Jammer Selection Policies for Secure Wireless Networks

João P. Vilela*, Pedro C. Pinto‡, João Barros§
*Instituto de Telecomunicações, Departamento de Ciência de Computadores,
Faculdade de Ciências da Universidade do Porto, Porto, Portugal. Email: joaovilela@dcc.fc.up.pt
‡School of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne (EPFL),
Lausanne, CH-1015, Switzerland. Email: pedro.pinto@epfl.ch
§Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores
Faculdade de Engenharia da Universidade do Porto, Porto, Portugal. Email: jbarros@fe.up.pt

***Abstract*— We consider a wireless network scenario in which the communicating nodes are assisted by a number of jammers. The goal of the jammers is to obstruct potential eavesdroppers while restricting the harmful interference experienced by the legitimate receiver. Based on a stochastic network model, we are able to show that packet collisions caused by jamming nodes can be used effectively to increase the level of secrecy. Various jammer selection policies are investigated depending on the position of source, destination and jamming nodes. Our results show the benefit of jamming for secrecy when employing contention of jammers near the legitimate receivers.**

I. Introduction

It is well known that interference in wireless channels can be used effectively by cooperating nodes to improve the performance of wireless networks [1], [2]. However, when nodes are not cooperating, interference can lead to severe degradation of the received signals, which motivates a number of multiple access schemes to be implemented in real-life wireless networks. A common technique is the RTS/CTS (Request To Send/Clear To Send) handshake used in the IEEE 802.11 standard, which performs channel reservation before transmission to accomplish two goals: (1) reduce the likelihood of a collision by making neighbor nodes defer from channel access, and (2) reduce the cost of collisions by using control packets much smaller than the data packets. However, from a secrecy perspective some collisions may actually be useful. This is the case, for example, when a node causes a collision on an eavesdropper without harming the legitimate receiver.

A suitable metric to assess the secrecy level of a system is the secrecy capacity [3], i.e. the maximum transmission rate at which the source can communicate with the receiver without the eavesdropper being able to acquire any information. Several interference generation schemes have been proposed to improve the secrecy capacity of different types of wireless channels. A scheme for generation of artificial noise is proposed in [4] whereby a transmitter with multiple antennas or, alternatively, a set of amplifying relays introduce noise in the system that results in low outage probabilities of secrecy capacity. In [5], a cooperative jamming scheme is proposed in which an otherwise disadvantaged user can help improve the secrecy rate by jamming a nearby eavesdropper. [6] presents a set of cooperation strategies for a relay node to improve the achievable secrecy rate. Interference-assisted secret communication in which an interferer improves the secrecy rate by injecting independent interference is considered in [7]. Related literature on secrecy of multiple access channels without considering interference generation appears in [8]–[10].

In [11], the secrecy level of two nodes communicating in the presence of eavesdroppers placed anywhere in a confined region is investigated. Friendly jammers, with different levels of channel state information, help the legitimate parties by causing interference to possible eavesdroppers. Results shows that (i) jamming near the legitimate receiver leads to a small secrecy improvement and requires channel state information that may not always be available, and (ii) multiple jammers are needed to achieve relevant secrecy gains throughout the entire confined region. [12] looks at the secrecy of wireless networks with multiple eavesdroppers and provides insight on how it is affected by the spatial distribution of the eavesdroppers. It is shown that even a modest number of scattered eavesdroppers can dramatically reduce the achievable secrecy rates. Techniques to overcome this are proposed in [13].

Our work differs from the state-of-the-art in that we analyze the benefits of jamming on secure communications using Medium Access Control (MAC)-related parameters such as the density of jammers and eavesdroppers and the selection of active jammers. In particular, we make the following contributions:

- *secure throughput*: we propose and provide a characterization of the secure throughput as a metric to assess the secrecy level of a network;
- *jammer selection policies*: we devise a set of policies for selection of active jammers with the intent of improving the secure throughput;
- *performance analysis*: we analyse the performance of the aforementioned policies with varying power and density of jammers.

The rest of the paper is organized as follows. In Section II, we present the system model and the used notation. Section III presents the concept of secure throughput and provides a generic characterization. In Section IV, we propose a set of jammer selection policies. The secure throughput of each policy is also characterized. Section V validates the analytical results and presents a comparison of the different policies.

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.

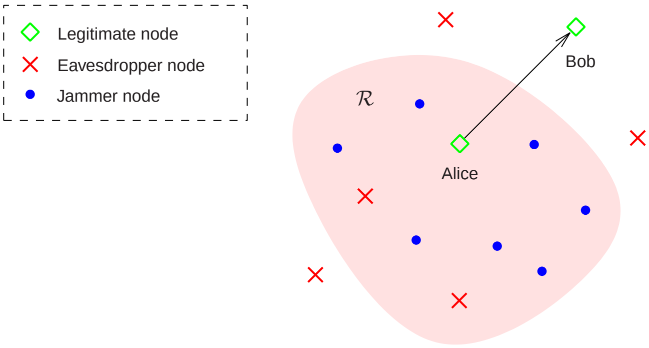


Fig. 1. Secure communication in the presence of eavesdroppers, assisted by jammers.

II. System Model

A. Node Configuration

We consider the scenario depicted in Fig. 1, where a legitimate user (Alice) wants to send messages to another user (Bob) with secrecy, i.e. without a set of eavesdroppers (Eve) having access to those messages. With the aim of improving the secrecy of such communication, multiple jammers transmit in cooperation with Alice and Bob. These jammers can arise in various scenarios: (i) they can be deployed by Alice and Bob with the single purpose of jamming potential eavesdroppers, or (ii) they can be legitimate nodes belonging to the same network as Alice and Bob, which transmit jamming signals during periods of communication inactivity. In terms of notation, Alice and Bob are located at $x_{\rm a}, x_{\rm b} \in \mathbb{R}^2$; the set of eavesdroppers is $\Pi_{\rm e} = \{e_i\} \subset \mathbb{R}^2$; and the set of jammers is $\Pi_\jmath = \{x_i\} \subset \mathcal{R}$, where $\mathcal{R} \subseteq \mathbb{R}^2$ is the *region of active jammers*. The transmit powers of Alice and the jammers are $P_{\rm a}$ and $P_\jmath$, respectively.

The spatial location of nodes can be modeled either deterministically or stochastically. In many cases, the node positions are unknown to the network designer a priori, so they may be treated as uniformly random according to a Poisson point process [14], [15]. Specifically, we consider that $\Pi_{\rm e}$ is an homogeneous Poisson point process (PPP) on $\mathbb{R}^2$ with density $\lambda_{\rm e}$, while $\Pi_\jmath$ is an homogeneous PPP restricted to region $\mathcal{R}$ with density $\lambda_\jmath$, independent of $\Pi_{\rm e}$.[1] The locations $x_{\rm a}, x_{\rm b}$ of Alice and Bob are deterministic.

We assume that the locations of the jammers and eavesdroppers are unknown. Although the jammers may not be silent, their location is still unknown in the sense that they can be regular nodes communicating in the network. The jammers and eavesdroppers can determine their connectivity to Alice and Bob if a proper signaling scheme is used before transmission (e.g. RTS/CTS). We also assume that neither the jammers nor the eavesdroppers collude, i.e. they only have access to their local information.

B. Wireless Propagation and Interference

To account for propagation in a wireless medium, we consider that the power $P_{\rm rx}$ received at a distance R from a source is given by $P_{\rm rx} = P/R^{2b}$, where P is the transmit power, and b is the amplitude loss exponent. To account for interference due to simultaneous transmissions, we use a model similar to [17], based on the notion of audible node.

Definition 1 (Audible Node [17]): A node x is *audible* to another node y if the power received by node y satisfies $P_{\rm rx} \geq P^*$, where P^* denotes some threshold (e.g., related to the sensitivity of y). Otherwise, node x is said to be *inaudible*.

We use $P_{\rm b}^*, P_{\rm e}^*$ to denote the sensitivities of Bob and the eavesdroppers, respectively. With respect to Fig. 1, let $x \to y$ denote the event of *successful reception* by node y (Bob or an eavesdropper) of the message sent by x (Alice or a jammer). We consider that the event $x \to y$ occurs iff two conditions are satisfied: i) node x is audible by y; and ii) there are no collisions between the packet transmitted by x and the packets transmitted by nodes that are audible to y. Similarly, let $x \nrightarrow y$ denote the event of *unsuccessful reception*, i.e., the complementary event of $x \to y$.

C. On Collisions

We define a collision on a node y to be the event of concurrent transmission of the source x with one or more nodes $\{z_i\}$ audible to y. We consider that the signals from $\{z_i\}$ become tangled together with the signal from x in a way that y is not able to correctly perceive it. From an analytical point of view, we consider that a collision happens if two or more nodes audible to y transmit. In this case, the transmit power of the source and the receiver sensitivity determines what is an audible node, and these parameters can be adjusted to encompass a wide range of scenarios. This implicitly assumes that the concurrent transmissions take place simultaneously or at least overlap long enough to make the receiver ignorant about their content.

III. Secure Throughput

A. Definition and Motivation

The *secrecy capacity* of a wireless link is the maximum transmission rate at which the source can communicate with the receiver without the eavesdropper being able to acquire any information. In several practical scenarios, it is desirable to have measures of secrecy that rely on simple link-layer parameters, much like the *throughput* of a link (defined as the probability of successful transmission) is a link-layer alternative to the *channel capacity* (defined as the maximum achievable rate). Based on the same principle, we introduce the notion of secure throughput.

Definition 2 (Secure Throughput): The secure throughput $\mathcal{T}_{\rm s}$ from Alice to Bob is the probability that a message transmitted by Alice is *successfully* received by Bob, and *unsuccessfully* received by every eavesdropper,[2]

$$\mathcal{T}_{\rm s} \triangleq \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \wedge \bigwedge_{e_i \in \Pi_{\rm e}} \mathrm{a} \nrightarrow e_i \right\}. \tag{1}$$

[1] In this paper, we assume for simplicity that the jammers transmit with probability $p = 1$. The case of arbitrary p can be easily accommodated replacing $\lambda_\jmath$ by $p\lambda_\jmath$, due to the splitting property of Poisson processes [16].

[2] In the above definition, the probability is implicitly conditioned on the event of Alice wishing to transmit, and Bob being silent and willing to receive. The malicious eavesdroppers are also assumed to be passive (i.e., silent at all times), as is often the case in practical scenarios.

TABLE I

Effect of interference from the jammers on the eavesdroppers and Bob and possible jammer selection policies with their respective regions.

Jammers Possibly Harm		Eavesdroppers	
		No	Yes
Bob	No	nojam: $\mathcal{R} = \emptyset$	jnrc: $\mathcal{R} = \mathcal{B}_{x_\text{a}}(r_{\text{a,e}}) \backslash \mathcal{B}_{x_\text{b}}(r_{\mathcal{J},\text{b}})$
	Yes	—	nsj: $\mathcal{R} = \mathcal{B}_{x_\text{a}}(r_{\text{a,e}})$ global: $\mathcal{R} = \mathbb{R}^2$

The secure throughput quantifies the secrecy of an uncoded link according to a collision-based MAC-layer model, depending only on simple parameters such as the spatial density of nodes and receiver sensitivities. This metric admits an outage interpretation. Since the node positions are typically slow varying (quasi-static), for a given realization of the point processes, the channel between a and b may not satisfy the condition $\text{a} \rightarrow \text{b} \wedge \bigwedge_{e_i \in \Pi_\text{e}} \text{a} \nrightarrow e_i$, in which case the system is said to be in outage.

B. Characterization of Secure Throughput

Define the following radiuses

$$r_{\mathcal{J},\text{b}} \triangleq \left(\frac{P_\mathcal{J}}{P_\text{b}^*}\right)^{1/2b}, \quad r_{\text{a,e}} \triangleq \left(\frac{P_\text{a}}{P_\text{e}^*}\right)^{1/2b}, \quad r_{\mathcal{J},\text{e}} \triangleq \left(\frac{P_\mathcal{J}}{P_\text{e}^*}\right)^{1/2b}.$$

With this notation, $\mathcal{B}_{x_\text{b}}(r_{\mathcal{J},\text{b}})$ is the ball inside which the jammers can interfere with Bob; $\mathcal{B}_{x_\text{a}}(r_{\text{a,e}})$ is the ball inside which the eavesdroppers can hear Alice; and $\mathcal{B}_x(r_{\mathcal{J},\text{e}})$ is the ball inside which the jammers can interfere with an eavesdropper located at x.

An exact expression for the secure throughput is in general hard to obtain. Appendix I shows that an *approximate* expression for the secure throughput is

$$\widetilde{\mathcal{T}}_\text{s} = \underbrace{\exp(-\mu_{\mathcal{J},\text{b}})}_{\widetilde{\mathcal{T}}_\text{b}} \times \underbrace{\exp\left(-\mu_{\text{a,e}} \cdot p_{\mathcal{J},\text{e}}\right)}_{1-\widetilde{\mathcal{T}}_\text{e}}, \qquad (2)$$

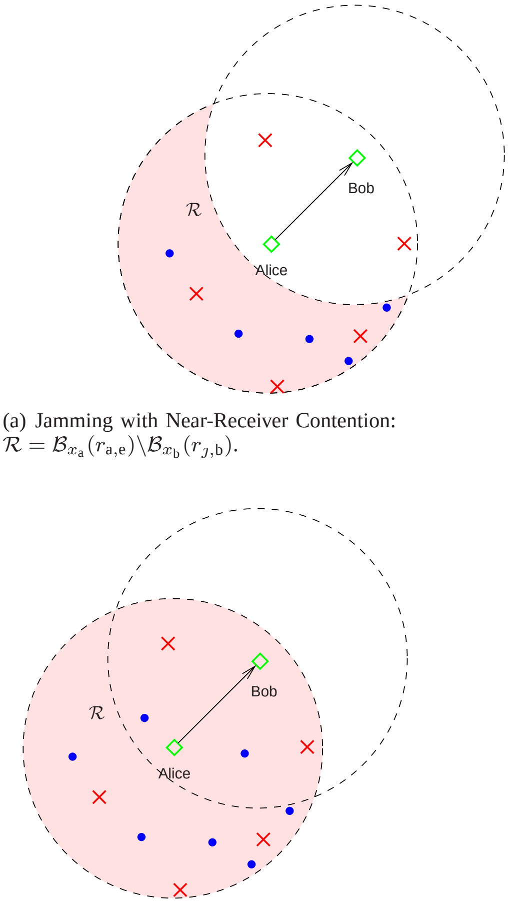
where the parameters are given by

$$\begin{aligned} \mu_{\mathcal{J},\text{b}} &= \lambda_\mathcal{J} \cdot \mathbb{A}\{\mathcal{B}_{x_\text{b}}(r_{\mathcal{J},\text{b}}) \cap \mathcal{R}\}, \\ \mu_{\text{a,e}} &= \lambda_\text{e} \cdot \pi r_{\text{a,e}}^2, \\ p_{\mathcal{J},\text{e}} &= \frac{1}{\pi r_{\text{a,e}}^2} \iint_{\mathcal{B}_{x_\text{a}}(r_{\text{a,e}})} \exp(-\mu_{\mathcal{J},x}) dx, \\ \mu_{\mathcal{J},x} &= \lambda_\mathcal{J} \cdot \mathbb{A}\{\mathcal{B}_x(r_{\mathcal{J},\text{e}}) \cap \mathcal{R}\}, \end{aligned}$$

where $\mathbb{A}\{\mathcal{R}\}$ is the area of a region $\mathcal{R}$. The left part of the expression corresponds to the throughput at Bob $\widetilde{\mathcal{T}}_\text{b}$, whereas the right part is one minus the throughput at Eve $\widetilde{\mathcal{T}}_\text{e}$. Later in the paper, we resort to simulations to confirm that (2) closely approximates the secure throughput.

IV. Jammer Selection Policies

Since Bob and the eavesdroppers must both lie in the audible region of Alice, in general there is a trade-off between the effect of interference from the jammers on Bob and the eavesdroppers. To analyze this trade-off, we propose a set of jammer selection policies in connection with the effect of the interference from the jammers, as summarized in Table I. We say that the jammers do not harm Bob if the region of active jammers excludes the area where jammers can harm Bob, $\mathcal{B}_{x_\text{b}}(r_{\mathcal{J},\text{b}})$. On the contrary, jammers can possibly harm the eavesdroppers if the region of active jammers contains part or all of the area where eavesdroppers can overhear from Alice, $\mathcal{B}_{x_\text{a}}(r_{\text{a,e}})$. The case in which jammers would harm Bob but not the eavesdroppers is not interesting from a security perspective and is not considered because the eavesdroppers can potentially share the same location as Bob.



(a) Jamming with Near-Receiver Contention: $\mathcal{R} = \mathcal{B}_{x_\text{a}}(r_{\text{a,e}}) \backslash \mathcal{B}_{x_\text{b}}(r_{\mathcal{J},\text{b}})$.

(b) Near-Source Jamming: $\mathcal{R} = \mathcal{B}_{x_\text{a}}(r_{\text{a,e}})$.

Fig. 2. Jammer selection policies. Jammers in the audible region of Alice are active in (a), whereas in (b) they are active if in the audible region of Alice and not audible to Bob.

In the following we characterize the policies of Table I and present the rationale behind them.

A. No Jamming

Although not relevant from a secrecy perspective, this is a simple reference policy for the case without jammers. In this case, no jammer is active, i.e. $\mathcal{R} = \emptyset$.

Proposition 1: The secure throughput for the *no jamming* (nojam) policy is given by

$$\widetilde{\mathcal{T}}_\text{s}^\text{nojam} = \exp\left(-\lambda_\text{e} \cdot \pi r_{\text{a,e}}^2\right).$$

Proof: This results from the general expression for the secure throughput in (2) with the parameters for $\mathcal{R} = \emptyset$

becoming $\mu_{\jmath,\mathrm{b}} = 0$, $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \cdot \pi r_{\mathrm{a,e}}^2$, $\mu_{\jmath,x} = 0$, and $p_{\jmath,\mathrm{e}} = 1$. ∎

This expression gives the exact secure throughput, because without jammers there are no dependencies between collisions on the eavesdroppers and Bob.

B. Global Jamming

In contrast with the previous, this policy corresponds to the case in which all jammers are active and the region of active jammers is $\mathcal{R} = \mathbb{R}^2$. Collisions may happen both on Bob as well as on the eavesdroppers.

Proposition 2: The secure throughput for the *global jamming* policy is given by

$$\widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{global}} = \exp(-\lambda_\jmath \pi r_{\jmath,\mathrm{b}}^2) \times \exp\left(-\lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2 \cdot \exp(-\lambda_\jmath \pi r_{\jmath,\mathrm{e}}^2)\right).$$

Proof: This results from the general expression for the secure throughput in (2) with the parameters for $\mathcal{R} = \mathbb{R}^2$ becoming $\mu_{\jmath,\mathrm{b}} = \lambda_\jmath \cdot \pi r_{\jmath,\mathrm{b}}^2$, $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \cdot \pi r_{\mathrm{a,e}}^2$, $\mu_{\jmath,x} = \lambda_\jmath \cdot \pi r_{\jmath,\mathrm{e}}^2 \ \forall x$, and $p_{\jmath,\mathrm{e}} = \exp(-\lambda_\jmath \cdot \pi r_{\jmath,\mathrm{e}}^2)$. ∎

C. Jamming with Near-Receiver Contention

This is a more conservative policy that aims to cause interference on eavesdroppers but reduce the interference caused to Bob by deactivating jammers audible to Bob. In such case, the region of active jammers becomes $\mathcal{R} = \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \backslash \mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}})$, as illustrated by *Figure 2(a)*. This should reduce the number of collisions on Bob but also on some eavesdroppers.

Proposition 3: The secure throughput for the *jamming with near-receiver contention* (jnrc) policy is given by

$$\widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{jnrc}} = \exp\left(-\lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2 \cdot p_{\jmath,\mathrm{e}}\right), \tag{3}$$

where

$$p_{\jmath,\mathrm{e}} = \frac{1}{\pi r_{\mathrm{a,e}}^2} \iint_{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})} \exp(-\mu_{\jmath,x}) dx,$$
$$\mu_{\jmath,x} = \lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_x(r_{\jmath,\mathrm{e}}) \cap \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \backslash \mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}})\}.$$

Proof: This results from the general expression for the secure throughput in (2) with the parameters for $\mathcal{R} = \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \backslash \mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}})$ becoming $\mu_{\jmath,\mathrm{b}} = 0$ and $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2$. ∎

D. Near-Source Jamming

This corresponds to a more aggressive policy that aims to cause as much interference as possible to all receiving eavesdroppers by having active jammers in the audible region of the source, without concerns with respect to Bob. The region of active jammers depicted in *Figure 2(b)* is then $\mathcal{R} = \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})$.

Proposition 4: The secure throughput for the *near-source jamming* (nsj) policy is given by

$$\begin{aligned} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nsj}} &= \exp\left(-\lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})\}\right) \\ &\quad \times \exp\left(-\lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2 \cdot p_{\jmath,\mathrm{e}}\right), \end{aligned}$$

where

$$p_{\jmath,\mathrm{e}} = \frac{1}{\pi r_{\mathrm{a,e}}^2} \iint_{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})} \exp(-\mu_{\jmath,x}) dx,$$
$$\mu_{\jmath,x} = \lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_x(r_{\jmath,\mathrm{e}}) \cap \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})\}.$$

Proof: This results from the general expression for the secure throughput in (2) with the parameters for $\mathcal{R} = \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})$ becoming $\mu_{\jmath,\mathrm{b}} = \lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})\}$ and $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2$. ∎

Proposition 5 (Asymptotic ordering of policies): In the limit of large transmission power and density of jammers, the secure throughput of the aforementioned policies satisfies the following ordering

$$\begin{aligned} \lim_{\lambda_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{global}} &= \lim_{\lambda_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nsj}} < \lim_{\lambda_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nojam}} \le \lim_{\lambda_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{jnrc}}, \\ \lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{global}} &< \lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nsj}} < \lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{jnrc}} = \lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nojam}}. \end{aligned}$$

Proof: The secure throughput of no jamming does not depend on the jammer parameters and is given by $\widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nojam}} = \exp(-\lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2)$. The secure throughput of jamming with near-receiver contention is always greater or equal to the previous because $p_{\jmath,\mathrm{e}} \le 1$ in (3). In the limit of large density of jammers, the secure throughput of the remaining policies becomes

$$\lim_{\lambda_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{global}} = \lim_{\lambda_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nsj}} = 0.$$

Asymptotic on $P_\jmath$, the secure throughput of the policies becomes

$$\lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{global}} = 0, \quad \lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{jnrc}} = \exp(-\lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2), \text{ and}$$

$$\lim_{P_\jmath \to \infty} \widetilde{\mathcal{T}}_{\mathrm{s}}^{\mathrm{nsj}} = \exp(-\lambda_\jmath \pi r_{\mathrm{a,e}}^2) \times \exp(-\lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2 \cdot \exp(-\lambda_\jmath \pi r_{\mathrm{a,e}}^2)).$$

The strict inequalities hold for finite $\lambda_{\mathrm{e}} > 0$. ∎

This shows that improving the secure throughput requires the transmit power of the jammers to be contained, otherwise no policy will overcome the reference policy without jammers. Also, policies allowing jammers near the legitimate receiver (such as global jamming and near-source jamming) fail to scale with density of jammers.

V. Discussion

We now compare the analytical approximation for the secure throughput in (2) with the simulated values obtained by Monte Carlo experiments for various system parameters. We consider a setup such as shown in *Figure 3*, where Alice and Bob are placed respectively at locations $(0, 0)$ and $(1, 1)$ of a region $\mathcal{S} = [-5, 5]\mathrm{m} \times [-5, 5]\mathrm{m}$ with area $A = 100$ m^2. We also place $\Pi_\jmath\{\mathcal{S}\} \sim \mathcal{P}(\lambda_\jmath A)$ jammers and $\Pi_{\mathrm{e}}\{\mathcal{S}\} \sim \mathcal{P}(\lambda_{\mathrm{e}} A)$ eavesdroppers uniformly and independently on $\mathcal{S}$, and the connectivity between nodes is assessed based on their relative distances as described in Section II-B. This information is then used to calculate the probabilities of interest over an ensemble of $20,000$ spatial realizations.

Figure 4 shows the secure throughput of the global jamming for varying density of jammers. The plot shows that the analytical secure throughput approximates the simulated values for a wide range of parameters. We observed that for all policies the approximation is not tight only for a combination of large λ_{e} and $P_\jmath$ values, since the independence approximations of Appendix I do not hold.

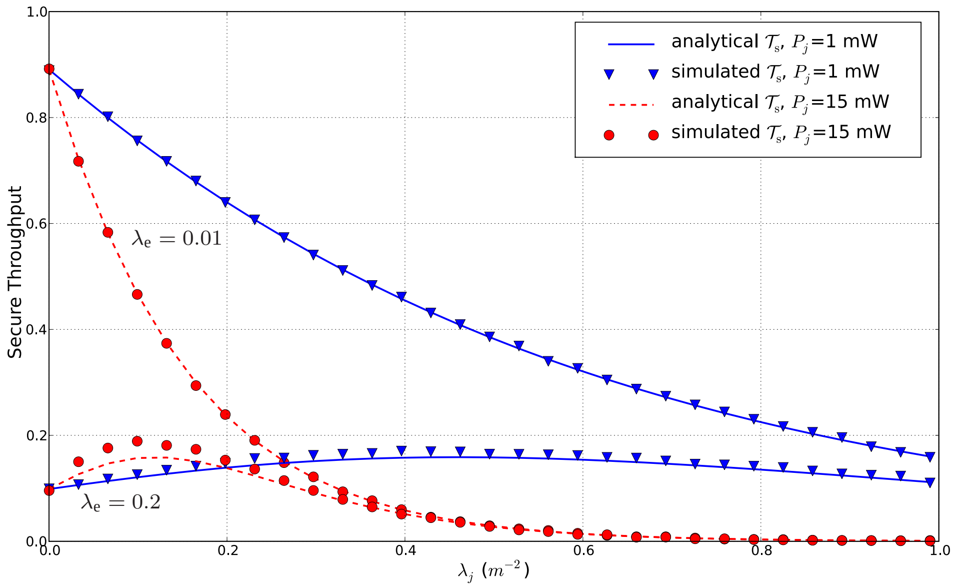


Fig. 4. Global Jamming: analytical vs simulated results.

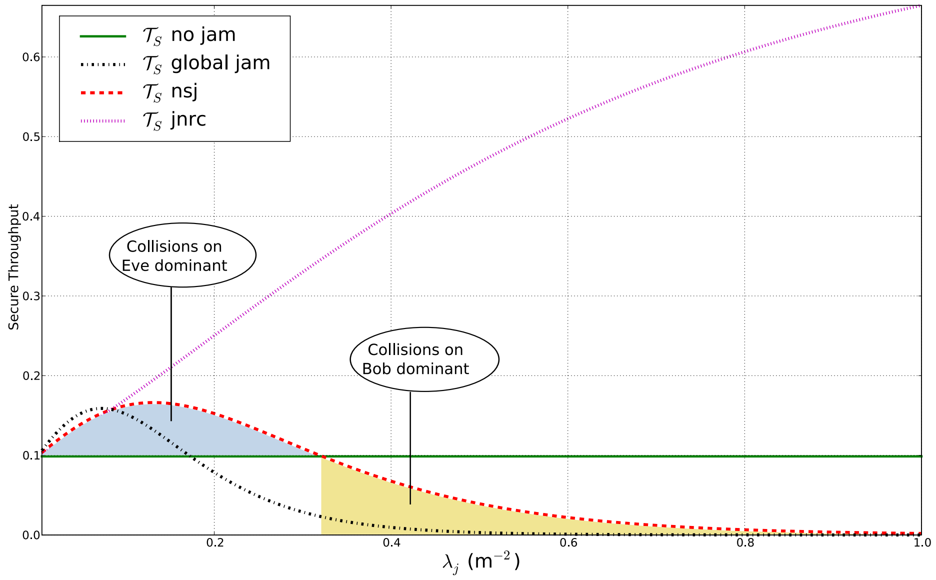


Fig. 5. Comparison of policies for varying $\lambda_\jmath$ ($P_\mathrm{a} = 40\mathrm{mW}$, $P_\jmath = 40\mathrm{mW}$, $\lambda_\mathrm{e} = 0.2\mathrm{m}^{-2}$).

A. *Comparison of Policies*

Figure 5 compares the different policies for varying density of jammers. Notice that these results comply with the ordering of policies in *Proposition 5*. Since there are no jammers in the system, the secure throughput of no jamming is steady for all $\lambda_\jmath$ values and serves mainly as a reference value. Global jamming and near-source jamming both exhibit a similar behavior, depending on λ_e:

1) for large λ_e, the secure throughput gets improved with increasing $\lambda_\jmath$, up to a cross-over value after which collisions on Bob become dominant and the secure throughput worsens (as illustrated in *Figure 5*). Near-source jamming leads to a larger cross-over value because there are less jammers audible to Bob;
2) for smaller λ_e, the secure throughput of global jamming and near-source jamming decreases for all values of $\lambda_\jmath$ (as illustrated for global jamming with $\lambda_\mathrm{e} = 0.01$ in *Figure 4*). This happens because the expected number of eavesdroppers is low and, therefore, collisions on Bob are dominant for all $\lambda_\jmath$ values.

As expected, jamming with near-receiver contention scales well with increasing $\lambda_\jmath$, because there are no jammers audible to Bob. Actually, only this policy is immune to variations in λ_e and consistently leads to improved secure throughput.

This shows that jamming can be used as a tool to increase the secure throughput. However, contention of jammers near the legitimate receiver is needed for relevant secrecy gains, specially for systems with large number of jammer nodes.

Appendix I
Derivation of (2)

Let $x \rightarrow y$ denote the event of successful transmission from node x to y, and $x \nrightarrow y$ denote the event of unsuccessful

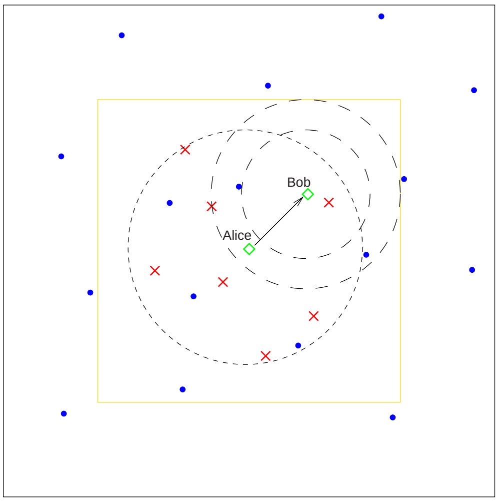


Fig. 3. Setup for Monte Carlo experiments: Alice and Bob are located respectively at the positions $(0,0)$ and $(1,1)$ of an inner region (highlighted) of a $\mathcal{S} = 10\mathrm{m}\times 10\mathrm{m}$ square. This prevents border effects on Alice and Bob. Alice transmits with power $P_\mathrm{a} = 40\mathrm{mW}$ and the 2 circles around Bob correspond to the regions where a jammer is audible for 2 different values of $P_\jmath = [1, 15]\mathrm{mW}$. The jammers and eavesdroppers are placed uniformly and independently on $\mathcal{S}$.

transmission. Let $\mathcal{E} \triangleq \Pi_\mathrm{e} \cap \mathcal{B}_{x_\mathrm{a}}(r_\mathrm{a,e})$ denote the random set of eavesdroppers that can hear Alice, and $N_\mathrm{a,e} \triangleq \#\mathcal{E}$. From the definition of secure throughput, we can write

$$\begin{aligned}\mathcal{T}_\mathrm{s} &= \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \wedge \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &= \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \middle| \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \times \mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &= \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \middle| \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &\quad \times \sum_{n=0}^{\infty} \mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \middle| N_\mathrm{a,e} = n \right\} \cdot \mathbb{P}\{N_\mathrm{a,e} = n\}, \qquad (4)\end{aligned}$$

We now make two approximations whose validity we evaluate in Section V: i) the event $\{\mathrm{a} \to \mathrm{b}\}$ is independent of $\{\bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i\}$; and ii) the events $\{\mathrm{a} \nrightarrow e_i | N_\mathrm{a,e} = n\}$ are independent identically distributed (IID) for different i. Then, (4) becomes

$$\widetilde{\mathcal{T}}_\mathrm{s} = \mathbb{P}\{\mathrm{a} \to \mathrm{b}\} \times \sum_{n=0}^{\infty} (1 - p_{\jmath,\mathrm{e}})^n \cdot \mathbb{P}\{N_\mathrm{a,e} = n\} \qquad (5)$$

where $p_{\jmath,\mathrm{e}} \triangleq \mathbb{P}\{\mathrm{a} \to e_i |\, N_\mathrm{a,e} = n\}$. To determine $\mathbb{P}\{\mathrm{a} \to \mathrm{b}\}$, note that from all the jammers inside region $\mathcal{R}$, Bob can only hear those falling inside $\mathcal{B}_{x_\mathrm{b}}(r_{\jmath,\mathrm{b}})$, whose number is a Poisson RV with mean $\mu_{\jmath,\mathrm{b}} = \lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_{x_\mathrm{b}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{R}\}$. Then,

$$\begin{aligned}\mathbb{P}\{\mathrm{a} \to \mathrm{b}\} &= \mathbb{P}\{\text{no jammers in } \mathcal{B}_{x_\mathrm{b}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{R}\} \\ &= \exp(-\mu_{\jmath,\mathrm{b}}).\end{aligned}$$

To determine the summation in (5), note that $N_\mathrm{a,e}$ is a Poisson RV with mean $\mu_\mathrm{a,e} = \lambda_\mathrm{e} \cdot \pi r_\mathrm{a,e}^2$, so from [17, Appendix A] we have

$$\sum_{n=0}^{\infty} (1 - p_{\jmath,\mathrm{e}})^n \cdot \mathbb{P}\{N_\mathrm{a,e} = n\} = \exp\left(-\mu_\mathrm{a,e} \cdot p_{\jmath,\mathrm{e}}\right).$$

We now determine $p_{\jmath,\mathrm{e}}$. Let $N_\jmath$ denote the (random) number of jammers that are audible by e_i. Conditional on the location $e_i = x$, the RV $N_\jmath$ is Poisson with mean $\mu_{\jmath,x} = \lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_x(r_{\jmath,\mathrm{e}}) \cap \mathcal{R}\}$. Also, conditional on $N_\mathrm{a,e}$, the location e_i has a uniform PDF over the ball $\mathcal{B}_{x_\mathrm{a}}(r_\mathrm{a,e})$. Using these two facts, we write

$$\begin{aligned}p_{\jmath,\mathrm{e}} &= \mathbb{E}_{e_i}\{p_{\jmath,\mathrm{e}} | e_i\} \\ &= \mathbb{E}_{e_i}\{\mathbb{P}\{N_\jmath = 0 | N_\mathrm{a,e}, e_i\}\} \\ &= \frac{1}{\pi r_\mathrm{a,e}^2} \iint_{\mathcal{B}_{x_\mathrm{a}}(r_\mathrm{a,e})} \exp(-\mu_{\jmath,x}) dx.\end{aligned}$$

This concludes the proof.

References

[1] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity—Part I: System description," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1938, 2003.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

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

[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] 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, 2008.

[7] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference-assisted secret communication," in *IEEE Information Theory Workshop (ITW)*, Porto, Portugal, 2008, pp. 164–168.

[8] R. Liu, I. Maric, R. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *IEEE International Symposium on Information Theory*, Seattle, WA, USA, July 2006.

[9] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[10] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[11] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless Secrecy Regions with Friendly Jamming," *submitted for publication*.

[12] P. Pinto, J. Barros, and M. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," in *Proc. of the 2009 IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, 2009, pp. 2442–2446.

[13] ——, "Techniques for Enhanced Physical-Layer Security," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Miami, FL, USA, December 2010.

[14] J. Kingman, *Poisson Processes*. Oxford University Press, 1993.

[15] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029–1046, 2009.

[16] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability*. Athena Scientific, 2008.

[17] P. Pinto and M. Win, "A unified analysis of connectivity and throughput in packet radio networks," in *IEEE Military Communications Conference, 2008. MILCOM 2008*, San Diego, California, November 2008, pp. 1–7.