notions of secrecy outage probability, jamming coverage and jamming efficiency. Section III extends the concept of secrecy outage probability to scenarios in which a friendly jammer is available and characterizes the performance different jamming strategies that rely on distinct CSI requirements. The effect of varying location and transmission power of the jammer on the performance of such strategies is evaluated in Section IV. The case of multiple jammers is considered in Section V. Finally, Section VI concludes the paper.

II. Preliminaries

We consider a setup in which a transmitter and the corresponding receiver are located in a confined region (say a building or a conference room) and wish to communicate securely in the presence of an illegitimate receiver, hereafter called the *eavesdropper*. In addition, a set of N nodes, hereafter called *jammers*, emit white Gaussian noise that causes interference to both the legitimate receiver and the eavesdropper. Channels between all pair of nodes are modeled as independent quasi-static Rayleigh fading channels; the transmitter is subject to the short term average-power constraint P_t whereas each jammer is subject to a short-term average power constraint P_j. Specifically, for each channel, fading coefficients remain constant during the transmission of an entire codeword but they change randomly and independently from one codeword to another according to a complex Gaussian distribution with variance c/d^α, where d is the distance between the two nodes, α is the path-loss exponent, and c is a normalization constant. We let d_{jr} and d_{tr} denote the distances from jammer j ($1 \leq j \leq N$) to the receiver and from the transmitter to the receiver, respectively, and we introduce the dimensionless constants $c_{jr} = \frac{P_j}{N_0}\frac{c}{d_{jr}^\alpha}$ and $c_{tr} = \frac{P_t}{N_0}\frac{c}{d_{tr}^\alpha}$. Then, the instantaneous signal-to-interference-plus-noise ratio (SINR) at the receiver is the random variable

$$\Gamma_r = \frac{c_{tr}G_{tr}}{1+\Sigma_{j=1}^N c_{jr}G_{jr}}, \tag{1}$$

where G_{tr} and G_{jr} are independent exponential random variables with unit mean. Similarly, we let d_{je} and d_{te} denote the distances from the jammer j to the eavesdropper and from the transmitter to the eavesdropper, respectively, and we introduce the constants $c_{je} = \frac{P_j}{N_0}\frac{c}{d_{je}^\alpha}$ and $c_{te} = \frac{P_t}{N_0}\frac{c}{d_{te}^\alpha}$. The instantaneous SINR at the eavesdropper is the random variable

$$\Gamma_e = \frac{c_{te}G_{te}}{1+\Sigma_{j=1}^N c_{je}G_{je}}, \tag{2}$$

where G_{te} and G_{je} are also exponential random variables with unit mean. For a given realization (γ_r,γ_e) of (Γ_r,Γ_e), the instantaneous secrecy capacity [3] of the channel between the transmitter and the legitimate receiver is

$$C_s = \max(C_r - C_e,\ 0),$$

where $C_r = \log(1+\gamma_r)$ is the capacity of the legitimate receiver channel and $C_e = \log(1+\gamma_e)$ denotes the capacity of the eavesdropper's channel. In presence of fading, these capacities can be treated as random variables that vary with the instantaneous signal-to-noise ratio.

We assume that the transmitter knows the instantaneous received SINR of the legitimate receiver, so that both can agree on a code with secrecy rate R_s. Communication is secure if the instantaneous secrecy capacity C_s is higher than the target secrecy rate R_s. If $C_s < R_s$, then security is compromised and we can say that a secrecy outage occurs. The secrecy outage probability was introduced in [14], [4] to evaluate the security of wireless communication systems and is defined as

$$\begin{aligned}\mathcal{P}_{out}(R_s) &= P[C_s < R_s] = P[C_r - C_e < R_s] \\ &= P[\log(1+\Gamma_r) - \log(1+\Gamma_e) < R_s].\end{aligned}$$

The operational meaning of this measure is twofold [5]. First, it provides the fraction of fading realizations for which the wireless channel can support a secure rate of R_s bits/channel use. Second, it provides a security metric for the situation in which the transmitter and receiver have no CSI about the eavesdropper. In this case, the transmitter has no choice but to set the secrecy rate to a constant R_s, thus implicitly assuming that the instantaneous capacity of the eavesdropper channel is at least $C_e' = C_r - R_s$. Notice that, to obtain low values of secrecy outage probability, the eavesdropper must be located far away from the communicating nodes, and there is a large area where the eavesdropper could compromise the secrecy of the system. The interference created by the jammer can potentially lead to smaller secrecy outage probability, even for situations in which the eavesdropper is not far from the transmitter or receiver.

To distinguish the cases with jamming ($P_j > 0$) and without jamming ($P_j = 0$), we add the superscripts j and nj, respectively, unless it is obvious from the context. For example, the secrecy outage probability without jamming is denoted as $\mathcal{P}_{out}^{nj}$ whereas the capacity of the legitimate receiver channel with a jammer is denoted by C_r^j.

A. Performance Measures

To analyze the effect of jamming on security, we focus on the ratio between the secrecy outage probability without and with jamming $\Delta\text{P}_{\text{out}} = \dfrac{\mathcal{P}_{out}^{nj}}{\mathcal{P}_{out}^{j}}$. This measure of security captures the reduction in the secrecy outage probability introduced the jammer, and should be as large as possible.

The *helpful interference region* is defined as the set of eavesdropper's positions (x_e, y_e) for which $\Delta\text{P}_{\text{out}}(x_e, y_e) > 1.0$. Similarly, the *harmful interference region* is the set of eavesdropper's positions (x_e, y_e) that satisfy $\Delta\text{P}_{\text{out}}(x_e, y_e) \leq 1.0$. Our measures of interest are (a) the *jamming coverage*, defined as the total area of the helpful interference region, and (b) the *jamming efficiency*, defined as the average $\Delta\text{P}_{\text{out}}(x_e, y_e)$

over all (x_e, y_e) belonging to a confined region $\mathcal{R}$. For a given system setup (i.e. location and power of source and jammers, and location of receiver and eavesdroppers), ΔP_{out} is an exact value obtained analytically with the formulas of Section III. In general, jamming coverage and jamming efficiency cannot be obtained in closed form; we evaluate them numerically by spatial sampling. For each location of the eavesdropper ΔP_{out} is calculated and the corresponding samples containing ΔP_{out} for all eavesdropper locations are then used to derive the jamming coverage and efficiency.

Ideally, we would like to maximize jamming coverage, while ensuring high jamming efficiency. We will see that, in general, this goal cannot be achieved with a single jammer.

B. Jamming strategies

Several jamming strategies have already been investigated in the literature, such as strategies based on Gaussian noise [14], [16], Gaussian codebooks [15], [17] or more structured codebooks based on lattices [18]. The latter strategies have been shown to outperform jamming with Gaussian noise for situations in which the jammer has access to perfect CSI for all channels, and a comprehensive survey of these techniques can be found in [19].

To analyze how the availability of CSI affects the secrecy benefits of jamming, we restrict ourselves to the simplest jamming strategy, in which the jammer emits white Gaussian noise. While we do not claim that this choice is necessarily optimal, we note that jamming noise is still relevant from a practical standpoint because it does not require interfering signals to be perfectly synchronized when they reach the eavesdropper's device.

III. Wireless Secrecy with One Jammer

A. Secrecy Outage Probability for Blunt Jamming

In this section, we consider the situation in which the jammer emits white Gaussian noise with variance P_j at all times. We call this jammer a *blunt jammer* because it disregards any possible CSI and transmits at a constant power $P_{\text{blunt}} = P_J$.

Proposition 1: The secrecy outage probability for the blunt jammer is given by

$$P[C_s < R] = 1 - \frac{e^{-\kappa}}{c_{jr}c_{je}} \frac{c_{je}}{\left(\kappa + \frac{1}{c_{jr}} - \frac{\beta}{c_{je}}\right)} + \frac{e^{-\kappa}}{c_{jr}c_{je}} \tag{3}$$
$$\times \left(\kappa + \tfrac{1}{c_{jr}} - \tfrac{\beta}{c_{je}}\right)^{-2} \left[\beta\left(\kappa + \tfrac{1}{c_{jr}} - \tfrac{\beta}{c_{je}} + 1\right) \times \Omega\left(\tfrac{1+\beta}{c_{je}}\right) + \left(\kappa + \tfrac{1}{c_{jr}} - \tfrac{\beta}{c_{je}} - \beta\right) \times \Omega\left(\tfrac{1+\beta}{\beta}\left(\kappa + \tfrac{1}{c_{jr}}\right)\right)\right]$$

with $\kappa = \dfrac{e^R - 1}{c_{tr}}$, $\beta = e^R \dfrac{c_{te}}{c_{tr}}$ and $\Omega(x) = e^x E_1(x)$ [1].

Proof: See Appendix A ∎

The effect of blunt jamming on the secrecy outage probability is illustrated in Figure 1, in which each point represents a potential location of the eavesdropper and shows the corresponding value of ΔP_{out}. The helpful interference region, delimited by the thick white line around the jammer, is the area where the jammer's interference reduces the secrecy outage probability. The harmful interference region corresponds to the area where the jammer's interference is more harmful to the legitimate receiver than the jammer. The lighter the region around the jammer, the smaller the secrecy outage probability. For example, if the eavesdropper is located close to the jammer at the position $(6, 0)$, jamming reduces the secrecy outage probability from 0.39 to 0.12 (i.e. $\Delta P_{out} = 3.25$).

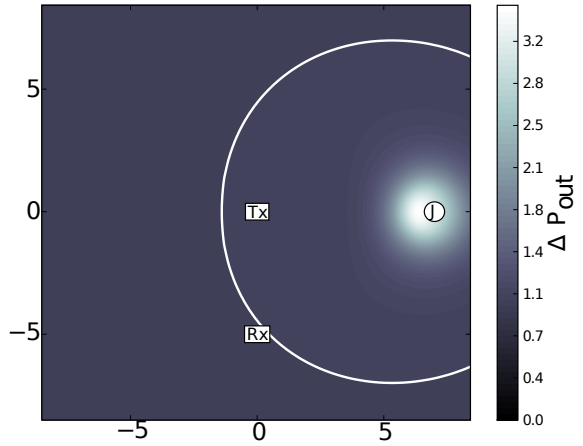


Fig. 1. Example of the impact of blunt jamming on the secrecy outage probability. For each position of the eavesdropper on the map, we compute the factor of change of the secrecy outage probability with blunt jamming, ΔP_{out}. The locations of the transmitter (Tx), receiver (Rx), and jammer (J) are (0,0), (0,-5), and (7,0), respectively. Secrecy outage probabilities are obtained for a target secrecy rate $R_s = 0.1$ and path-loss $\alpha = 4$. The target secrecy rate is normalized with respect to the capacity of the AWGN channel with the same average SNR.

Understanding the trade-off between these two types of interference and the impact of CSI is crucial. Factors such as received power and distance, as well as channel quality from the jammer to other nodes play an important role in securing the wireless system. This observation calls for jamming strategies that dynamically adjust to the environment and whose goal is to maximize the helpful interference region while keeping the harmful interference region constrained.

B. Jamming Strategies

In this section we characterize alternative jamming strategies that rely on different levels of CSI.

1) Cautious Jamming: A cautious jammer takes advantage of the knowledge of the CSI between itself and both the legitimate receiver and the eavesdropper and decides opportunistically when to jam. It jams whenever it has a higher gain to the eavesdropper than to the legitimate receiver, and switches off otherwise. The power transmitted by a cautious jammer P_{cautious} is then given by

$$P_{\text{cautious}} = \begin{cases} P_J & \text{if } \dfrac{G_{jr}}{d_{jr}^{\alpha}} < \dfrac{G_{je}}{d_{je}^{\alpha}} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 2: The secrecy outage probability for the cau-

[1] $E_1(x)$ represents the exponential integral – a non-elementary function given by the integral $\int_x^{\infty} \frac{e^{-t}}{t} dt$. This integral is easily computable numerically.

tious jammer is given by

$$P[C_s < R] = 1 - \frac{e^{-\kappa}}{\lambda(1+\beta)} + \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\Omega(\nu)-\Omega(\mu\rho)}{\xi}\right) + \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\eta\xi-\Omega(\mu\rho(1-\eta)+\eta\nu)(\mu-\eta\xi)}{\xi^2(\mu-\eta\xi)} - \frac{\Omega(\mu\rho)(\mu-\eta\xi)(\eta\mu\rho-\eta\nu-1)}{\xi^2(\mu-\eta\xi)}\right) - \frac{e^{-\kappa}}{c_{jr}c_{je}}\eta(\eta(\beta+1)-1)\left(\frac{\Omega(\mu\rho(1-\eta)+\eta\nu)-\Omega(\mu\rho)}{\eta\xi}\right) - \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\xi-\Omega(\nu)(\mu-\xi)-\Omega(\mu\rho)(\mu-\xi)(\mu\rho-\nu-1)}{\xi^2(\mu-\xi)}\right)$$

where $\delta = \left(\frac{d_{jr}}{d_{je}}\right)^{\alpha}$, $\lambda = \begin{cases} 2 & \text{if } \delta \leq 1 \\ 1+\delta & \delta > 1 \end{cases}$ and $\eta = \begin{cases} \frac{c_{je}}{c_{je}+\beta c_{jr}} & \text{if } \delta \leq 1 \\ \frac{c_{je}}{c_{je}+\beta c_{jr}\delta} & \delta > 1 \end{cases}$.

The variables κ and β are defined as in Proposition 1, and $\xi = \left(\kappa + \frac{1}{c_{jr}} - \frac{\beta}{c_{je}}\right), \nu = \left(\frac{1+\beta}{c_{je}}\right), \mu = \left(\kappa + \frac{1}{c_{jr}}\right)$ and $\rho =$

Proof: See Appendix B. ∎

2) Adaptive Jamming: An adaptive jammer has CSI about the channel to the legitimate receiver only. This strategy corresponds to a situation in which the eavesdropper intercepts the communications without providing any sign of its presence. In this case, the jammer defines a threshold for the channel quality τ, above which it will stop jamming since it is likely that his induced noise will hurt the legitimate receiver more than a potential eavesdropper. The transmission power of the jammer, P_{adaptive}, is then given by

$$P_{\text{adaptive}} = \begin{cases} P_J & \text{if } G_{jr} < \tau \\ 0 & \text{otherwise} \end{cases}$$

Proposition 3: The secrecy outage probability for the adaptive jammer is given by

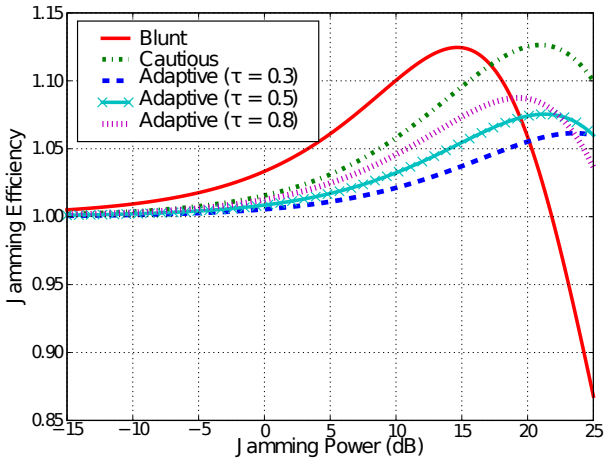
$$P[C_s < R] = 1 - \frac{e^{-\tau}e^{-\kappa}}{1+\beta} + \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\Omega(\nu)-\Omega(\mu\rho)}{\xi}\right) - \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\xi-\Omega(\nu)(\mu-\xi)-\Omega(\mu\rho)(\mu-\xi)(\mu\rho-\nu-1)}{\xi^2(\mu-\xi)}\right) - \frac{e^{-\kappa}\beta\ e^{-\mu c_{jr}\tau}(1+c_{jr}\tau)}{c_{jr}c_{je}}\left(\frac{\Omega(\nu+\beta\frac{c_{jr}}{c_{je}}\tau)-\Omega(\mu\rho+\mu c_{jr}\tau)}{\xi}\right) - \frac{e^{-\kappa}\beta\ e^{-\mu c_{jr}\tau}}{c_{jr}c_{je}}\left[\frac{\Omega(\mu\rho+\mu c_{jr}\tau)(\mu-\xi)(\mu\rho-\nu+\tau c_{jr}(\mu-\frac{\beta}{c_{je}})-1)}{\xi^2(\mu-\xi)} - \frac{\xi-\Omega(\nu+\beta\frac{c_{jr}}{c_{je}}\tau)(\mu-\xi)}{\xi^2(\mu-\xi)}\right]$$

where κ and β are defined as in Proposition 1, and ξ, ν, μ and ρ are defined as in Proposition 2.

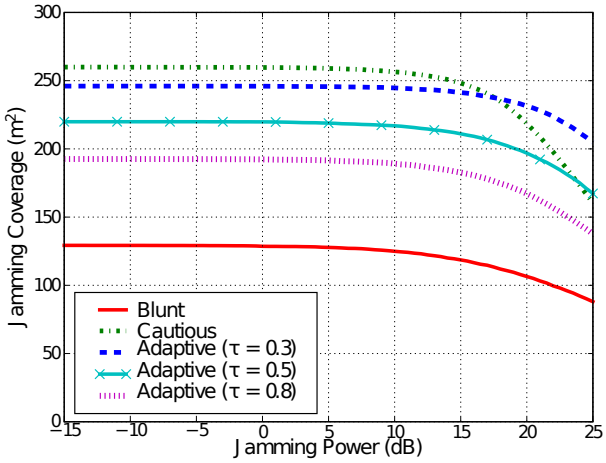
Proof: See Appendix B. ∎

IV. Impact of Channel State Information on Secrecy

Although the jammer can have an adverse effect on the legitimate receiver, a careful selection of the location and transmission power can enhance security by causing controlled interference to the eavesdropper. Figure 2 shows an example of the potential benefits of increased transmit power for a specific location of the jammer. Notice that up to a certain jamming power, the efficiency increases without a significant loss of coverage. However, the exact tradeoff between coverage and efficiency depends on the jamming strategy used. In the remainder of this section, we analyze how the variation of jammer location and transmission power affects coverage and efficiency for the various jamming strategies, in connection with their requirements in terms of CSI.



(a) Efficiency

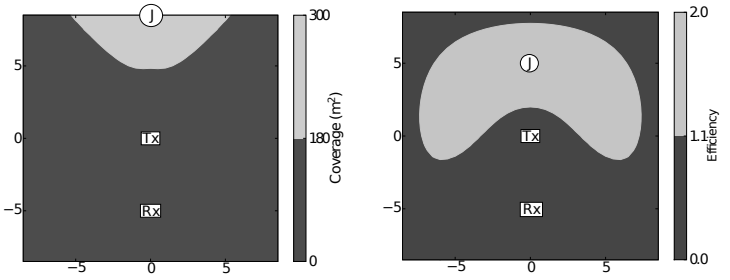


(b) Coverage

Fig. 2. This figure shows an example of the effect of varying the transmit power of the jammer on the jamming coverage and efficiency for a specific location of the jammer ($x_j = 0$, $y_j = 2$).

A. System Setup and Measure Computation

We consider a scenario in which the transmitter and the receiver are located in a confined area (say a building or a conference room) and wish to communicate securely with the aid of a friendly jammer. In particular, any eavesdropper located within the confined region should not be able to extract much information from the intercepted signals. To model the wireless nature of the medium, we set the path loss exponent to 4 and the normalization constant c to the free-space path gain for 2.4 GHz transmission at the reference distance of 1 m, which is common for micro-cellular systems [20]. The transmitter and receiver are fixed at locations of $(0, 0)$ and $(0, -5)$, respectively. The target secure transmission rate is



(a) Coverage (b) Efficiency

Fig. 3. Figures (a) and (b) illustrate the value of coverage and efficiency obtained for various jammer locations. J indicates the optimal placement of the jammer. The maximum coverage results from $P_j = 10$dBm and the maximum efficiency from $P_j = 10$dB. Regions where placing a jammer leads to a coverage above 180 m^2 and efficiency above 1.1 are also shown in light gray.

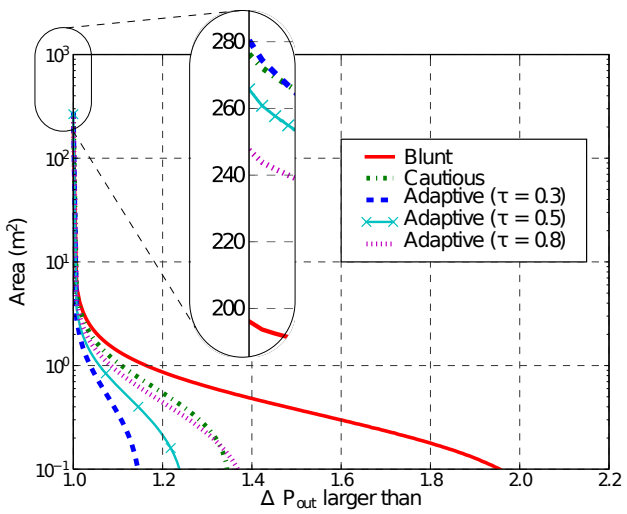


Fig. 4. Comparison between the three strategies for the jammer location of Figure 3(a). The plot shows the area of eavesdropper locations leading to a ΔP_{out} above a certain value (x axis). The zoomed area at $\Delta P_{out} = 1$ shows the coverage attained by each strategy, namely 197 m^2 - blunt, 278 m^2 - cautious, 283 m^2 - adaptive ($\tau = 0.3$), 267 m^2 - adaptive ($\tau = 0.5$) and 249 m^2 - adaptive ($\tau = 0.8$).

set to 10% of the capacity of the AWGN channel with the same average SNR. All nodes can transmit with power up to 10 dB, and the transmitter employs a fixed power $P_t = 3$ dB.

We consider the confined region $\mathcal{R} = [-8.5, 8.5]$ m $\times$ $[-8.5, 8.5]$ m, and a sampling interval for the locations of the eavesdropper of 0.18m. This results in 9025 samples of eavesdropper locations being considered for each system setup. The jamming coverage and efficiency thus provide a measure to assess the security benefits of a particular jammer configuration (location and transmit power), irrespectively of the location of the eavesdropper. To analyze the effect of different jamming configurations, for each strategy we select a sample of locations on a grid and, for each location, we consider 30 different levels of transmit power, from 10 dBm to 10 dB. From this set, we consider the optimal configurations of each strategy, i.e. the location and power of the jammer that, for a given strategy, leads to the largest coverage and efficiency. Using the optimal configurations, we compare the different jamming strategies under identical system conditions.

B. Jamming Coverage

First, we analyze the effect of different jamming configurations on coverage. The configurations maximizing coverage depend on the jamming strategy, but for all strategies, the largest coverage is achieved with low transmit power by the jammer. Moreover, since proximity to the legitimate receiver is harmful, all strategies lead to regions where placing the jammer provides maximum coverage in the upper part of the confined region. Figure 3(a) shows such region and the corresponding maximum coverage location for blunt jamming. Cautious jamming leads to a larger coverage than blunt jamming by using CSI to encompass locations in which the eavesdropper is further away. In the case of adaptive jamming, which is based solely on CSI for the channel to the legitimate receiver, the location and transmit power of the jammer can be adjusted to provide large coverage, albeit with a cost in terms of efficiency.

Figure 4 compares the different strategies with optimal coverage configurations. Namely, it depicts the area (y axis) over which a given strategy is able to achieve a ΔP_{out} above a certain value (x axis). The figure shows that although all strategies provide large coverage (the lowest being blunt jamming with a coverage of 197 m^2), only low values of ΔP_{out} are achieved and over small regions. For example, none of the strategies is able to reduce the secrecy outage by half ($\Delta P_{out} = 2$). This happens because the jammer employs low transmit power on these optimal configurations, thus resulting in little interference to eavesdroppers. As we will see with the optimal efficiency configurations, a controlled increase of the transmit power of the jammer can lead to higher ΔP_{out} values.

C. Jamming Efficiency

Locations where placing a jammer provides the largest efficiencies appear close to the source, yet tending towards the opposite direction of the main receiver, as illustrated in Figure 3(b) for the case of blunt jamming. This is natural, since it is close to the source that the secrecy outage probability is higher and, therefore, the jammer is able to provide highest security benefits. The harmful effect of the jammer when close to the receiver makes the region asymmetric with respect to the source. For the three strategies, the optimal configurations also result from the jammer employing higher transmit powers ($P_j = 10$ dB), whenever active, thus leading to increased interference to possible eavesdroppers.

Figure 5 compares the optimal efficiency configurations for the three strategies. As expected, blunt jamming provides the lowest coverage, but the highest efficiency. Cautious jamming leads to a smaller efficiency over large regions, and the operation of adaptive jamming can be adjusted with the typical coverage-efficiency trade-off. Notice that, apart from the advantage in efficiency, blunt jamming also leads to a much higher maximum ΔP_{out} value. In particular, this strategy is able to reduce the secrecy outage probability by at least one

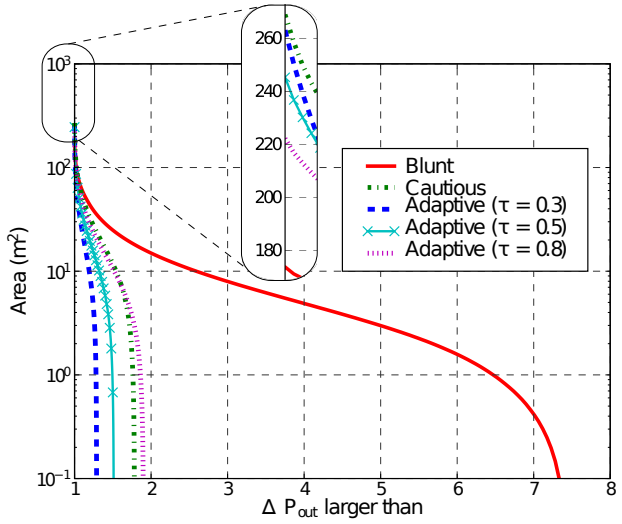


Fig. 5. Comparison between the three jamming strategies for the maximum efficiency configurations of the jammer. The plot shows the area of eavesdropper locations leading to a ΔP_{out} above a certain value (x axis). The zoomed area at $\Delta P_{out} = 1$ shows the coverage attained by each strategy, namely 174 m^2 - blunt, 271 m^2 - cautious, 264 m^2 - adaptive ($\tau = 0.3$), 246 m^2 - adaptive ($\tau = 0.5$) and 223 m^2 - adaptive ($\tau = 0.8$).

half ($\Delta P_{out} > 2$) in a region of 15 m^2. This shows that this strategy excels in terms of jamming efficiency.

D. Relevance of CSI

Irrespectively of the jamming strategy considered, the optimal configurations of the jammer favor a large distance to the receiver. In such cases, we have seen that CSI proves useful to provide large coverage, although it fails to provide desirable ΔP_{out} values, therefore resulting in low jamming efficiency. Although a precise analytical comparison of the jamming strategies seems beyond reach, it is possible to establish generic ordering results that confirms the effect of CSI and the inherent tradeoff between coverage and efficiency.

Proposition 4: Let $\mathcal{C}(\cdot)$ denote the coverage of a jamming strategy. The strategies satisfy the following coverage ordering:

$$\mathcal{C}(\text{Blunt}) = \mathcal{C}(\text{Adaptive with } \tau \to \infty) \leq \mathcal{C}(\text{Cautious}) \leq \mathcal{C}(\text{Adaptive with } \tau \to 0)$$

Proof: As $\tau \to \infty$, the probability that the jammer is active under adaptive jamming tends to 1. This limiting case is therefore equivalent to blunt jamming and $\mathcal{C}(\text{Blunt}) = \mathcal{C}(\text{Adaptive with } \tau \to \infty)$, which could also be verified by taking the limit $\tau \to \infty$ in Proposition 3.

Cautious jamming avoids situations in which jamming hurts the legitimate receiver more than the eavesdropper. Assume that the realization of the channel gains g_{tr} and g_{te} is such that $c_{tr}g_{tr} \geq c_{te}g_{te}$ so that there is no outage without jamming. Since a cautious jammer only jams if $c_{jr}g_{jr} \leq c_{je}g_{je}$, then

$$\frac{c_{tr}g_{tr}}{1 + c_{jr}g_{jr}} \geq \frac{c_{te}g_{te}}{1 + c_{je}g_{je}},$$

and there is no outage with cautious jamming either. Therefore, unlike blunt jamming, cautious jamming never creates an outage unless the system is already in outage without jamming. Consequently, the coverage of cautious jamming can only exceed that of blunt jamming and $\mathcal{C}(\text{Blunt}) \leq \mathcal{C}(\text{Cautious})$.

Finally, we show that as $\tau \to 0$, adaptive jamming achieves full coverage. In fact, the probability of outage with adaptive jamming and no jamming differ only in the term

$$P\left[\frac{c_{tr}G_{tr}}{1 + c_{jr}G_{jr}} < \frac{c_{te}G_{te}}{1 + c_{je}G_{je}} | G_{jr} < \tau\right],$$

which can be bounded as

$$\begin{aligned} & P\left[\frac{c_{tr}G_{tr}}{1 + c_{jr}G_{jr}} < \frac{c_{te}G_{te}}{1 + c_{je}G_{je}} | G_{jr} < \tau\right] \\ \leq\ & P\left[\frac{c_{tr}G_{tr}}{1 + c_{jr}\tau} < \frac{c_{te}G_{te}}{1 + c_{je}G_{je}} | G_{jr} < \tau\right] \\ \leq\ & P\left[c_{tr}G_{tr} < c_{te}G_{te}\right] \end{aligned}$$

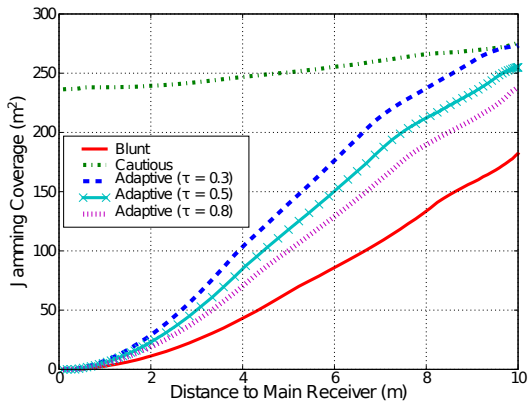
for τ small enough. Note that the last inequality only holds because of the fading term G_{te}. Therefore, $\mathcal{C}(\text{Adaptive with } \tau \to 0) = 100\%$ and $\mathcal{C}(\text{Cautious}) \leq \mathcal{C}(\text{Adaptive with } \tau \to 0)$. ■

Note that the only way to avoid harming the receiver more than the eavesdropper at all times would be to exploit the knowledge of CSI for all channels. Consequently, cautious and adaptive jamming, which do not exploit CSI for the channels from the transmitter to the receiver and the eavesdropper, are unable to detect all favorable jamming opportunities. This explains the lower values of ΔP_{out} and the resulting lower efficiencies achieved by these strategies.

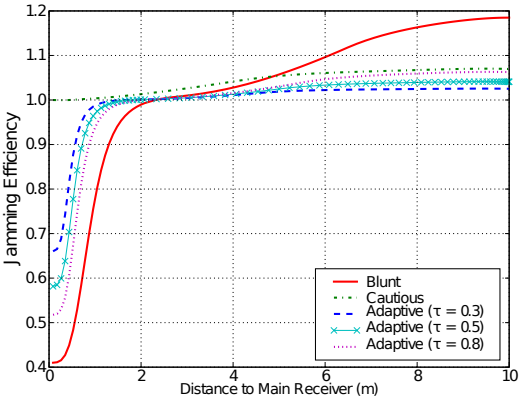
Even with partial information, the benefit of CSI becomes apparent when the jammer is closer to the legitimate receiver. Figure 6(a) illustrates the effect of increased distance between the jammer and the legitimate receiver on coverage. For all strategies, the coverage grows with increased distance. However, cautious jamming is able to sustain a large coverage even at small distances to the receiver. This happens because this strategy uses CSI to reduce the impact on the legitimate receiver. In terms of efficiency, Figure 6(b) shows that the conservative approach of cautious jamming again leads to better results at smaller distances. As distance increases, the impact of the jammer on the legitimate receiver is lower and the strategy of cautious jamming becomes less useful, eventually getting surpassed by a simpler approach such as blunt jamming. This result highlights once more the importance of CSI to improve secrecy, most notably in the vicinity of the legitimate receiver.

V. Multiple Jammers

None of the aforementioned strategies is capable of achieving high efficiency over large regions. Furthermore, the strategies that are capable to detect beneficial jamming opportunities require CSI that may not always be available. To overcome these difficulties, we now extend our analysis to more than one jammer. Specifically, we provide a characterization of the secrecy outage probability for the case of multiple blunt jammers and discuss the effect of having more jammers on the defined secrecy measures.



(a) Coverage vs Distance to Receiver



(b) Efficiency vs Distance to Receiver

Fig. 6. This figure shows the variation of the coverage (a) and the efficiency (b) measures according to the distance to the receiver for optimal power allocations of the jammer.

A. Secrecy Outage Probability for Multiple Blunt Jammers

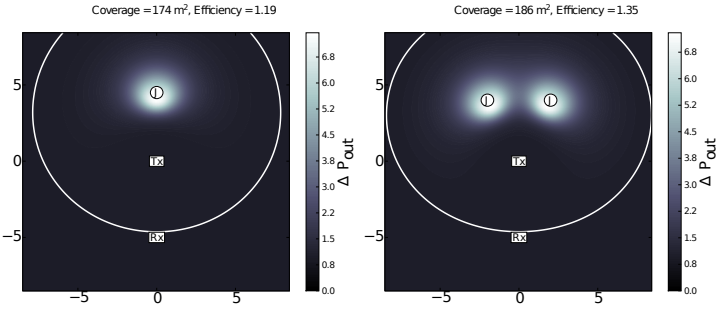
Proposition 5: Letting $\kappa = \dfrac{e^R - 1}{c_{tr}}$, $\beta = e^R \dfrac{c_{te}}{c_{tr}}$ and $\Omega(x) = e^x E_1(x)$, the secrecy outage probability for multiple blunt jammers is given by

$$P[C_s < R] = 1 - \frac{1}{\prod_j c_{jr}} \frac{1}{\prod_j c_{je}} \times \sum_j \sum_{j'} \frac{1}{\prod_{l \neq j} \left(\frac{1}{c_{lr}} - \frac{1}{c_{jr}}\right)} \frac{1}{\prod_{l \neq j'} \left(\frac{1}{c_{le}} - \frac{1}{c_{j'e}}\right)} I(j,j')\, e^{-\kappa}$$

with $I(j,j')$ given by

- Case 1: $\kappa + \dfrac{1}{c_{jr}} \neq \dfrac{\beta}{c_{j'e}}$

$$I(j,j') = \frac{c_{j'e}}{\left(\kappa + \frac{1}{c_{jr}}\right) - \frac{\beta}{c_{j'e}}} - \frac{1}{\left(\kappa + \frac{1}{c_{jr}} - \frac{\beta}{c_{j'e}}\right)^2} \times \left[\kappa + \frac{1}{c_{jr}} - \frac{\beta}{c_{j'e}} - \beta\right] \Omega\left[\left(\kappa + \frac{1}{c_{jr}}\right)\left(\frac{1+\beta}{\beta}\right)\right] - \frac{\beta}{\left(\kappa + \frac{1}{c_{jr}} - \frac{\beta}{c_{j'e}}\right)^2} \left[\kappa + \frac{1}{c_{jr}} - \frac{\beta}{c_{j'e}} + 1\right] \Omega\left(\frac{1+\beta}{c_{j'e}}\right)$$



(a) Single blunt jammer (b) Two blunt jammers

Fig. 7. This figure shows the impact of the maximum efficiency configurations for the single jammer and the case with two jammers, respectively in (a) and (b). The helpful interference region is delimited by the thick white line surrounding the jammers.

- Case 2: $\kappa + \dfrac{1}{c_{jr}} = \dfrac{\beta}{c_{j'e}}$

$$I(j,j') = -\frac{\beta}{\left(\kappa + \frac{1}{c_{j'r}}\right)} \left(1 - \frac{1+\beta}{c_{j'e}}\, \Omega\left(\frac{1+\beta}{c_{j'e}}\right)\right) + \frac{1}{2} \frac{1}{\left(\kappa + \frac{1}{c_{jr}}\right)} \frac{\beta}{\left(\kappa + \frac{1}{c_{jr}}\right)} \left(1 + \frac{1+\beta}{c_{j'e}} - \left(\frac{1+\beta}{c_{j'e}}\right)^2 \Omega\left(\frac{1+\beta}{c_{j'e}}\right)\right)$$

Proof: See Appendix C ■

B. Analysis

Let $\mathcal{S}$ be a set of active jammers. When $|\mathcal{S}| \gg 0$, the capacity of the receiver and eavesdropper channels are likely to decrease as a result of added interference. In the limit, we have $P[C_s < R_s] \to 1$, i.e. $\Delta\mathcal{P}_{out} \leq 1$ across the entire region. However, we shall see that two jammers and a proper allocation of power can lead to significant improvements.

For simplicity, we focus on configurations with only one or two jammers, and we distinguish between (a) a *regular* scenario with individual power constraints, and (b) a *fair* scenario in which the collective power sum of the jammers is, at most, the same as in the single jammer case, i.e. $\sum_j P_j \leq 10$W. Table I shows a comparison of the maximum coverage and maximum efficiency configurations, for one and two jammers.

1) Coverage: The maximum coverage configurations with two jammers are the same for the regular scenario and the fair scenario. This happens because these configurations operate at low jamming power and therefore, the results are not affected by the power sum restriction of the fair scenario. It is clear that multiple jammers offer some advantage over a single jammer, increasing the secrecy benefits both in terms of efficiency and coverage, as illustrated by Figure 7. Beyond these gains, multiple jammers also lead to the following benefits:

- The area where a jammer is useful without the need of CSI becomes larger. Specifically, the joint operation of the two jammers allows one of them to be located closer to the legitimate receiver, while still achieving significant coverage results;
- Higher transmit powers can be used by the jammers, thus yielding improved efficiency results.

TABLE I

COMPARISON BETWEEN CONFIGURATIONS LEADING TO MAXIMUM COVERAGE AND EFFICIENCY RESULTS FOR ONE AND TWO JAMMERS.

Configuration	# Jammers	Coverage (m^2)	Efficiency	P_j (W)
Maximum Coverage	1	197	1.0024	0.01
	2	229	1.0075	$[0.01, 0.01]$
	$2^\dagger$	229	1.0075	$[0.01, 0.01]$
Maximum Efficiency	1	174	1.19	10
	2	186	1.35	$[9.5, 9.5]$
	$2^\dagger$	157	1.21	$[0.5, 9.5]$

The case of two jammers considers the regular scenario as well as the fair scenario(†).

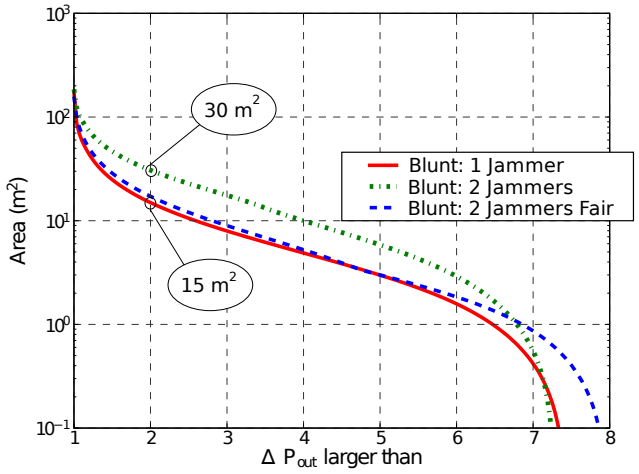


Fig. 8. Comparison between single and multiple blunt jammers for the maximum efficiency configurations of the jammer.

2) Efficiency: Since jamming efficiency increases with higher jamming power, the fair scenario prevents the two jammers from achieving their full potential; however, two jammers still provide higher efficiency than the single jammer. Removing the power sum restriction leads to further improvements and the two jammers outperform the single jammer, albeit at a cost in terms of energy expenditure. This is consistent with previous results, which show that a controlled increase in the transmit power of the jammers leads to improved efficiency results.

Figure 8 shows that along with these efficiency gains, the availability of more jammers greatly increases the area where a relevant ΔP_{out} is achieved. For example, the area in which the secrecy outage probability gets reduced by half ($\Delta P_{out} > 2$) goes from 15 m^2 with one jammer to 30 m^2 with two jammers. Besides, the availability of more jammers enlarges the area where placing a jammer is useful. The potential jammer positions that fail to provide security benefits occur close to the legitimate receiver. This is a consequence of the harmful effect of the interference of the jammer on the legitimate receiver, and can be dealt with by employing a more conservative strategy such as cautious jamming.

VI. CONCLUSIONS

Friendly jamming is a powerful tool to increase the secrecy of wireless systems. Our results show that high transmit power and proximity to the legitimate receiver can become harmful, but a proper selection of such parameters leads to significant secrecy gains. Moreover, there is an inherent trade-off between the coverage and efficiency achieved by the jammer, which is reflected on the different jamming strategies and their requirements in terms of CSI. As an example, blunt jamming without CSI provides the highest efficiency but fails to achieve large coverage. By using CSI of the impact of jamming on the legitimate receiver, adaptive jamming can be adjusted to provide large coverage yet paying a price in terms of efficiency. Cautious jamming highlights the usefulness of CSI by using full CSI about the impact of the jammer to improve on the results of the remaining strategies, specifically when close to the legitimate receiver. Unfortunately, a strategy able to determine every favorable opportunity to jam requires CSI for all channels, which may not always be available realistically. Our analysis of multiple jammers suggests that the key to achieve high coverage and high efficiency simultaneously lies in having more than one jammer.

Finally, we note that there is still much work to do in evaluating the secrecy potential of different spatial configurations. A natural extension to this work includes analyzing the behavior of other system parameters, such as the interplay between the secure communication rate R_s and the transmission power of the jammer P_j that guarantees a prescribed level of jamming efficiency.

Acknowledgements

The authors gratefully acknowledge useful discussions with Tiago T. V. Vinhoza and Rui A. Costa from Universidade do Porto, Portugal.

REFERENCES

[1] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *IEEE International Conference on Communications*, Cape Town, South Africa, May 2010.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, USA, July 2006, pp. 356–360.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[6] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proceedings of the 44th Annual Allerton Conference on Communication, Control, and Computing*. Monticello, IL, USA, September 2006.

[7] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

[9] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[10] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing*. Monticello, IL, USA, September 2007.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *IEEE International Symposium on Information Theory*. Toronto, Ontario, Canada, July 2008, pp. 524–528.

[12] S. Shafiee, N. Liu, and S. Ulukus, "Towards the Secrecy Capacity of the Gaussian MIMO Wiretap Channel: The 2-2-1 Channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, September 2009.

[13] M. Médard, "Capacity of Correlated Jamming Channels," in *Proceedings of the 35th Allerton Conference on Communication Control and Computing*. Monticello, IL, USA, 29 September - 1 October 1997, pp. 1043–1052.

[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[15] E. Tekin and A. Yener, "The General Gaussian Multiple-Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[16] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.

[17] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian Wiretap Channel with a Helping Interferer," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 389–393.

[18] X. He and A. Yener, "Providing Secrecy with Lattice Codes," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, September 2008, pp. 1199–1206.

[19] ——, "Cooperative Jamming: The Tale of Friendly Interference for Secrecy," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Springer, 2009, pp. 65–88.

[20] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, New Jersey, 1996.

[21] R. K. Mallik, M. Z. Win, J. W. Shao, M.-S. Alouini, and A. J. Goldsmith, "Channel capacity of adaptive transmission with maximal ratio combining in correlated Rayleigh fading," *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1124–1133, July 2004.

APPENDIX

A. Proof for Proposition 1

The secrecy outage probability is given by [4]

$$P[C_s < R] = P[C_r - C_e < R]$$

which, by using the definitions of Section II yields

$$P[C_s < R] = P\left[G_{tr} < \kappa(1 + c_{jr}G_{jr}) + \beta G_{te}\frac{1 + c_{jr}G_{jr}}{1 + c_{je}G_{je}}\right],$$

where $\kappa = \frac{e^R - 1}{c_{tr}}$ and $\beta = e^R \frac{c_{te}}{c_{tr}}$.

Let the pdfs of $\xi = g_{te}$, $\nu_1 = g_{jr}$ and $\nu_2 = g_{je}$ be $f(\xi)$, $h_m(\nu_1)$ and $h_e(\nu_2)$, respectively.

Since the pdf of g_{tr} is $f(x) = e^{-x}$, we get

$$P[C_s < R] = 1 - \iiint_0^\infty \exp\left(-\kappa(1 + c_{jr}\nu_1) - \beta\xi\frac{1 + c_{jr}\nu_1}{1 + c_{je}\nu_2}\right) \times f(\xi)\ h_m(\nu_1)\ h_e(\nu_2)\ d\xi\ d\nu_1\ d\nu_2$$

Proposition 1 then results through standard calculus.

B. Proof for Propositions 2 and 3

The proof for the secrecy outage probability for both cautious and adaptive jamming is similar to the proof for blunt jamming. The main difference comes from the fact that, instead of adjusting the transmit power according to the defined jamming scheme as mentioned in Section III-B, we equivalently adjust the fading distributions as follows.

Cautious jammer:

$$G'_{jr} = \begin{cases} G_{jr} & \text{if } \frac{G_{jr}}{d_{jr}^\alpha} < \frac{G_{je}}{d_{je}^\alpha} \\ 0 & \text{otherwise} \end{cases} \quad \Big| \quad G'_{je} = \begin{cases} G_{je} & \text{if } \frac{G_{jr}}{d_{jr}^\alpha} < \frac{G_{je}}{d_{je}^\alpha} \\ 0 & \text{otherwise} \end{cases}$$

Adaptive jammer:

$$G'_{jr} = \begin{cases} G_{jr} & \text{if } G_{jr} < \tau \\ 0 & \text{otherwise} \end{cases} \quad \Big| \quad G'_{je} = \begin{cases} G_{je} & \text{if } G_{jr} < \tau \\ 0 & \text{otherwise} \end{cases}$$

We then get the following joint pdf of $\nu_1 = g'_{jr}$ and $\nu_2 = g'_{je}$.

Cautious jammer:

$$h_{me}(\nu_1, \nu_2) = \begin{cases} 0 & \text{if } \nu_1 > \nu_2 \\ 0 & \text{if } \nu_1 > \delta\nu_2,\ \nu_1 \le \nu_2 \text{ and } \delta < 1 \\ e^{-\nu_1}e^{-\nu_2} & \text{if } \nu_1 \le \delta\nu_2,\ \nu_1 > 0 \text{ and } \delta < 1 \\ e^{-\nu_1}e^{-\nu_2} & \text{if } \nu_1 \le \nu_2,\ \nu_1 > 0 \text{ and } \delta > 1 \\ \frac{1}{1+\delta} & \text{if } \nu_1 = \nu_2 = 0 \text{ and } \delta < 1 \\ \frac{1}{2} & \text{if } \nu_1 = \nu_2 = 0 \text{ and } \delta > 1 \end{cases},$$

with $\delta = \left(\frac{d_{jr}}{d_{je}}\right)^\alpha$.

Adaptive jammer:

$$h_{me}(\nu_1, \nu_2) = \begin{cases} 0 & \text{if } \nu_1 > \tau \\ e^{-\nu_1}e^{-\nu_2} & \text{if } \nu_1 < \tau \quad \text{and } \nu_1 > 0 \\ e^{-\tau} & \text{if } \nu_1 = \nu_2 = 0 \end{cases}$$

By plugging $h_{me}(\nu_1, \nu_2)$ in the formulas of Section A we get,

$$P[C_s < R] = 1 - \iiint_0^\infty \exp\left(-\kappa(1 + c_{jr}\nu_1) - \beta\xi\frac{1 + c_{jr}\nu_1}{1 + c_{je}\nu_2}\right) \times f(\xi)\ h_{me}(\nu_1, \nu_2)\ d\xi\ d\nu_1\ d\nu_2$$

which leads to the final formulas for the secrecy outage probability presented in Proposition 2 and Proposition 3.

C. Proof for Proposition 5

Extending the results of Appendix A to multiple jammers yields

$$P[C_s < R] = P\left[G_{tr} < \kappa\left(1 + \sum_j c_{jr}G_{jr}\right) + \beta G_{te}\frac{1 + \sum_j c_{jr}G_{jr}}{1 + \sum_j c_{je}G_{je}}\right].$$

The pdf of $\nu_1 = \sum_j c_{jr}G_{jr}$ is given by [21]

$$h_m(\nu_1) = \frac{1}{\prod_j c_{jr}} \sum_j \frac{\exp\left(-\frac{\nu_1}{c_{jr}}\right)}{\prod_{l \ne j}\left(\frac{1}{c_{lr}} - \frac{1}{c_{jr}}\right)}.$$

Likewise, for $\nu_2 = \sum_j c_{je} G_{je}$,

$$h_e(\nu_2) = \frac{1}{\prod_j c_{je}} \sum_j \frac{\exp\left(-\frac{\nu_2}{c_{je}}\right)}{\prod_{l \neq j}\left(\frac{1}{c_{le}} - \frac{1}{c_{je}}\right)}.$$

Let the pdf of $\xi = g_{te}$ be $f(\xi) = e^{-\xi}$. Since the pdf of g_{tr} is given by e^{-x}, we have,

$$\begin{aligned} P[C_s < R] &= 1 - \iiint_0^\infty \exp\left(-\kappa(1 + c_{jr}\nu_1) - \beta\xi\frac{1 + c_{jr}\nu_1}{1 + c_{je}\nu_2}\right) \\ &\quad \times f(\xi)\ h_m(\nu_1)\ h_e(\nu_2)\ d\xi\ d\nu_1\ d\nu_2 \\ &= 1 - \frac{1}{\prod_j c_{jr}} \frac{1}{\prod_j c_{je}} \sum_j \sum_{j'} \frac{1}{\prod_{l \neq j}\left(\frac{1}{c_{lr}} - \frac{1}{c_{jr}}\right)} \frac{1}{\prod_{l \neq j'}\left(\frac{1}{c_{lr}} - \frac{1}{c_{j'm}}\right)} \times \\ &\iiint_0^\infty \exp\left(-\kappa(1 + c_{jr}\nu_1) - \beta\xi\frac{1 + c_{jr}\nu_1}{1 + c_{je}\nu_2}\right) e^{-\xi - \frac{\nu_1}{c_{jr}} - \frac{\nu_2}{c_{je}}} d\xi d\nu_1 d\nu_2. \end{aligned}$$

This finally leads to the results presented in Proposition 5.

João P. Vilela received his degree in Computer Science and Network Engineering in 2005 and the M.S. degree in Information Systems in 2007, both from University of Porto, Porto, Portugal. He is currently pursuing the Ph.D. degree in Computer Science in the same University and is also a researcher of Instituto de Telecomunicações in Porto, Portugal. His research interests include security and cooperation in wireless networks, wireless network models, protocol design and distributed systems. Mr Vilela was awarded a doctoral scholarship from the Portuguese Foundation for Science and Technology.

Matthieu Bloch received the Engineering degree from Supélec, Gif-sur-Yvettes, France, the M.S. degree in Electrical Engineering from the Georgia Institute of Technology, Atlanta, in 2003, the Ph.D. degree in Engineering Science from the Université de Franche-Comté, Besançon, France, in 2006, and the Ph.D. degree in Electrical Engineering from the Georgia Institute of Technology in 2008. In 2008-2009, he was a postdoctoral research associate at the University of Notre Dame, South Bend, IN, USA. Since July 2009, Dr. Bloch has been on the faculty of the School of Electrical and Computer Engineering at the Georgia Institute of Technology, where he is currently an Assistant Professor. His research interests are in the areas of information theory, error-control coding, wireless communications, and quantum cryptography. Dr. Bloch is a member of the IEEE and currently serves as the Chair of the Online Committee of the IEEE Information Theory Society. He is the Co-Chair of the ICC 2011 Workshop on Physical-Layer Security and the co-author of "Physical-Layer Security: From Information Theory to Security Engineering", which will be published by Cambridge University Press in July 2011.

João Barros is an Associate Professor of Electrical and Computer Engineering at the University of Porto and the head of the Instituto de Telecomunições in Porto, Portugal. Since 2008 he has also been a Visiting Professor with the Massachusetts Institute of Technology (MIT). In February 2009, Dr. Barros was appointed National Director of the CMU-Portugal Program, a five-year international partnership with a total budget of 56M Euros, which fosters collaborative research and advanced training among 12 Portuguese universities and research institutes, Carnegie Mellon University and more than 70 companies. In recent years, João Barros has published extensively in the fields of information theory, networking and security, with a special focus on network coding, physical-layer security, sensor networks, and intelligent transportation systems. He was the recipient of a best teaching award by the Bavarian State Ministry of Sciences, Research and the Arts and the winner of the 2010 IEEE Communications Society Young Researcher Award for the Europe, Middle East and Africa region. He received his undergraduate education in Electrical and Computer Engineering from the Universidade do Porto (UP), Portugal and Universitaet Karlsruhe, Germany, and the Ph.D. degree in Electrical Engineering and Information Technology from the Technische Universitaet Muenchen(TUM), Germany.

Steven W. McLaughlin received the B.S.E. E. degree from Northwestern University, the M.S.E. degree from Princeton University, and the Ph.D. degree from the University of Michigan. He joined the School of Electrical and Computer Engineering at Georgia Tech in September 1996 where is now Vice Provost for International Initiatives and Ken Byers Professor of ECE. As Vice Provost he is responsible for Georgia Tech's global engagement and is the point person for international initiatives in research, education, and economic development. He is also President of GT Global, Inc. a not-for-profit corporation recently created to manage select Georgia Tech international initiatives. He was previously Deputy Director of Georgia Tech - Lorraine - the European Campus of the Georgia Institute of Technology - in Metz, France from 2006-2007. He was President of the IEEE Information Theory Society in 2005. He has held positions at Booz, Allen and Hamilton, AT&T Bell Labs, and Eastman Kodak. From 1992-1996 he was on the Electrical Engineering faculty at the Rochester Institute of Technology. His research interests are in the general area of communications and information theory. His research group has on-going projects in the areas of turbo, LDPC, and constrained codes for magnetic and optical recording; FEC and equalization for wireless and optical networks; quantum key distribution, wireless and RFID security; and theory of error control coding. He has published more than 230 papers in journals and conferences and holds 28 US patents. He has served as the research and thesis advisor to more than 50 students at the bachelors, masters, doctoral and post-doctoral levels. He is a Fellow of the IEEE and served as an Associate Editor for Coding Techniques for the IEEE Transactions on Information Theory. He also served as the Publications Editor for that journal from 1995-1999.