Position-based Jamming for Enhanced Wireless Secrecy

João P. Vilela, Pedro C. Pinto, João Barros

Abstract— **Signal interference and packet collisions are typically viewed as negative factors that hinder wireless communication networks. When security is the primary concern, signal interference may actually be very helpful. Starting with a stochastic network model, we are able to show that packet collisions caused by jamming nodes can indeed be used effectively to attain new levels of secrecy in multi-terminal wireless environments. To this effect, we propose a practical jamming protocol that uses the well-known RTS/CTS (Request to Send/Clear to Send) handshake of the IEEE 802.11 standard as a signaling scheme. Various jammer selection strategies are investigated depending on the position of source, destination and jamming nodes. The goal is to cause as much interference as possible to eavesdroppers that are located in unknown positions, while limiting the interference observed by the legitimate receiver. To evaluate the performance of each strategy, we introduce and compute a measure for the secure throughput. Our results show that jamming can increase the levels of secrecy significantly albeit at a substantial cost in terms of energy efficiency.**

I. Introduction

The broadcast nature of wireless networks enables devices to overhear communications that are not intended to them. This paves the way to new forms of cooperation [1], [2] for improved performance of wireless networks, but it is also an issue in terms of communication (due to collisions) and confidentiality (due to eavesdroppers). The severe degradation that collisions can cause on wireless networks has led to a substantial body of literature that focuses on reducing their frequency, and several schemes have been proposed. The most well-known is the RTS/CTS 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.

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.

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.
Pedro C. Pinto (pedro.pinto@epfl.ch) is with the School of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne (EPFL), Lausanne, CH-1015, Switzerland.
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.

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 previous in that we analyze the benefits of jamming on secure communications according to Medium Access Control (MAC)-related parameters such as the density of jammers and eavesdroppers and the choice 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 level of secrecy of a network;
- *jammer selection strategies*: we devise a set of jammer selection strategies to improve the secure throughput;
- *practical jamming protocol*: we propose and evaluate a practical jamming protocol to employ the aforementioned strategies.

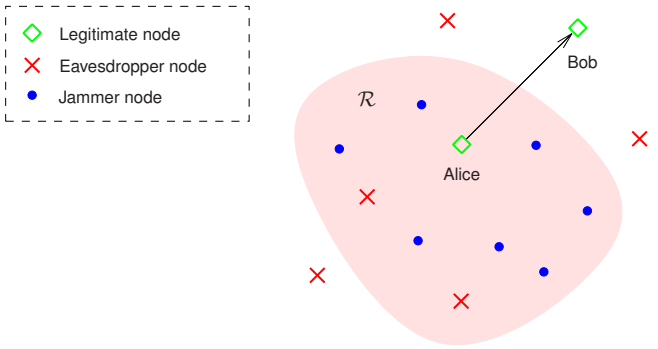


Fig. 1: Secure communication in the presence of eavesdroppers, assisted by jammers.

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 strategies. The secure throughput of each strategy is also characterized. Section V validates the analytical results and presents a comparison of the different strategies. A practical jamming protocol to implement those strategies is presented and evaluated in Section VI, and Section VII concludes the paper.

II. System model

We start by describing our system model. The notation and symbols used throughout the paper are summarized in Table III.

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 $x_{\mathrm{a}}, x_{\mathrm{b}} \in \mathbb{R}^2$; the set of eavesdroppers is $\Pi_{\mathrm{e}} = \{e_i\} \subset \mathbb{R}^2$; 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_{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 Π_{e} is an homogeneous Poisson point process (PPP) on $\mathbb{R}^2$ with density λ_{e}, while $\Pi_{\jmath}$ is an homogeneous PPP restricted to region $\mathcal{R}$ with density $\lambda_{\jmath}$, independent of Π_{e}.[1] The locations $x_{\mathrm{a}}, x_{\mathrm{b}}$ 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_{rx} received at a distance R from a source is given by $P_{\mathrm{rx}} = P/R^{2b}$, 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 $P_{\mathrm{rx}} \geq P^*$, where P^* denotes some threshold (e.g., related to the sensitivity of y). Otherwise, node x is said to be *inaudible*.

We use $P_{\mathrm{b}}^*, P_{\mathrm{e}}^*$ 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.

Due to the inherent variance of wireless communications signals (e.g. because of aspects such as fading and multipath propagation), there is a large difference in the signal powers received by different users. A packet can then be decoded successfully even if a collision happens. To take that into

[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].

account we also validate our results by performing simulations with the discrete-event network simulator ns-3 [18].

Our goal is to evaluate the benefit of jamming from a secrecy perspective in connection with MAC-related parameters such as the density of jammers and eavesdroppers in the system. The jammers cause collisions on both eavesdroppers as well as on legitimate receivers. It is therefore necessary to have a metric that captures this trade-off in a multi-terminal environment.

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. We emphasize that the secure throughput is not an approximation or generalization of the secrecy capacity. Our goal with this metric is to assess the level of secrecy for communication in a multi-terminal environment, in connection with link-layer aspects such as the density of jammers and eavesdroppers in the system.

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]

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

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 ${\rm a} \to {\rm b} \wedge \bigwedge_{e_i \in \Pi_{\rm e}} {\rm a} \nrightarrow e_i$, in which case the system is said to be in outage.

B. Characterization of Secure Throughput

Define the following radiuses

$$r_{\jmath,{\rm b}} \triangleq \left(\frac{P_\jmath}{P_{\rm b}^*}\right)^{1/2b}, \; r_{\rm a,e} \triangleq \left(\frac{P_{\rm a}}{P_{\rm e}^*}\right)^{1/2b}, \; r_{\jmath,{\rm e}} \triangleq \left(\frac{P_\jmath}{P_{\rm e}^*}\right)^{1/2b}.$$

[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.

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

Proposition 1 (Conditions for Maximum Secure Throughput): Consider that the following conditions hold:

1) $\mathcal{B}_{x_{\rm b}}(r_{\jmath,{\rm b}}) \cap \mathcal{R} = \emptyset$, and
2) $\mathcal{B}_x(r_{\jmath,{\rm e}}) \cap \mathcal{R} \neq \emptyset$ for all $x \in \mathcal{B}_{x_{\rm a}}(r_{\rm a,e})$.

Then, $\lim_{\lambda_\jmath \to \infty} \mathcal{T}_{\rm s}(\lambda_\jmath) = 1$.

Proof: See Appendix II. ∎

In essence, the above proposition says that the maximum secure throughput can be achieved if the region $\mathcal{R}$ of active jammers is appropriately chosen so that it does not affect Bob (Condition 1), but still affects the eavesdroppers (Condition 2).

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

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

where the parameters are given by

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

The left part of the expression corresponds to the throughput at Bob $\widetilde{\mathcal{T}}_{\rm b}$, whereas the right part is one minus the throughput at Eve $\widetilde{\mathcal{T}}_{\rm e}$. Later in the paper, we resort to simulations to confirm that (2) closely approximates the secure throughput. This formula is relevant to assess the secrecy level of communication and allows us to analyze the effect of varying certain parameters over which one may have control, such as the region of active jammers $\mathcal{R}$, $\lambda_\jmath$, $P_{\rm a}$ and $P_\jmath$.

C. Choice of Region of Active Jammers

The region of active jammers is a critical factor to improve the secure throughput and should encompass as many eavesdroppers as possible without causing much harm to the legitimate receiver. Although a generic analysis of the effect of various regions on the secure throughput seems beyond reach, it is possible to establish relationships between the individual throughputs as follows.

Lemma 1: For arbitrary regions of active jammers $\mathcal{R}_1 \subset \mathcal{R}_2$, $\widetilde{\mathcal{T}}_{\rm b}^{\mathcal{R}_2} \leq \widetilde{\mathcal{T}}_{\rm b}^{\mathcal{R}_1}$ and $\widetilde{\mathcal{T}}_{\rm e}^{\mathcal{R}_2} \leq \widetilde{\mathcal{T}}_{\rm e}^{\mathcal{R}_1}$.

However, the effect of these regions $\mathcal{R}_1$ and $\mathcal{R}_2$ on the secure throughput is highly dependent on the specific regions under consideration. For example, with $\mathcal{R} = \emptyset$ since there are no jammers in the system the throughput at Bob is 1, and the secure throughput depends only on the density of eavesdroppers as follows $\lim_{\lambda_{\rm e} \to 0} \mathcal{T}_{\rm s}^{(\mathcal{R}=\emptyset)} = 1$ and $\lim_{\lambda_{\rm e} \to \infty} \mathcal{T}_{\rm s}^{(\mathcal{R}=\emptyset)} = 0$. On the other hand, with $\mathcal{R} = \mathbb{R}^2$ the density of jammers affects

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

TABLE I: Effect of interference from the jammers on the eavesdroppers and Bob and possible jamming strategies with their respective regions of active jammers.

the secure throughput in the following way $\lim_{\lambda_\jmath\to 0}\mathcal{T}_\mathrm{s}^{(\mathcal{R}=\mathbb{R}^2)}=\mathcal{T}_\mathrm{s}^{(\mathcal{R}=\emptyset)}$ and $\lim_{\lambda_\jmath\to\infty}\mathcal{T}_\mathrm{s}^{(\mathcal{R}=\mathbb{R}^2)}=0$. Ideally, a region of active jammers should ensure that the secure throughput does not asymptotically go to 0 with increasing density of jammers, neither should it depend on having no eavesdropper to achieve maximum secure throughput.

IV. Jammer Selection Strategies

The conditions for maximum secure throughput in *Proposition 1* accommodate two important aspects of secure communications – the need to cause as much interference as possible to as many eavesdroppers as possible while causing little interference to Bob. 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 strategies 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, $\mathcal{B}_{x_\mathrm{b}}(r_{\jmath,\mathrm{b}})$. 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, $\mathcal{B}_{x_\mathrm{a}}(r_{\mathrm{a,e}})$. 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.

In the following we characterize the strategies summarized in Table I and present the rationale behind them.

A. No Jamming

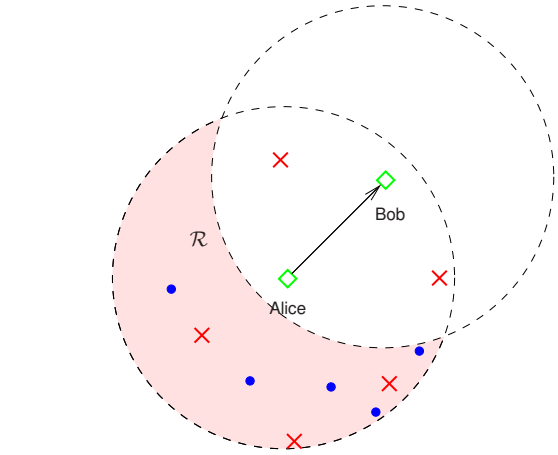
Although not relevant from a secrecy perspective, this is a simple reference strategy for the case without jammers. In this case, no jammer is active and the region of active jammers is $\mathcal{R}=\emptyset$.

Proposition 2: The secure throughput for the no jamming (nojam) strategy is given by

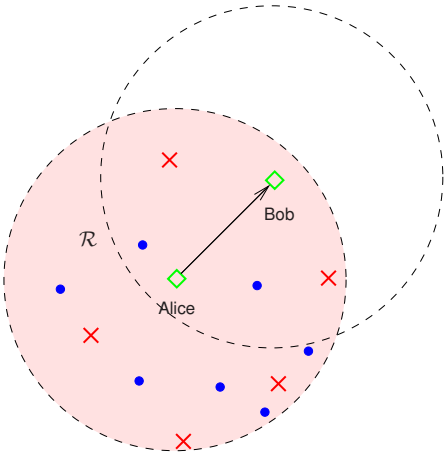
$$\widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{nojam}}=\exp\left(-\lambda_\mathrm{e}\cdot\pi r_{\mathrm{a,e}}^2\right). \tag{3}$$

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.



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



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

Fig. 2: Jammer selection strategies. 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.

B. Global Jamming

In contrast with the previous, this strategy 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 3: The secure throughput for the global jamming strategy is given by

$$\widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{global}}=\exp(-\lambda_\jmath\cdot\pi r_{\jmath,\mathrm{b}}^2)\times\exp\left(-\lambda_\mathrm{e}\cdot\pi r_{\mathrm{a,e}}^2\cdot\exp(-\lambda_\jmath\cdot\pi r_{\jmath,\mathrm{e}}^2)\right). \tag{4}$$

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 strategy 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 4: The secure throughput for the jamming with near-receiver contention (jnrc) strategy is given by

$$\widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{jnrc}} = \exp\left(-\lambda_\mathrm{e}\pi r_{\mathrm{a,e}}^2 \cdot p_{\jmath,\mathrm{e}}\right), \tag{5}$$

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 strategy 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 5: The secure throughput for the near-source jamming (nsj) strategy is given by

$$\begin{aligned}\widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{nsj}} &= \exp\left(-\lambda_\jmath \cdot \mathbb{A}\{\mathcal{B}_{x_\mathrm{b}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{B}_{x_\mathrm{a}}(r_{\mathrm{a,e}})\}\right)\\ &\times \exp\left(-\lambda_\mathrm{e}\pi r_{\mathrm{a,e}}^2 \cdot p_{\jmath,\mathrm{e}}\right),\end{aligned} \tag{6}$$

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

$$\lim_{\lambda_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{global}} = \lim_{\lambda_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{nsj}} = 0 < \lim_{\lambda_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{nojam}} \leq \lim_{\lambda_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{jnrc}}, \tag{7}$$

$$\lim_{P_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{global}} = 0 < \lim_{P_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{nsj}} < \lim_{P_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{jnrc}} = \lim_{P_\jmath\to\infty} \widetilde{\mathcal{T}}_\mathrm{s}^{\mathrm{nojam}}. \tag{8}$$

Proof: The secure throughput of the no jamming strategy 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 $p_{\jmath,\mathrm{e}} \leq 1$ in (5). In the limit of large density of jammers, the secure throughput of the remaining strategies becomes

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

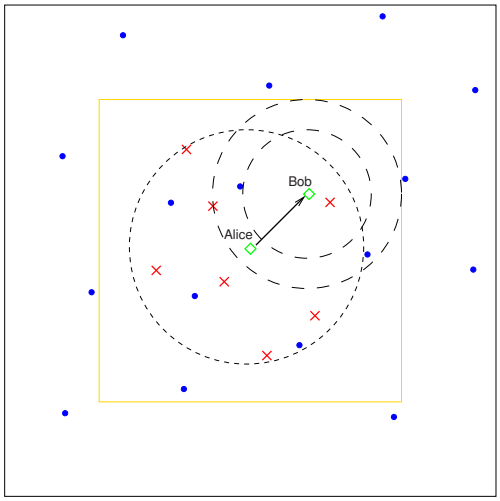


Fig. 3: Setup for Monte Carlo experiments: Alice and Bob are located respectively at the positions $(0,0)$ and $(1,1)$ of an inner region (highlighted) of a $\mathcal{S} = 10\mathrm{m}\times10\mathrm{m}$ square. This prevents border effects on Alice and Bob. Alice transmits with power $P_\mathrm{a} = 40\mathrm{mW}$ 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 $\mathcal{S}$.

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

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

$\mathbb{A}\{\mathcal{B}_x(r_{\jmath,\mathrm{e}}) \cap \mathcal{B}_{x_\mathrm{a}}(r_{\mathrm{a,e}})\backslash\mathcal{B}_{x_\mathrm{b}}(r_{\jmath,\mathrm{b}})\} = 0$ in (5) when $P_\jmath \to \infty$.

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 strategy will overcome the reference strategy without jammers. Also, strategies 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 actual 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 $A = 100\ \mathrm{m}^2$. 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 $\mathcal{S}$. The sensitivity thresholds of Bob and the eavesdroppers are both set to the value of $\approx 2.94\mathrm{mW}$, derived from the maximum connectivity range in ns-3 of roughly 20 meters scaled down to the system setup under consideration. The connectivity between nodes is then assessed based on their

relative distances and sensitivity thresholds 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 strategy for varying density of jammers. The plot shows that the analytical secure throughput in (4) approximates the simulated values for a wide range of parameters. We observed that for all strategies the approximation is not tight only for a combination of large λ_e and P_j values, since the independence approximations of Appendix I do not hold.

A. Comparison of Strategies

Figure 5 compares the different strategies for varying density of jammers. Since there are no jammers in the system, the secure throughput of the no jamming strategy is steady for all λ_j values and serves mainly as a reference value. The strategies of 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 λ_j, up to a cross-over value after which collisions on Bob become dominant and the secure throughput worsens (as illustrated in *Figure 5*). The strategy of 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 λ_j (as illustrated for global jamming with $\lambda_e = 0.01$ in *Figure 4*). This happens because the expected number of eavesdroppers is low and, therefore, collisions on Bob are dominant for all λ_j values.

As expected, the strategy of jamming with near-receiver contention scales well with increasing λ_j, because there are no jammers audible to Bob. Actually, only this strategy is immune to variations in λ_e and consistently leads to improved secure throughput. These results comply with the ordering of strategies of *Proposition 6*.

B. Power Expenditure

The expected total jamming power P_j^{tot} varies among the different strategies and is given by

$$P_j^{tot} = P_j \cdot \lambda_j \mathbb{A}\{\mathcal{R}\}, \tag{9}$$

where $\lambda_j \mathbb{A}\{\mathcal{R}\}$ is the expected number of jammers as a function of the region of active jammers $\mathcal{R}$. For the same density of jammers λ_j, the expected total jamming power P_j^{tot} employed by the different strategies changes proportionally to the size of the corresponding region of active jammers and P_j^{tot} is then lower for near-receiver contention, followed by near-source jamming and then global jamming[3].

Equivalently, for fixed P_j at all jammers, the near-receiver contention strategy can employ a larger density of jammers λ_j and result in the same P_j^{tot} as, for example, near-source jamming. This basically changes the rate at which the strategies converge when P_j^{tot} grows. The resulting plot is omitted because it follows a very similar behavior to *Figure 5*.

[3]The expected total jamming power of global jamming is unrestrained because all jammers in $\mathbb{R}^2$ are active.

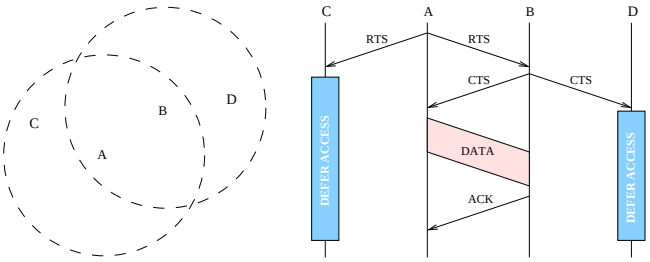


Fig. 6: RTS/CTS handshake on action. A is the source and B the receiver.

VI. A JAMMING PROTOCOL FOR SECRECY-IMPROVED IEEE 802.11

Aspects such as fading and the distance between nodes lead to large differences in the signal powers received by different users. Hence, a packet can be decoded successfully even if a collision happens. To take that into account, we now propose and evaluate a practical protocol to implement the strategies of Section IV.

A. IEEE 802.11

The wireless networking standard IEEE 802.11 implements a random access protocol named CSMA/CA (carrier sense multiple access with collision avoidance). With CSMA/CA, each node senses the channel before transmission and refrains from transmitting if the channel is sensed busy. This type of channel sensing is called physical carrier sensing. Collision avoidance is performed by waiting a random amount of time before trying to transmit again, if the channel is sensed busy. This reduces the number of collisions, but collisions can still occur, for example, if two stations are hidden from each other (hidden terminal issue).

To address the hidden terminal issue, the IEEE 802.11 includes a channel reservation scheme performed through the well-known RTS/CTS handshake. This is a form of virtual carrier sensing that operates as follows. Whenever a node receives a RTS or a CTS, it gets blocked and defers from channel access. This happens to avoid hidden terminal related collisions and allows the communicating devices to successfully receive data and control traffic, as shown in *Figure 6*. In particular A is able to receive the CTS and ACK messages, which respectively announce that A can transmit and report that data was received with success by B. On the other end, B is able to receive data from A without the obstruction from D.

B. Implementation of Strategies

The implementation of the strategies of Section IV depends on a signaling scheme that conveys connectivity information of the jammers with respect to Alice and Bob. We chose to use the RTS/CTS handshake, whose goal is to address

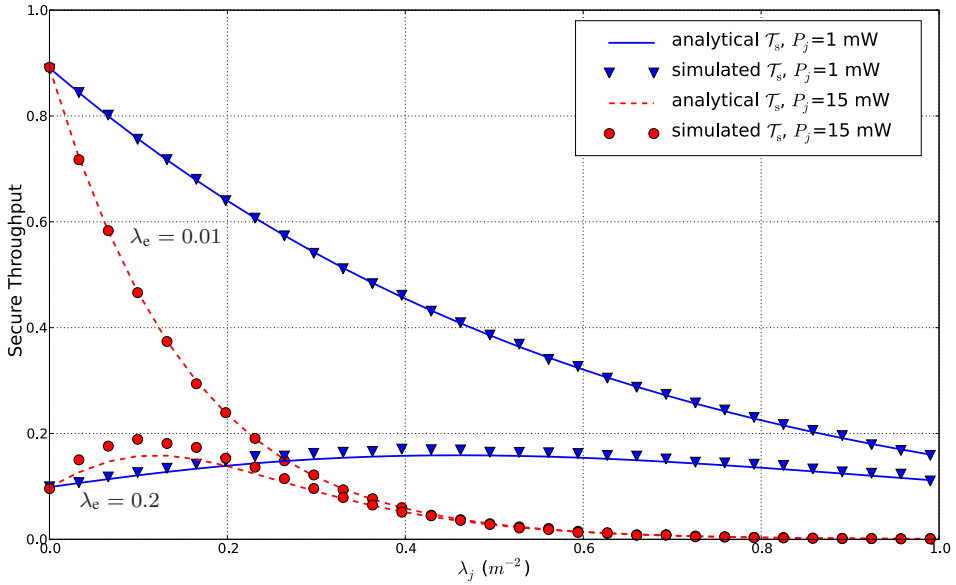


Fig. 4: Global Jamming: analytical vs simulated results.

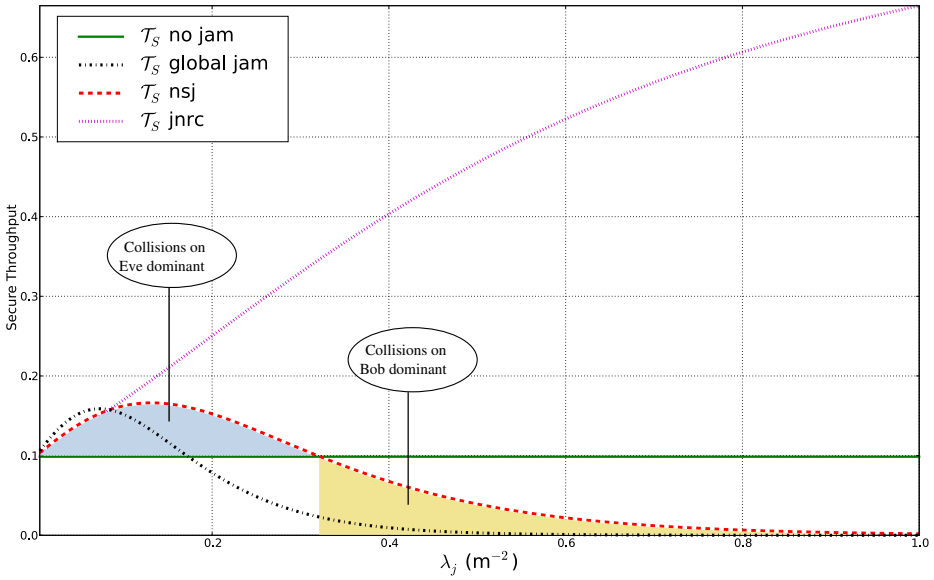


Fig. 5: Comparison of strategies for varying λ_j ($P_a = 40$mW, $P_j = 40$mW, $\lambda_e = 0.2\text{m}^{-2}$).

the hidden terminal problem by blocking neighboring users of the communicating devices. Although possibly useful, the RTS/CTS is barely used in practice because it usually reduces the performance of a wireless network, and these blocked nodes have been identified as one of the reasons for that [19]. We argue that this mechanism can be used to identify jammers that are useful from a secrecy perspective. Namely, a jammer will only receive a RTS or a CTS if it is connected to Alice or Bob, respectively. *Figure 7* shows a setup in which a neighbor of the source jams after reception of a RTS message. A practical jamming protocol in which jammers decide if they are active or not based on this signaling scheme is described in Table II, for the near-source jamming and the jamming with near-receiver contention strategies.

C. Simulations Setup

To evaluate the proposed strategies we resort to network simulator ns-3. We consider a system setup identical to the one of *Figure 3*, although featuring multiple source-sink pairs. Namely, a set of 25 nodes is placed randomly in the inner region of a larger square with 10000 m^2, such that some transmissions require multi-hop communication. Jammers and eavesdroppers are also placed randomly in the overall region. Several forms of jamming have already been investigated [20]. For simplicity, in the simulations the jammers simply broadcast a packet of the same length as the source packet, thus

[4]This means that the jammer is not on the audible region of Bob because no CTS was received, but Alice got a CTS and that is why transmission is taking place.

TABLE II: A jamming protocol for secrecy-improved IEEE 802.11.

Operation at communicating nodes (regular RTS/CTS scheme):

1) Alice wants to send a packet to Bob and, therefore, sends a RTS requiring channel reservation; this message is received by all neighbors of Alice and contains an estimation of the total time for transmission of the DATA and the corresponding acknowledgement (ACK);
2) If available for communication, Bob replies with a CTS, and this message is received by all neighbors of Bob;
3) Alice sends the desired data packet;
4) If successfully received, Bob sends an ACK back to Alice.

Operation at jammers:

Near-source jamming strategy:

1) Upon reception of a RTS the jammer is aware of the intent of transmission by Alice;
2) Start jamming after either (1) the CTS is received or (2) the beginning of the source transmission is detected through physical carrier sensing;
3) Jam until the estimated time for transmission received in the RTS reservation minus a short time interval (to ensure no collision with the ACK frame);

Jamming with near-receiver contention strategy:

1) Upon reception of a RTS the jammer is aware of the intent of transmission by Alice;
2) Start jamming if a CTS was not received, and the beginning of transmission from the source is detected, e.g. through physical carrier sensing[4];
3) Jam until the estimated time for transmission received in the RTS minus a short time interval (to ensure no collision with the ACK frame);

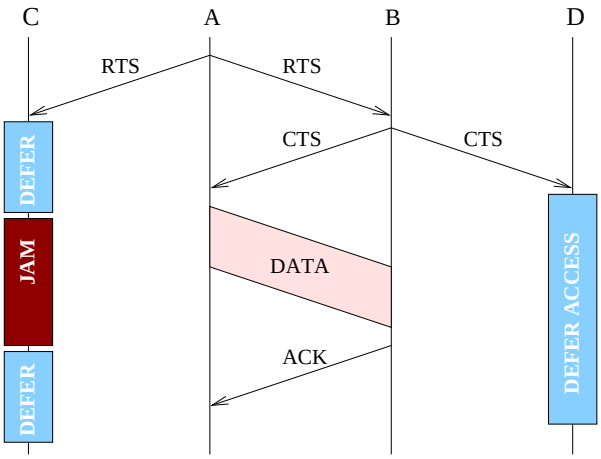


Fig. 7: RTS/CTS with jamming from a neighbor of A.

causing the desired added interference to the neighboring nodes. In this setup, the signal strength of a received packet is affected by the transmission of any neighbor and a packet is successfully received if it meets a minimum required signal strength level.

For the ns-3 simulations we resort to a 802.11b physical layer model with network interface cards in ad-hoc mode and Optimized Link State Routing as the routing protocol. The channels follow the log-distance channel propagation model where the pathloss PL is given by

$$PL(dB) = PL(d_0) + 10n\log_{10}\left(\frac{d}{d_0}\right),$$

where n is the path loss exponent, d is the transmitter-receiver distance and d_0 is the reference close-in distance. Modeling the environment as a building with obstructions [21] (e.g. from walls) we set the pathloss exponent to 4 and reception gain to -15dB, thus resulting in a maximum connectivity range of roughly 20 meters. The pathloss at the reference distance of $d_0 = 1$m is evaluated based on free space propagation. The remaining parameters take the default values defined in ns-3.

For statistically rigorous results, we use the method of independent replications of [22]. For that, 5 independent replications are run and, for each replication, 50 observations are performed. At each observation all nodes are placed at random. Then, 5 source-sink pairs are randomly selected and exchange packets of 500 bytes at a rate of 25 packets/sec. These source-sink pairs change every 2 seconds over a 30 second time interval that starts after the route setup process has already taken place. The 95% confidence intervals are then calculated based on all observations of the system.

D. Metrics

To assess the secrecy level in the network, we focus on the secure throughput $\mathcal{T}_s$ defined in (1) as the probability of successful transmission of packets from source to destination without any eavesdropper having access to those packets. With multiple source-sink pairs and multi-hop transmissions, this metric is taken over all transmissions in the network, therefore taking into consideration the effect of active jammers on other simultaneously active devices.

We also consider the energy cost of jamming for secrecy. Let $\mathcal{N}_{\text{data}}$ and $\mathcal{N}_{\text{jam}}$ be respectively the total number of data and jamming bytes transmitted at the physical layer. $\mathcal{N}_{\text{app}}$ represents the total number of end-to-end data bytes received at the application level. The energy efficiency captures the relation between the total number of received end-to-end data bytes and the number of number of bytes (data or jamming) required to be transmitted at the physical layer so that an end-to-end transmission is successful.

$$\mathbb{E}_{\text{eff}} = \frac{\mathcal{N}_{\text{app}}}{\mathcal{N}_{\text{data}} + \mathcal{N}_{\text{jam}}} \in [0,1]. \tag{10}$$

Note that this metric is 1 only when no jamming is used and a transmission is performed successfully in a single hop without any retransmission.

E. Transmission Power of Jammers

The analytical results have shown that improved secure throughput depends on contained transmission power by the

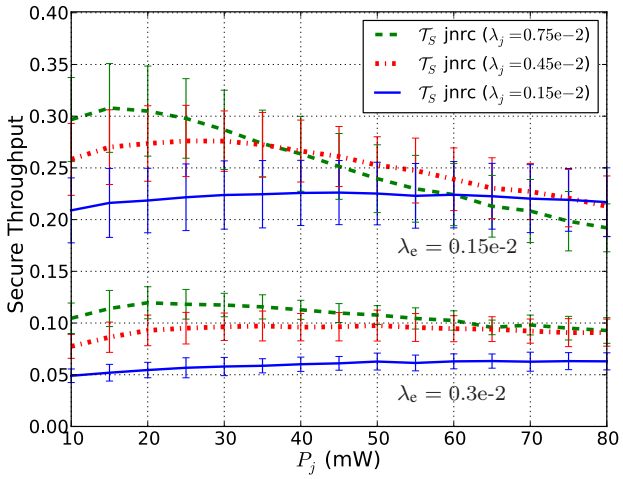
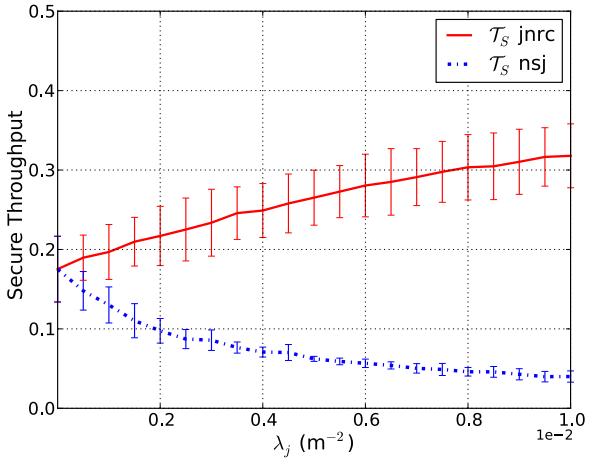


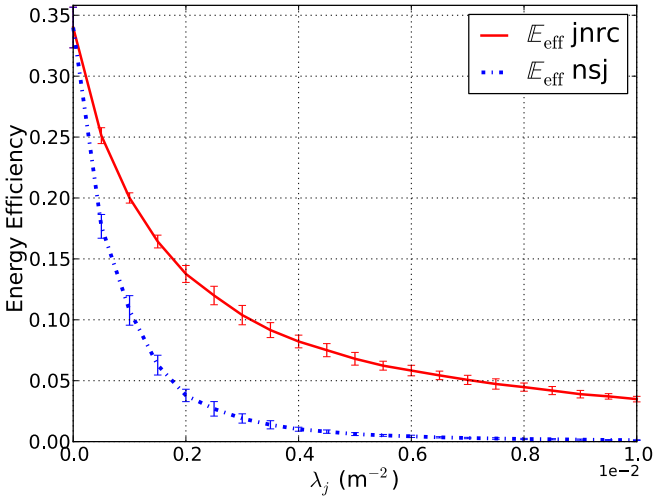
Fig. 8: Simulation results for varying P_J with different (λ_e, λ_J) configurations.

jammers. *Figure 8* exhibits the secure throughput of jamming with near-receiver contention as a function of P_J for different combinations of λ_J and λ_e.

These results show that (1) for low density of jammers there is room for $\mathcal{T}_s$ improvement by increasing P_J up to a certain point, however the gain is marginal, possibly not justifying the energy cost for the jammers; (2) for higher densities of jammers, a low P_J leads to the maximum benefit on $\mathcal{T}_s$, which then decays with increasing P_J. Results for near-source jamming show that the effect of increasing P_J is even more damaging, as consequence of the proximity between the jammers and the source. These results indicate that a large density of jammers with low transmission power is a sensible choice to perform jamming for secrecy.



(a) Variation in $\mathcal{T}_s$.



(b) Variation in $\mathbb{E}_{\text{eff}}$.

Fig. 9: Simulation results for varying λ_J (λ_e = 0.15e-2 m^{-2}, P_J = 10mW).

F. Results and Discussion

Figure 9 depicts the secure throughput and energy efficiency for simulations with varying density of jammers. Notice that both strategies have a common value of $\mathcal{T}_s$ and $\mathbb{E}_{\text{eff}}$ at $\lambda_J = 0$ that corresponds to the secure throughput and energy efficiency of the no jamming strategy.

1) Secure Throughput: As expected, the secure throughput of the jamming with near-receiver contention strategy scales well with λ_J. In particular, this strategy results in a steady increase on $\mathcal{T}_s$ with growing λ_J and leads to a secure throughput gain of nearly $1/3$ when there are twice as much jammers than eavesdroppers in the system (i.e. λ_J = 0.3e-2 m^{-2}). On the contrary, the secure throughput of near-source jamming worsens with increasing λ_J. As mentioned in Section V, this may happen because λ_e is relatively low and, therefore, collisions on Bob are predominant. Contrary to our initial belief, we have found that this behavior of near-source jamming holds for larger λ_e values as well. This happens because of two factors: (1) multiple sources cause more transmissions to take place, and (2) those transmissions may require traversing multiple hops from source to destination. This causes more jammers to be active than expected, which leads to retransmissions of lost packets. This in turn increases jammer activity. Further simulations with a single source and single-hop transmissions led to the expected results of Section V-A, where near-source jamming leads to an improvement up to a certain cross-over value of λ_J. However, the above results suggest that in a typical network with multiple sources and multi-hop transmissions only jamming with near receiver contention is capable of improving the secure throughput in a consistent manner.

2) Energy Efficiency: The secrecy benefits of jamming come at a cost in terms of energy expenditure. Namely, collisions caused by the jammers may lead to retransmission of lost packets and the jammers themselves have to expend resources to jam. For example, for jamming with near-receiver contention there is an energy efficiency loss to nearly $1/3$ for λ_J = 0.3e-2 m^{-2}. This means that there was a large reduction on the number of bytes received at the application level (goodput) and/or a large increase in the number data and jamming bytes transmitted at the physical layer to achieve that goodput. The energy efficiency loss is even higher for the near-source jamming strategy, as more jammers are active.

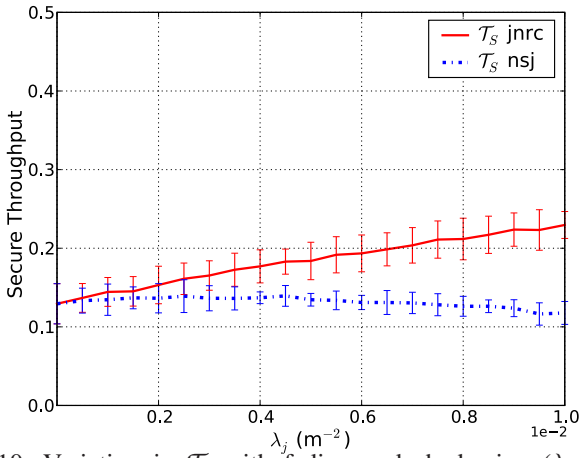


Fig. 10: Variation in $\mathcal{T}_\mathrm{s}$ with fading and shadowing ($\lambda_\mathrm{e} = 0.15\text{e-}2$ m^{-2}, $P_J = 10$mW).

G. Effect of Fading and Shadowing

The results obtained so far assume a simple log-distance pathloss model that closely relates to the analytical part of this work. In *Figure 10* we present simulation results for a setup that includes multipath Rayleigh fading and log-normal shadow fading. For Rayleigh fading we resort to the Nakagami propagation loss model with parameter $m = 1$, whereas shadowing results from adding a random propagation loss model with a Gaussian random variable with mean 0 and variance 6.8 (typical values for wireless networks [21]). In this case, the signal strength varies such that we no longer have nicely shaped circular connectivity regions as shown in Section IV.

The secure throughput of *Figure 10* at $\lambda_J = 0$ is lower, which is normal since fading is known to reduce the capacity of wireless networks. This figure shows that jamming with near-receiver contention leads to similar gains as in the case without fading and scales well with λ_J. Somewhat surprisingly, near-source jamming benefits from the effect of fading and shadowing. Since fading reduces the throughput, fewer transmissions take place. This leads to fewer active jammers and, consequently, fewer retransmissions of lost packets. This was identified as one of the reasons for the decay of $\mathcal{T}_\mathrm{s}$ for near-source jamming in *Figure 9(a)*. However, the secure throughput is still barely improved with near-source jamming. As expected, near-receiver contention remains the best strategy.

VII. Conclusions

The location of active jammers is a crucial aspect in designing jamming protocols to improve the secrecy of wireless networks. We proposed and evaluated a set of strategies that capture the secrecy trade-off of the impact of jammers on legitimate receivers and eavesdroppers on a multi-terminal environment. Our results show 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 jammers. We proposed and evaluated a practical jamming protocol for wireless networks. Our analysis shows that there is a significant energy cost of jamming for secrecy. This calls for power control at the jammers and a more selective choice of jammers based on their relative locations in the network. Another line of work that would be interesting to pursue is the analysis of time-adaptive jamming strategies that employ different jammers in disparate time slots.

Appendix I
Derivation of (2)

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

$$\begin{aligned}\mathcal{T}_\mathrm{s} &= \mathbb{P}\left\{\mathrm{a}\to\mathrm{b} \wedge \bigwedge_{e_i\in\mathcal{E}} \mathrm{a}\nrightarrow e_i\right\}\\ &= \mathbb{P}\left\{\mathrm{a}\to\mathrm{b}\,\middle|\bigwedge_{e_i\in\mathcal{E}} \mathrm{a}\nrightarrow e_i\right\}\times\mathbb{P}\left\{\bigwedge_{e_i\in\mathcal{E}} \mathrm{a}\nrightarrow e_i\right\}\\ &= \mathbb{P}\left\{\mathrm{a}\to\mathrm{b}\,\middle|\bigwedge_{e_i\in\mathcal{E}} \mathrm{a}\nrightarrow e_i\right\}\times\sum_{n=0}^{\infty}\mathbb{P}\left\{\bigwedge_{e_i\in\mathcal{E}} \mathrm{a}\nrightarrow e_i\,\middle|\, N_\mathrm{a,e}=n\right\}\\ &\times\mathbb{P}\{N_\mathrm{a,e}=n\}, \end{aligned} \tag{11}$$

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, (11) becomes

$$\widetilde{\mathcal{T}}_\mathrm{s} = \mathbb{P}\{\mathrm{a}\to\mathrm{b}\}\times\sum_{n=0}^{\infty}(1-p_{J,\mathrm{e}})^n\cdot\mathbb{P}\{N_\mathrm{a,e}=n\} \tag{12}$$

where $p_{J,\mathrm{e}} \triangleq \mathbb{P}\{\mathrm{a}\to e_i|\,N_\mathrm{a,e}=n\}$. 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 $\mathcal{B}_{x_\mathrm{b}}(r_{J,\mathrm{b}})$, whose number is a Poisson RV with mean $\mu_{J,\mathrm{b}} = \lambda_J\cdot\mathbb{A}\{\mathcal{B}_{x_\mathrm{b}}(r_{J,\mathrm{b}})\cap\mathcal{R}\}$. Then,

$$\begin{aligned}\mathbb{P}\{\mathrm{a}\to\mathrm{b}\} &= \mathbb{P}\{\text{no jammers in } \mathcal{B}_{x_\mathrm{b}}(r_{J,\mathrm{b}})\cap\mathcal{R}\}\\ &= \exp(-\mu_{J,\mathrm{b}}).\end{aligned} \tag{13}$$

To determine the summation in (12), 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

$$\sum_{n=0}^{\infty}(1-p_{J,\mathrm{e}})^n\cdot\mathbb{P}\{N_\mathrm{a,e}=n\} = \exp\left(-\mu_\mathrm{a,e}\cdot p_{J,\mathrm{e}}\right). \tag{14}$$

We now determine $p_{J,\mathrm{e}}$. Let N_J denote the (random) number of jammers that are audible by e_i. Conditional on the location $e_i = x$, the RV N_J is Poisson with mean $\mu_{J,x} = \lambda_J\cdot\mathbb{A}\{\mathcal{B}_x(r_{J,\mathrm{e}})\cap\mathcal{R}\}$. 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

$$\begin{aligned}p_{J,\mathrm{e}} &= \mathbb{E}_{e_i}\{p_{J,\mathrm{e}}|e_i\}\\ &= \mathbb{E}_{e_i}\{\mathbb{P}\{N_J=0|N_\mathrm{a,e},e_i\}\}\\ &= \frac{1}{\pi r_\mathrm{a,e}^2}\iint_{\mathcal{B}_{x_\mathrm{a}}(r_\mathrm{a,e})}\exp(-\mu_{J,x})dx.\end{aligned} \tag{15}$$

Symbol	Usage
$\mathbb{E}\{\cdot\}$	Expectation operator
$\mathbb{P}\{\cdot\}$	Probability operator
b	Amplitude loss exponent
$x_{\mathrm{a}}, x_{\mathrm{b}}$	Location of Alice and Bob
$\Pi_{\mathrm{e}} = \{e_i\}, \Pi_{\jmath} = \{x_i\}$	Poisson processes of eavesdroppers and jammers
$\lambda_{\mathrm{e}}, \lambda_{\jmath}$	Spatial densities of eavesdroppers and jammers
$P_{\mathrm{a}}, P_{\jmath}$	Transmit power of Alice and jammers
$P_{\mathrm{b}}^*, P_{\mathrm{e}}^*$	Sensitivity of Bob and eavesdroppers
$\Pi\{\mathcal{R}\}$	Number of nodes of process Π in region $\mathcal{R}$
$\mathcal{B}_x(\rho)$	Ball centered at x with radius ρ
$\mathbb{A}\{\mathcal{R}\}$	Area of region $\mathcal{R}$
$\mathcal{T}_{\mathrm{s}}$	Secure throughput
$\widetilde{\mathcal{T}}_{\mathrm{s}}$	Approximation of the secure throughput
$\widetilde{\mathcal{T}}_{\mathrm{b}}$,$\widetilde{\mathcal{T}}_{\mathrm{e}}$	Throughput at Bob and Eve, respectively
$\mathcal{T}_{\mathrm{s}}^{(\mathcal{R})}$	Secure throughput with region of active jammers $\mathcal{R}$ (can be any region in $\mathbb{R}^2$)
$\widetilde{\mathcal{T}}_{\mathrm{b}}^{(\mathcal{R})}$, $\widetilde{\mathcal{T}}_{\mathrm{e}}^{(\mathcal{R})}$	Throughput at Bob and Eve with region of active jammers $\mathcal{R}$, respectively

TABLE III: Notation and symbols.

This concludes the proof.

APPENDIX II
DERIVATION OF PROPOSITION 1

Letting $\mathcal{E} \triangleq \Pi_{\mathrm{e}} \cap \mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})$, we rewrite (1) as

$$\mathcal{T}_{\mathrm{s}} = \mathbb{P}\left\{\mathrm{a} \to \mathrm{b}\right\} \times \mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i | \mathrm{a} \to \mathrm{b} \right\}. \tag{16}$$

Now,

$$\begin{aligned} \mathbb{P}\left\{\mathrm{a} \to \mathrm{b}\right\} &= \mathbb{P}\{\text{no jammers in } \mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{R}\} \\ &= \exp(-\lambda_{\jmath} \cdot \mathbb{A}\{\mathcal{B}_{x_{\mathrm{b}}}(r_{\jmath,\mathrm{b}}) \cap \mathcal{R}\}) \\ &= 1, \end{aligned} \tag{17}$$

due to Condition 1. Furthermore,

$$\begin{aligned} &\mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i | \mathrm{a} \to \mathrm{b} \right\} \\ &= \mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &= 1 - \mathbb{E}_{\mathcal{E}}\left\{ \mathbb{P}\left\{ \bigvee_{e_i \in \mathcal{E}} \mathrm{a} \to e_i \,\middle|\, \mathcal{E} \right\} \right\} \\ &\geq 1 - \mathbb{E}_{\mathcal{E}}\left\{ \sum_{e_i \in \mathcal{E}} \mathbb{P}\left\{\mathrm{a} \to e_i | \mathcal{E}\right\} \right\} \\ &= 1 - \mathbb{E}_{\mathcal{E}}\left\{ \sum_{e_i \in \mathcal{E}} \exp(-\lambda_{\jmath} \cdot \mathbb{A}\{\mathcal{B}_{e_i}(r_{\jmath,\mathrm{e}}) \cap \mathcal{R}\}) \right\}, \end{aligned} \tag{18}$$

where the inequality above is due to the union bound. Because of Condition 2, the exponential term converges to zero as $\lambda_{\jmath} \to \infty$, and the whole expression converges to one. Thus, we have $\lim_{\lambda_{\jmath} \to \infty} \mathcal{T}_{\mathrm{s}}(\lambda_{\jmath}) = 1$ as desired.

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," *accepted 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.

[18] "Network simulator 3, version 3.7.1," `http://www.nsnam.org/`.

[19] S. Ray, J. Carruthers, and D. Starobinski, "RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs," in *IEEE Wireless Communications & Networking Conference*, vol. 3, New Orleans, LA, USA, 2003, pp. 1516–1521.

[20] X. He and A. Yener, "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.

[21] P. Stuedi, O. Chinellato, and G. Alonso, "Connectivity in the presence of shadowing in 802.11 ad hoc networks," in *IEEE Wireless Commu-*

nications and Networking Conference, vol. 4, New Orleans, LA, USA, 2005, pp. 2225–2230.

[22] D. Goldsman and G. Tokol, "Output analysis procedures for computer simulations," in *Winter Simulation Conference*, Orlando, FL, USA, 2000, pp. 39–45.