This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings

Friendly Jamming for Wireless Secrecy

João P. Vilela*, Matthieu Bloch†§, João Barros‡, Steven W. McLaughlin†
*Instituto de Telecomunicações, Department of Computer Science, Universidade do Porto, Porto, Portugal.
Email: joaovilela@dcc.fc.up.pt
‡Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores
Faculdade de Engenharia da Universidade do Porto, Porto, Portugal.
Email: jbarros@fe.up.pt
§GT-CNRS UMI 2958, 2-3 rue Marconi, 57070 Metz, France
†§School of ECE, Georgia Institute of Technology Atlanta, Georgia 30332–0250
Email: {mbloch,swm}@ece.gatech.edu

***Abstract*—We analyze the role of jamming as a means to increase the security of wireless systems. Specifically, we characterize the impact of cooperative/friendly jamming on the secrecy outage probability of a quasi-static wiretap fading channel. We introduce *jamming coverage* and *jamming efficiency* as security metrics, and evaluate the performance of three different jamming strategies that rely on various levels of channel state information. The analysis provides insight for the design of optimal jamming configurations and indicates that one jammer is not enough to maximize both metrics simultaneously.**

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 [1] 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 known a growing interest, motivated in large part by applications to wireless communications.

A substantial body of work lays its foundation on the Gaussian wiretap channel [2], in which the channels linking the source to the legitimate receiver and to the eavesdropper 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 capacities of the aforementioned channels.

There are basically two solutions to increase the target secrecy rate: (a) improving the SNR of the legitimate receiver (e.g. by shortening the distance to the source) or (b) 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 [3]. However, jamming can be used to increase the noise level of the eavesdropper and ensure a higher secrecy capacity. This idea has already appeared in the literature under the name of artificial noise [4] or cooperative jamming [5].

Our work is different in that we consider fading channels (as opposed to the Gaussian case) and provide closed-form expressions for the secrecy outage probability. This measure is derived for several jamming strategies that rely on different levels of CSI knowledge. We also incorporate a simple path-loss model and introduce metrics that bestow a spatial interpretation of the impact of jamming in terms of secrecy.

Our main contributions are as follows:

- *Security metrics for jamming:* we introduce the jamming coverage and the jamming efficiency as security metrics;
- *Jamming strategies:* we provide a complete characterization of the secrecy outage probability for three jamming strategies that rely on various levels of channel state information (CSI);
- *Jamming configuration design:* based on the defined metrics, we evaluate the impact of different system configurations (transmission power and location of the jammer) on the performance of each jamming strategy.

The remainder of the paper is organized as follows. Section II, presents the system setup and introduces the secrecy outage probability and the associated metrics of jamming coverage and jamming efficiency. Section III extends the concept of secrecy outage probability to situations in which a friendly jammer is available. A characterization of different jamming strategies that rely on distinct CSI requirements is also provided. Section IV evaluates the effect of varying location and transmission power of the jammer on the performance of these strategies, and Section V concludes the paper.

II. Preliminaries

We consider the wireless system illustrated in Figure 1, in which a source communicates with a legitimate receiver while an illegitimate receiver, hereafter called the *eavesdropper*, overhears all transmissions. In addition, a node, hereafter called *jammer*, emits white Gaussian noise that causes interference to both the legitimate receiver and the eavesdropper. The source and jammer are subject to average power constraints

978-1-4244-6404-3/10/$26.00 ©2010 IEEE

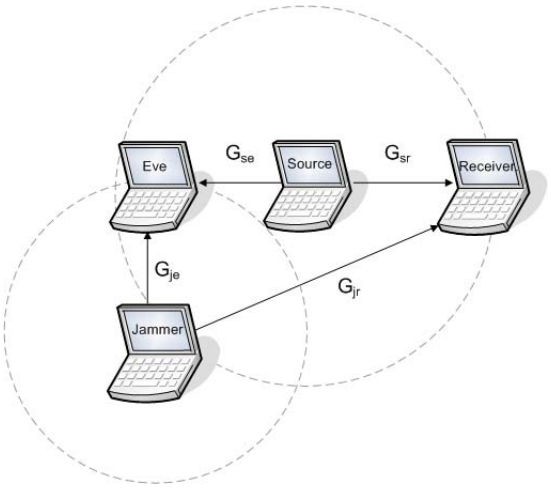

Fig. 1. Example of a wireless network where a source wants to communicate with a receiver and there is a potential eavesdropper (Eve) in vicinity. There is also a jammer, which can be used to interfere with communications.

P_s and P_j, respectively. Channels between all pair of nodes are modeled as independent quasi-static Rayleigh fading channels. Specifically, for each channel, fading coefficients remain constant during the transmission of an entire codeword but change randomly and independently from one codeword to another according to a 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. Letting N_0 represent the noise level, d_{jr} and d_{sr} denote the distances from the jammer to the receiver and from the source to the receiver, respectively, and introducing the constants $c_{jr} = \frac{P_j}{N_0}\frac{c}{d_{jr}^\alpha}$ and $c_{sr} = \frac{P_s}{N_0}\frac{c}{d_{sr}^\alpha}$, we have that the instantaneous signal-to-interference-plus-noise ratio (SINR) at the receiver can be represented by the random variable

$$\Gamma_r = \frac{c_{sr}G_{sr}}{1 + c_{jr}G_{jr}},$$

where G_{sr} and G_{jr} are independent exponential random variables with unit mean. Similarly, letting d_{je} and d_{se} denote the distances from the jammer to the eavesdropper and from the source to the eavesdropper, respectively, and introducing the constants $c_{je} = \frac{P_j}{N_0}\frac{c}{d_{je}^\alpha}$ and $c_{se} = \frac{P_s}{N_0}\frac{c}{d_{se}^\alpha}$, the instantaneous SINR at the eavesdropper is represented by the random variable

$$\Gamma_e = \frac{c_{se}G_{se}}{1 + c_{je}G_{je}},$$

where G_{se} 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 [2] of the channel between the source and the main receiver is given by

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

where $C_r = \log(1+\gamma_r)$ is the capacity of the main channel and $C_e = \log(1 + \gamma_e)$ denotes the capacity of the eavesdropper's channel. Because of fading, there is a non-zero probability that any specified secure rate is not achievable.

The use of secrecy outage as a security performance measure for wireless fading systems was proposed in [4], [6]; If the source and receiver target a secrecy rate R_s, the secrecy outage probability is given by

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

The operational meaning of this measure is twofold [7]. 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 source and receiver have no CSI about the eavesdropper. In this case, the source 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 given by $C_e' = C_r - R_s$. 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. Nevertheless, the interference created by the jammer can lead to smaller secrecy outage probability, even for situations where the eavesdropper is not far from the source or receiver.

A. Performance Metrics

We focus on the difference, $\Delta\text{P}_{\text{out}}$, between the secrecy outage probability without jamming (i.e. $P_j = 0$) and the secrecy outage probability with jamming. For each possible position of the eavesdropper (x_e, y_e), we define the *helpful interference region* as the area where $\Delta\text{P}_{\text{out}}(x_e, y_e) > 0$, and the *harmful interference region* as the area where $\Delta\text{P}_{\text{out}}(x_e, y_e) < 0$. We consider the following metrics.

- *jamming coverage*: the total area of the helpful interference region;
- *jamming efficiency*: the average change in outage probability because of jamming, i.e. the average $\Delta\text{P}_{\text{out}}(x_e, y_e)$ over all eavesdropper positions (x_e, y_e).

Depending on the security requirements, other metrics could be used. For example, the area over which the secrecy outage probability is below a certain threshold, captures the need for a low secrecy outage probability throughout the entire region. Our goal with the jamming coverage and jamming efficiency is to evaluate the overall benefit of jammer configurations (transmission power and location) in terms of secrecy. Optimal coverage configurations guarantee that the reduction of the secrecy outage probability occurs over a large region, although, this may happen with marginal outage reductions. The jamming efficiency complements this metric by favoring large reductions on the secrecy outage probability. The ultimate goal is, naturally, to achieve the most extensive jamming coverage while assuring the highest possible jamming efficiency.

III. Wireless Secrecy with Jamming

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 the jammer disregards any possible information about 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

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

with $\kappa = \dfrac{e^R - 1}{c_{sr}}$, $\beta = e^R \dfrac{c_{se}}{c_{sr}}$ and $\Omega(x) = e^x E_1(x)$ (see [8]).

Proof: See Appendix. ∎

The impact of jamming on the secrecy outage probability using this result is illustrated in Figure 2, where each point represents a potential location of the eavesdropper and shows the corresponding ΔP_{out} value. The helpful interference region, delimited by the thick white line around the jammer, is the area where the secrecy outage probability gets decreased. 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 0.33 to 0.04 (i.e. $\Delta P_{\text{out}} = 0.29$).

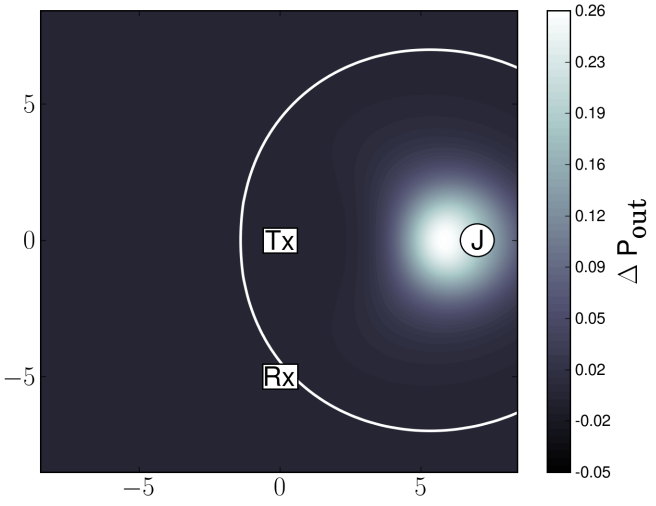

Fig. 2. Impact of blunt jamming on secrecy outage probability. For each position of the eavesdropper on the map, we compute ΔP_{out}. The locations of the source (Tx), receiver (Rx), and jammer (J) are (0,0), (0,-5), and (7,0), respectively. Secrecy outage probabilities are obtained for a target secrecy 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 helpful and harmful interference and the impact of CSI is crucial. Factors such as the received power and the distance, as well as the channel quality from the jammer to the communicating nodes and to a potential eavesdropper 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 to perform a cautious decision about when to jam. It jams whenever it finds the channel to the eavesdropper to be better than the one 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 cautious jammer is given by

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

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

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

Proof: See Appendix. ∎

2) Adaptive Jamming: The adaptive jammer only has CSI about the channel to the legitimate receiver. 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 possible 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

$$\begin{aligned} P\{C_s < R\} &= 1 - \frac{e^{-\tau}e^{-\kappa}}{1+\beta} \\ &- \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\xi - \Omega(\nu)(\mu-\xi) - \Omega(\mu\rho)(\mu-\xi)(\mu\rho-\nu-1)}{\xi^2(\mu-\xi)}\right) \\ &+ \frac{e^{-\kappa}\beta\, e^{-\mu c_{jr}\tau}}{c_{jr}c_{je}}\left(\frac{\xi - \Omega(\nu+\beta\frac{c_{jr}}{c_{je}}\tau)(\mu-\xi)}{\xi^2(\mu-\xi)}\right. \\ &\qquad \left. - \frac{\Omega(\mu\rho+\mu c_{jr}\tau)(\mu-\xi)(\mu\rho-\nu+\tau c_{jr}(\mu-\frac{\beta}{c_{je}})-1)}{\xi^2(\mu-\xi)}\right) \\ &+ \frac{e^{-\kappa}\beta}{c_{jr}c_{je}}\left(\frac{\Omega(\nu)-\Omega(\mu\rho)}{\xi}\right) \\ &- \frac{e^{-\kappa}\beta\, e^{-\mu c_{jr}\tau}(1+c_{jr}\tau)}{c_{jr}c_{je}}\left(\frac{\Omega(\nu+\beta\frac{c_{jr}}{c_{je}}\tau)-\Omega(\mu\rho+\mu c_{jr}\tau)}{\xi}\right) \end{aligned}$$

where κ, β and $\Omega(x)$ are defined as in Proposition 1, and ξ, ν, μ and ρ are defined as in Proposition 2.

Proof: See Appendix. ■

IV. Transmit Power and Location of the Jammer

Irrespective of the CSI available, the power and location of the jammer have a crucial impact on the security benefits of jamming. When $P_j \gg 0$, the capacity of both the main channel and the eavesdropper channel decrease and, in the limit, $P\{C_s < R_s\} \to 1$. Hence, high transmit power of the jammer becomes harmful in terms of security. Equivalently, setting the jammer close to the main receiver increases the interference to the main channel, leading to $C_r \to 0$ as $d_{jr} \to 0$. Since $C_e \geq 0$, we have $P\{C_s < R_s\} \to 1$. This confirms the intuition that having a jammer nearby the main receiver is harmful in terms of security.

Although the location and transmission power of the jammer can have an adverse effect on the security of the system, a careful selection of such parameters can still enhance security by causing controlled interference to the eavesdropper. The goal in this section is to analyze how different system configurations (location and transmission power of the jammer) affect the metrics of coverage and efficiency according to the employed jamming strategy.

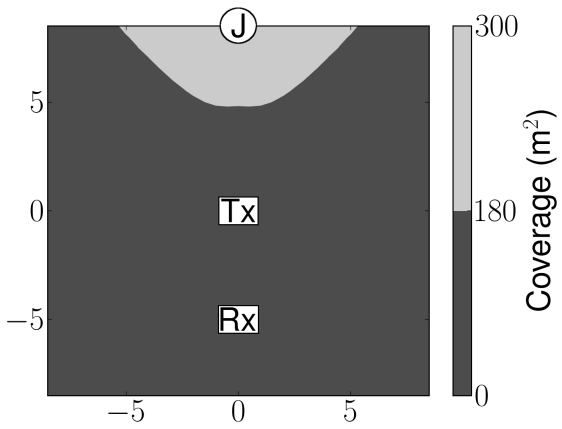

Fig. 3. This figure shows the optimal location for blunt jamming in terms of coverage (P_j = 10 dBm). The region where placing a jammer leads to a coverage above 180 m^2 is also depicted.

A. System Setup

We consider a scenario in which a source and receiver in an office building want to communicate secretly with the help of a jammer that aims to prevent an eavesdropper placed anywhere in a confined region in the vicinity of the communicating devices – where the secrecy outage probability is higher – from overhearing the transmissions. A path loss exponent of 4 is used, and the normalization constant c is set 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 [9]. The source and receiver are fixed at locations of $(0, 0)$ and $(0, -5)$, respectively, and aim to achieve a secure communication rate of 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 source transmits with a fixed power $P_s = 3$ dB.

An arbitrary location for the eavesdropper is assumed and the metrics of jamming coverage and efficiency are computed by considering the ΔP_{out} value for a large sample of eavesdropper locations. The jamming coverage and efficiency thus provide a measure to assess the security benefits of a particular jammer configuration, irrespectively of the location of the eavesdropper. To analyze the effect of different jamming configurations we select a sample of locations on a grid and, for each location, a set of 30 transmit powers is tested, ranging from 10 dBm to 10 dB. Under this restricted setting, we consider the optimal coverage and efficiency configurations. Although these optimal configurations do not necessarily hold for other system setups, they enable a comparison of the different jamming strategies.

B. Jamming Coverage

In this section, we analyze the effect of different jamming configurations on coverage. The optimal coverage configurations vary with the chosen jamming strategy. According to previous results that show that proximity to the main receiver is harmful, all strategies lead to optimal coverage regions in the upper part of the confined region. Figure 3 shows such region and the corresponding optimal location for blunt

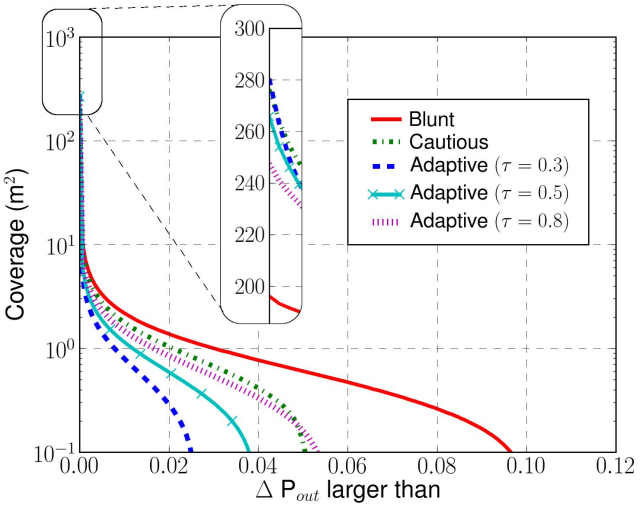

Fig. 4. Comparison between the three jamming strategies for a selected location in the optimal coverage region of Figure 3. The plot shows the area in which ΔP_{out} is above a certain value (x axis). The zoomed area at $\Delta P_{out} = 0$ shows the coverage attained by each strategy, namely 196 m^2 - blunt, 276 m^2 - cautious, 280 m^2 - adaptive ($\tau = 0.3$), 266 m^2 - adaptive ($\tau = 0.5$) and 248 m^2 - adaptive ($\tau = 0.8$).

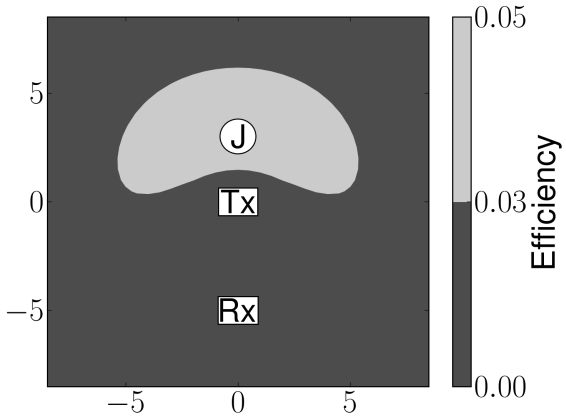

Fig. 5. This figure shows the optimal location for blunt jamming in terms of efficiency (P_j = 10 dB). The region where placing a jammer leads to an efficiency above 0.03 is also depicted.

jamming. Cautious jamming increases coverage by using CSI knowledge to encompass locations where the eavesdropper is further away. The secrecy gain is naturally lower there, thus leading to a decreased efficiency. The operation of adaptive jamming is based solely on CSI with respect to the main channel and can be adjusted to provide large coverage, yet with a cost in terms of efficiency as well.

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 (the x axis). For example, a cautious jammer is able to provide $\Delta P_{out} \geq 0.02$ over an area of $1m^2$. The figure shows that, although all strategies provide large coverage (the lowest being blunt jamming with a coverage of 213 m^2), the corresponding efficiencies are actually quite reduced – low values of ΔP_{out} are achieved. This happens because the jammer employs low transmit power on these optimal configurations, thus resulting in little interference to possible 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

In terms of efficiency, the optimal regions appear close to the source, yet tending towards the opposite direction of the main receiver, as illustrated in Figure 5 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 renders the region to become asymmetric with respect to the source and tending to the opposite direction of the receiver. 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.

Remark 1: 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 source 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.

Figure 6 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. This clearly shows that this strategy excels in terms of jamming efficiency. Since the optimal efficiency locations appear closer to the receiver than the optimal coverage locations, the use of CSI by cautious jamming provides a clearer advantage. Namely, it leads to a much larger coverage than blunt jamming and higher efficiency than adaptive jamming. The fact that cautious jamming overcomes any of the adaptive jamming strategies in terms of coverage as well, highlights the fact that the specific configurations of adaptive jamming are not suitable for every system setup.

Although the optimal efficiency configurations lead to smaller coverage than the optimal coverage configurations, it is clear that only the later configurations yield non-negligible security gains (e.g. for a coverage of 1 m^2 blunt jamming assures a ΔP_{out} above 0.03 for the optimal coverage configuration, against a ΔP_{out} above 0.73 for the optimal efficiency configuration). This is a natural consequence of employing higher transmit powers by the jammer.

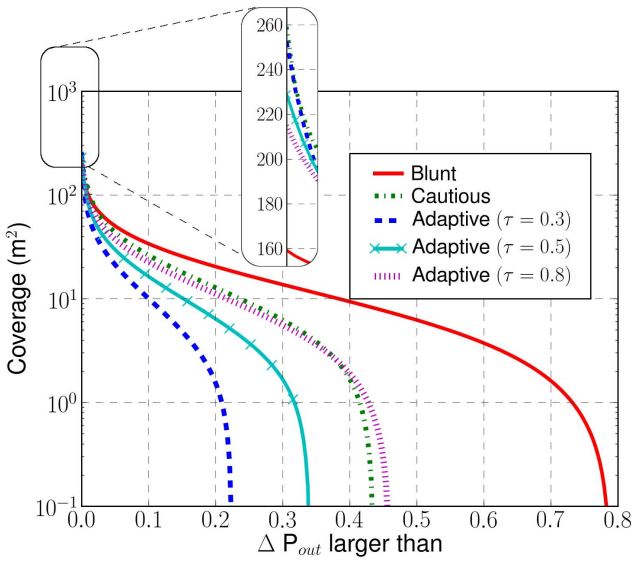

Fig. 6. Comparison between the three jamming strategies for the optimal configuration of the jammer with respect to jamming efficiency. The plot shows the area in which ΔP_{out} is above a certain value (x axis). The zoomed area at $\Delta P_{out} = 0$ shows the coverage attained by each strategy, namely 159 m^2 - blunt, 259 m^2 - cautious, 252 m^2 - adaptive ($\tau = 0.3$), 228 m^2 - adaptive ($\tau = 0.5$) and 214 m^2 - adaptive ($\tau = 0.8$).

V. Conclusions

We have seen that friendly jamming can be used as a powerful tool to increase the secrecy of wireless systems. Our results show that, although high transmit power and proximity to the legitimate receiver can become harmful, a proper selection of such parameters actually brings 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. For instance blunt jamming provides the highest efficiency results but fails to achieve large coverage. In contrast, adaptive jamming can be adjusted to result in large coverage yet paying a price in terms of efficiency. Cautious jamming exposes the usefulness of CSI. This reveals that having more than one jammer as well as relying on CSI knowledge actually becomes a necessity.

Appendix

A. Proof for Proposition 1

The secrecy outage probability is given by [6]

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

which, by using the definitions of Section II yields

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

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

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

Since the pdf of g_{sr} 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.

Proofs for Propositions 2 and 3 follow the same approach, yet with different pdfs for ν_1 and ν_2.

References

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

[2] 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.

[3] M. Médard, "Capacity of Correlated Jamming Channels," in *Proc. 35th Allerton Conference on Communication Control and Computing*. Monticello, IL, USA, 1997, pp. 1043–1052.

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

[5] 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.

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

[7] 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, 2008.

[8] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Table*. Courier Dover, 1965.

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