Physical-layer Security Against Non-degraded Eavesdroppers

João P. Vilela, João Sá Sousa
CISUC, Department of Informatics Engineering
University of Coimbra, Coimbra, Portugal.
Email: {jpvilela, jagsousa}@dei.uc.pt

***Abstract*—Most of current physical-layer security techniques rely on a degraded eavesdropper, thus warranting some sort of advantage that can be relied upon to achieve higher levels of security. We consider instead *non-degraded eavesdroppers*, that possess equal or better capabilities than legitimate receivers. Under this challenging setup, most of current physical-layer security techniques become hard to administer and new dimensions to establish advantageous periods of communication are needed. For that, we characterize the secrecy level of two schemes for physical-layer security under non-degraded eavesdroppers: a spread spectrum uncoordinated frequency hopping scheme, and a jamming receiver with self-interference cancellation.**

I. Introduction

Recent works on physical-layer security [1] show that the physical characteristics of wireless channels can be used to enhance the secrecy level of these networks. These works typically assume that an eavesdropper adversary is, at least in some periods of time, in a degraded situation. This can be enabled, for instance, by (a) having the eavesdropper on a disadvantaged position/location with respect to the legitimate receiver, (b) the eavesdropper suffering interference [2] that can possibly be removed at the legitimate receiver [3], or (c) using relays to improve the quality of information available at the receiver [4]. This is legitimate if, for example, there is a protected area such as a warehouse of RFID devices where eavesdroppers are not able to enter [5], or cooperative devices are able to strictly synchronize with legitimate devices.

If we assume that a set of eavesdroppers is able to choose an optimal overhearing location (close to the transmitter), for example by analysis of traffic from the source [6], eavesdroppers will most likely benefit from a comparable, if not better, signal quality than the legitimate receiver. This leads to a severe degradation of the *secure throughput* (i.e. probability of a transmission being received by the legitimate receiver without being received by any eavesdropper) with increased number of eavesdroppers, as depicted in *Figure 1*.

Without some sort of advantage over the eavesdroppers, the practical applicability of the aforementioned schemes can become compromised. For example, if the eavesdropper is well-placed, periods of better signal to the legitimate receiver will become very sparse (if any); causing interference to eavesdroppers which cleverly select their location (e.g. on top of the receiver) without affecting the receiver too much or allowing it to filter/remove that interference becomes hard to administer; and having selected relays cooperate in providing a better signal to the legitimate receiver will lead to an eventually even better signal for an ingenious eavesdropper.

This work was partially funded by the Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) under project PEst-OE/EEI/LA0008/2013 (WINCE - Wireless Interference and Coding for Secrecy) conducted at Instituto de Telecomunicações, and project PTDC/EEI-TEL/3684/2014 (SWING2 - Securing Wireless Networks with Coding and Jamming). It was also partly supported by project iCIS under grant CENTRO-07-ST24-FEDER-002003.

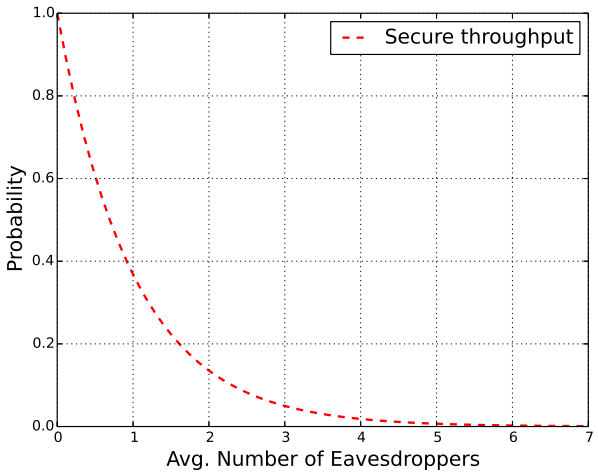

Fig. 1: Variation of the secure throughput with varying number of eavesdroppers close to the transmitter for a spatial stochastic network model as described in Section III.

Other venues for secrecy against non-degraded eavesdroppers are then required. In this work we evaluate two schemes for wireless physical-layer security when eavesdroppers are close to the transmitter, most likely in a favorable situation with respect to the legitimate receiver. The first is based on the Uncoordinated Frequency Hopping (UFH) spread spectrum technique, while the second consists of a jamming receiver with self-interference cancellation to cause interference to nearby eavesdroppers without affecting its received signal.

II. State of the Art

We now review the state of the art of solutions against powerful eavesdroppers, jamming for secrecy, and the Uncoordinated Frequency Hopping spread spectrum technique.

A. Security Against Non-degraded Eavesdroppers

There is a growing interest in physical layer security techniques for disrupting eavesdropper attacks without relying on secret cryptographic keys. A substantial body of literature focus on so called *cooperative jamming* [7]. This security mechanism tries to combat eavesdroppers by combining the efforts of external helpers, jammers, in order to enhance the system's security level. However, few works consider non-degraded eavesdropper adversaries, and in fact, opt to uphold

the opposite (e.g. eavesdroppers are further away from the transmitter than the legitimate receiver).

Nonetheless, there are several articles that consider enhanced eavesdroppers and analyze their impact on secure communication. For example, without jammers, the effect of colluding eavesdroppers [8] which collaborate to degrade the secrecy capacity was considered, showing that even a very small density of eavesdroppers threatens the overall security of the system. This work was extended to consider large wireless networks [9] using secrecy graphs [10] that represent the connections between nodes and their inherent security levels. Results confirm that these non-degraded eavesdroppers significantly improve their ability to decode messages.

Another type of enhanced eavesdropper with multiple antennas was also considered [11]. In this case, each eavesdropper is geared up with multiple antennas that are divided to perform different attacks. The first group of antennas performs conventional eavesdropping, attempting to read the transmitted message, whereas the second set jams nearby channels to deny the receiver the ability to decode the message. This two-way attack either forces the system to deploy more cooperative jammers to prevent eavesdropping, therefore possibly helping the attacker to jam the legitimate channel, or the risk of having insecure communication is significantly increased.

Automatic repeat-request protocols have also been considered [12] against eavesdroppers with channel quality equal to or better than Bob.

B. Interference from a Jamming Receiver

Noise interference [7], [13] is a natural mechanism to address more or less powerful eavesdroppers in a shared medium. As these approaches develop, some new, unconventional techniques emerge, such as generation of artificial noise by the receiver itself. This alternative solution to traditional cooperative jamming from external helpers is considered through a receiver with two antennas [14]: one to receive and another to transmit, which he uses to jam eavesdroppers. This allows the destination node to simultaneously act as a jammer and a receiver, therefore improving the secrecy rate. An extension of this idea was considered [15] by assuming self-interference cancellation, and employing a loop interference model to describe the effect of self-generated noise. These solutions are deemed useful whenever one can not guarantee an efficient jammer placement, or in short-range communications.

Gollakota and Katabi [16] propose a new, channel independent, physical layer security technique where the sender repeats the transmission of a message while the receiver randomly jams a sample of each of these signals. In the end the eavesdropper is incapable of reconstructing the actual data since it cannot distinguish between jammed and clean signal samples. On the contrary, the receiver only needs to pick up all the correct chunks of the message from all the repetitions to get the clean signal, thus eliminating the need of out-of-band interference by external helpers. Practical results show that this scheme is capable of achieving a bit error rate at the eavesdropper between 40% and 60%. However, multiple collaborative eavesdroppers still provide a tough challenge.

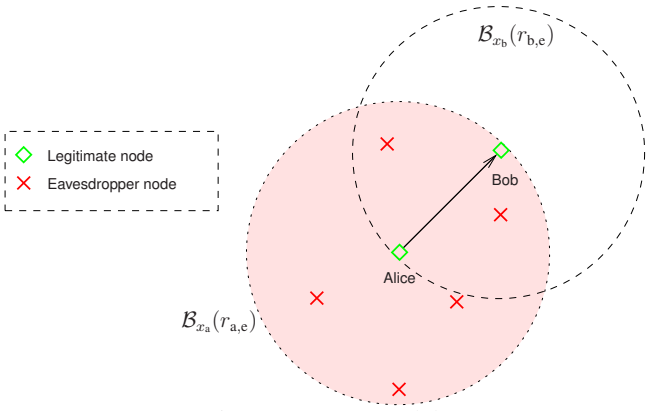

Fig. 2: System model.

C. Uncoordinated Frequency Hopping

Uncoordinated Frequency Hopping (UFH) [17] is a spread spectrum (SS) scheme that addresses Denial-of-Service (DoS) jamming attacks without requiring a pre-shared secret that may be hard to establish. Without the availability of an agreed channel sequence, devices jump uniformly at random between frequencies. Since adversaries are unaware of the random hopping sequence, this enables periods of free communication against a jammer adversary whenever transmitter and receiver lie in the same frequency without the jammer adversary doing so. Communication in adverse environments comes at the cost of a rather low throughput, but enables periods of communication in harsh jammed environments that may be used to establish a shared key [17] for regular coordinated frequency hopping with higher throughput levels.

We have considered the use of UFH for secure communication instead [18], by making it harder for eavesdroppers to overhear legitimate communication. Jammers are, in this case, considered friendly and employed to cause interference to malicious eavesdroppers. We analyze the secure throughput (probability of secure communication) under UFH, both with and without cooperative jammers. We also determine the optimal number of frequencies to optimize secure throughput by with respect to the number of eavesdroppers. Results have shown that it is possible to use this scheme for securing legitimate communication from eavesdroppers, and unveiled the positive effect of using friendly jammers.

Our work differs from previous works in that we consider *non-degraded eavesdroppers* with better or equal reception conditions than the legitimate receiver. To address these powerful adversaries, we consider techniques based on UFH and a jamming receiver. We evaluate the security level of these techniques through a spatial stochastic network model for which we determine and analyze the secure throughput (i.e. the probability of a message being received by the legitimate receiver without being accessed by any eavesdropper) of a system where eavesdroppers arise in advantageous conditions.

III. System and Attacker Model

We consider the scenario depicted in *Figure 2*, 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 [2]. Alice and Bob are located at $x_{\rm a}, x_{\rm b} \in \mathbb{R}^2$, and the set of eavesdroppers is $\Pi_{\rm e} = \{e_i\} \subset \mathbb{R}^2$. The transmit powers of Alice and Bob (whenever transmitting) are $P_{\rm a}$ and $P_{\rm b}$, respectively.

The spatial location of nodes/users can be modeled either deterministically or stochastically. When nodes' positions are unknown to the network designer a priori, they may be treated as uniformly random according to a Poisson point process. Specifically, we consider that $\Pi_{\rm e}$ is an homogeneous Poisson point process (PPP) on $\mathbb{R}^2$ with density $\lambda_{\rm e}$. The locations $x_{\rm a}, x_{\rm b}$ of Alice and Bob are deterministic.

A. 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 [19], based on the notion of audible node.

Definition 1 (Audible Node [19])**.** *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. Let $x \to y$ denote the event of *successful reception* by node y (Bob or an eavesdropper) of the message sent by x (Alice). 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 $x \to y$.

B. 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 analytic 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 assumes that the concurrent transmissions take place simultaneously or at least overlap long enough to make the receiver ignorant.

C. Secure Throughput

To assess the secrecy level of communication in a multi-terminal environment with locations of nodes modeled according to a spatial stochastic model, we consider the secure throughput metric.

Definition 2 (Secure Throughput [2])**.** *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,*

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

Let us consider the following radiuses

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

With this notation, $\mathcal{B}_{x_{\rm a}}(r_{\rm a,e})$ in *Figure 2* is the ball inside which the eavesdroppers can hear Alice, and $\mathcal{B}_{x_{\rm b}}(r_{\rm b,e})$ is the ball inside which eavesdroppers can suffer interference from Bob.

Under this setup, successful communication happens when (1) Alice and Bob are within communication range (i.e. the received power from Alice is above the sensitivity threshold of Bob), and (2) Alice and Bob operate in the same frequency.

Proposition 1. (Secure Throughput without Jamming [2]) The secure throughput for a setup with 1 Tx-Rx pair and a set of eavesdroppers spread uniformly in space according to a Poisson Point Process on $\mathbb{R}^2$ with density $\lambda_{\rm e}$ is given by

$$\mathcal{T}_{\rm s}^{nojam} = \exp(-\mu_{\rm a,e}), \tag{2}$$

where $\mu_{\rm a,e} = \lambda_{\rm e} \cdot \pi r_{\rm a,e}^2$.

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.

D. Attacker Model

We consider *non-degraded eavesdropper* adversaries.

Definition 3 (Non-degraded eavesdropper)**.** *A non-degraded eavesdropper is a network device with the same or higher capabilities (e.g. processing capabilities, number of antennas) as the legitimate receiver, that stands in a location at closer or equal distance to the source and, therefore, at most times benefits from a better signal quality than the legitimate receiver.*

In our case, we consider passive/silent non-degraded eavesdroppers with a location advantage, i.e. they lie within the audible region of Alice, $\mathcal{B}_{x_{\rm a}}(r_{\rm a,e})$, at a distance smaller or equal to that between Alice and Bob. The eavesdroppers have the same capabilities as Alice and Bob. In particular, eavesdroppers are equipped with the same type of transceivers as other devices, which allows all of them to hop between frequencies at a similar rate R. Although eavesdroppers could easily benefit from an advantage by hopping between frequencies much faster, the same kind of reasoning can be applied to Alice and Bob, and, therefore, we evaluate them on equal terms. Eavesdroppers lie silently within vicinity of Alice and we assume that eavesdroppers do not collude, i.e. they only have access to their local information. We further assume that their locations are unknown, albeit closer to the source.

With non-degraded eavesdroppers, the secure throughput decreases quickly with the number of eavesdroppers as seen in *Figure 1*. The non-degraded nature of eavesdroppers limits the applicability of existing techniques such as interference generation/alignment, or cooperative relays. This calls for new approaches for physical-layer security that are not location-dependent as we now explore.

IV. Uncoordinated Frequency Hopping against Non-degraded Eavesdroppers

One possibility to address non-degraded eavesdroppers with a better location than Bob is to explore the frequency dimension, in order to obtain periods of advantageous communication against strong and possibly numerous adversary eavesdroppers. UFH has been proposed as a frequency hopping scheme to deal with DoS attacks from jammer adversaries. In this section we consider UFH against non-degraded eavesdropper adversaries. For that, we consider that Alice and Bob hop uniformly at random through a set of N frequency channels, while the eavesdroppers randomly hop through the same set of frequencies with the goal of overhearing communication. Secure communication happens when Alice and Bob lie in the same frequency without any eavesdropper doing so. The secure throughput under this UFH setup is obtained as follows.

Proposition 2. (*Secure Throughput under UFH*): The secure throughput for one Tx-Rx pair and a density λ_{e} of eavesdroppers spread near the source (at distance smaller of equal than Bob) operating under UFH with N frequencies is given by

$$\mathcal{T}_{\mathrm{s}}^{ufh} = \underbrace{\frac{1}{N}}_{\mathcal{T}_{\mathrm{b}}} \times \underbrace{\exp(-\mu_{\mathrm{a,e}}/N)}_{1-\mathcal{T}_{\mathrm{e}}} \tag{3}$$

where $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \cdot \pi r_{\mathrm{a,e}}^2$.

Proof. See Appendix A. □

The left part of the expression corresponds to the throughput with UFH at Bob $\mathcal{T}_{\mathrm{b}}$, while the right part is one minus the throughput at Eve $\mathcal{T}_{\mathrm{e}}$ also operating under UFH. Note that this corresponds to a typical exponential function with value at start of $\frac{1}{N}$ and decay rate of $\mu_{\mathrm{a,e}}/N$.

Lemma 1. *Similarly to $\mathcal{T}_{\mathrm{s}}^{nojam}$ [2], the limit of the secure throughput with UFH in large density of eavesdroppers is* $\lim_{\lambda_e \to \infty} \mathcal{T}_{\mathrm{s}}^{ufh} = 0$.

A. Analysis

Although the $\mathcal{T}_{\mathrm{s}}^{ufh}$ limit for large number of eavesdroppers is 0 (the same as for $\mathcal{T}_{\mathrm{s}}^{nojam}$), looking at the results of *Figure 3* we can see that for a range of number of eavesdroppers, $\mathcal{T}_{\mathrm{s}}^{ufh}$ exceeds $\mathcal{T}_{\mathrm{s}}^{nojam}$.

Lemma 2. *The secure throughput of UFH exceeds $\mathcal{T}_{\mathrm{s}}^{nojam}$ when the expected number of eavesdroppers $\mathbb{E}\{N_{a,e}\}$ exceeds a value that is a function of the number of frequencies N,*

$$\mathbb{E}\{N_{a,e}\} > \frac{N \log(N^{-1})}{1-N}, N \geq 2.$$

Proof. Results straightforwardly from solving the inequality $\mathcal{T}_{\mathrm{s}}^{ufh} > \mathcal{T}_{\mathrm{s}}^{nojam}$, with $\mathbb{E}\{N_{\mathrm{a,e}}\} = \lambda_{\mathrm{e}} \pi r_{\mathrm{a,e}}^2$. □

This is explained by the lower decay rate ($\mu_{\mathrm{a,e}}/N$) of (3) with respect to (2), thus providing a secure throughput advantage in the presence of a larger number of eavesdroppers. This advantage is particularly relevant for intermediate values of number of eavesdroppers, where $\mathcal{T}_{\mathrm{s}}^{nojam}$ gets closer to 0, while UFH is still able to provide security. For example, with an average number of eavesdroppers of 4, the secure throughput raises from 8.9% to 18.3% with UFH.

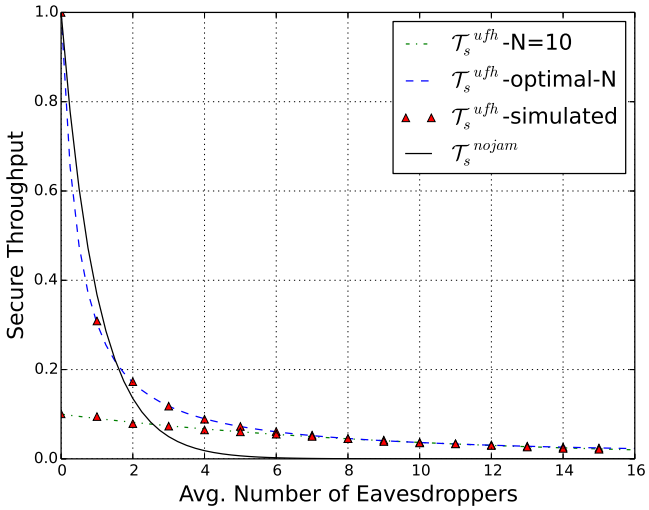

Fig. 3: Secure throughput with varying number of overhearing eavesdroppers close to the transmitter: without jamming (nojam) vs UFH. $\mathcal{T}_{\mathrm{s}}^{ufh}$-optimal-N corresponds to the case in which the number of frequencies, N, is set to the optimal value [18] (number of eavesdroppers + 1) that maximizes $\mathcal{T}_{\mathrm{s}}^{ufh}$.

If an estimate of the number of eavesdroppers is available, the number of frequencies of UFH can be adjusted accordingly to maximize the secure throughput [18]. This corresponds to the case $\mathcal{T}_{\mathrm{s}}^{ufh}$-optimal-N in *Figure 3* , where the number of frequencies is adjusted to the optimal value of $\mathbb{E}\{N_{\mathrm{a,e}}\} + 1$. However, in the more likely case of not having information about the (silent) eavesdroppers, a non-optimal UFH still provides a secrecy advantage for a large range of number of eavesdroppers, as depicted in the curve for $N = 10$.

B. UFH for secret key establishment

While the secure throughput for UFH is rather low, we argue that it can be useful for secret key establishment in adversarial setups without any added cost (nodes are only required to randomly hop through frequencies). For example, say a user expects a worst-case secure throughput of $\mathcal{T}_{\mathrm{s}}^{min} = 0.1$, meaning that, on average only 1/10 packets are secure. Without knowing which packet is secure, this information may not be very useful. However, by applying a one-way hash function over a set of packets n, if a single packet is secure from the eavesdropper, this is sufficient to generate a shared secret without knowing exactly which packet was secure. Moreover, from a secure throughput of $\mathcal{T}_{\mathrm{s}}$, one can increase the probability of having a shared secret key (at least one secure packet) by simply exchanging more packets as follows.

Lemma 3. *(Probability of having at least one secure packet): For a given secure throughout $\mathcal{T}_{\mathrm{s}}$, the probability of having at least one secure packet for n transmitted packets is given by*

$$\mathbb{P}\{\text{at least 1 secure packet}\} = 1 - (1 - \mathcal{T}_{\mathrm{s}})^n$$

and this can be made arbitrarily close to 1 with increasing number of transmissions n.

V. Jamming Receiver with Self-interference Cancellation against Non-degraded Eavesdroppers

Another dimension to explore against non-degraded eavesdroppers is that of a jamming receiver. While interference alignment is a promising approach [3] for effective jamming of eavesdroppers with reduced impact on legitimate receivers, current designs suffer from several shortcomings and limiting assumptions. For example, most works are of theoretical nature and their applicability in practical scenarios with several decentralized interferers depends on strict synchronization among devices. Moreover, an ingenious eavesdropper that is able to perform traffic analysis and better select snooping locations (e.g. on top of Alice) is hard to combat.

A more realistic practical approach is that of the legitimate receiver acting as a jammer itself, in that its knowledge of the added noise characteristics favors the cancellation of noise from the transmitted signal [15], although at the cost of added complexity. In this section, we evaluate the effect of a jamming receiver that is able to cause interference against non-degraded eavesdroppers while still listening to the transmission from the source. For that, we consider that the receiver is able to adjust its jamming transmit power P_b in order to affect a growing number of non-degraded eavesdroppers that lie in vicinity of the source.

Proposition 3. (*Secure throughput with jamming receiver*): The secure throughput for one Tx-Rx pair and a number of eavesdroppers spread near the source (at distance smaller of equal than Bob) with density λ_{e} and a jamming receiver that causes interference with power P_b is given by

$$\mathcal{T}_{\mathrm{s}}^{jamrx} = \exp\Bigg(-\lambda_{\mathrm{e}}\Big(\pi r_{\mathrm{a,e}}^2 - r_{\mathrm{a,e}}^2\cos^{-1}(d_1/r_{\mathrm{a,e}}) + d_1\sqrt{r_{\mathrm{a,e}}^2 - d_1^2} - r_{\mathrm{b,e}}^2\cos^{-1}(d_2/r_{\mathrm{b,e}}) + d2\sqrt{r_{\mathrm{b,e}}^2 - d_2^2}\Big)\Bigg) \tag{4}$$

where

$$d_1 = \frac{d_{\mathrm{a,b}}^2 - r_{\mathrm{b,e}}^2 + r_{\mathrm{a,e}}^2}{2d_{\mathrm{a,b}}}, d_2 = \frac{d_{\mathrm{a,b}}^2 + r_{\mathrm{b,e}}^2 - r_{\mathrm{a,e}}^2}{2d_{\mathrm{a,b}}},$$

$d_{\mathrm{a,b}}$ is the distance between Alice and Bob, and $r_{\mathrm{a,e}}$, $r_{\mathrm{b,e}}$ are functions of the transmit powers and receiver sensitivities as follows $r_{\mathrm{a,e}} = (P_{\mathrm{a}}/P_{\mathrm{e}}^*)^{1/b}$, $r_{\mathrm{b,e}} = (P_{\mathrm{b}}/P_{\mathrm{e}}^*)^{1/b}$.

Proof. See Appendix B. □

A. Analysis

In *Figure 4* we depict the variation of the secure throughput with growing number of eavesdroppers, for two jamming transmit powers from Bob. This shows that although the secure throughput still tends to 0 with growing number of eavesdroppers, the increase of jamming power from the receiver enables a slower decay of the secure throughput or, equivalently, the ability to support more eavesdroppers for the same desired secure throughput.

In *Figure 5* we fix a density of eavesdroppers and analyze the effect of varying the jamming power at Bob, expressed as the ratio with respect to the transmit power at Alice, P_b/P_a.

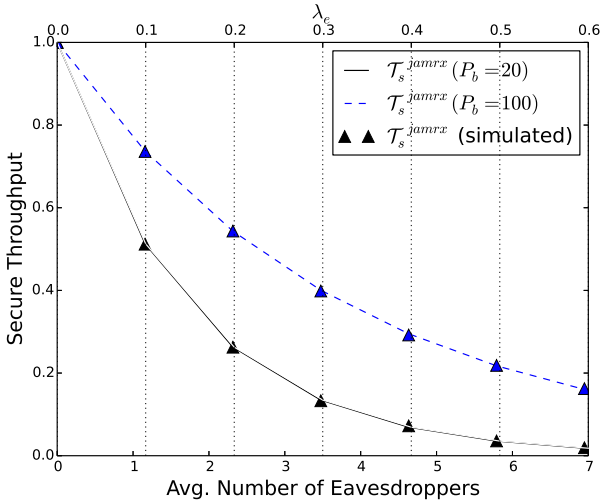

Fig. 4: Secure throughput for the jamming receiver ($jamrx$) case against varying density/average number of eavesdroppers for two levels of jamming power from Bob (P_b), and $P_a = 40$mW.

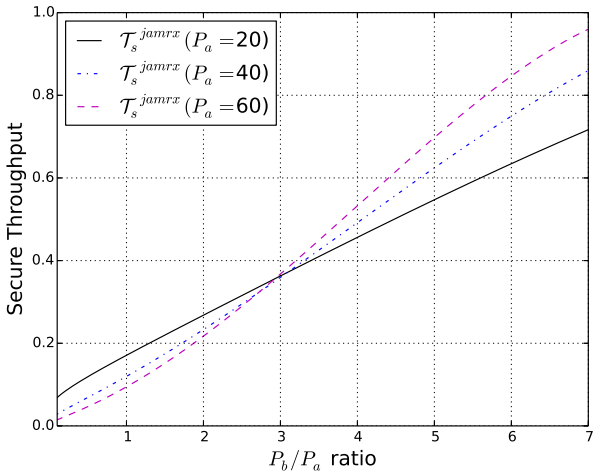

Fig. 5: Secure throughput for the jamming receiver ($jamrx$) case against varying ratio P_b/P_a of power allocation between Alice and Bob, for a density of eavesdroppers $\lambda_e = 0.4$.

Expected results show that lower transmit powers from Alice lead to higher secure throughput, at least up until the transmit power from Bob exceeds 3 times the transmit power from Alice. Naturally, this specific turnover value is a function of the distance between Alice and Bob.

These results also show that increasing the jamming power at Bob leads to a secure throughput advantage, albeit at a cost that may become prohibitively expensive: for this setup, to reach a secure throughput close to 1 for $P_a = 60$mW Bob requires 7 times more power than Alice, i.e. $P_b = 420$mW.

VI. Conclusion

We consider two schemes for physical-layer security against non-degraded eavesdroppers that, unlike the commonly considered scenario, are in advantage with respect to the legitimate receiver. These powerful adversaries call for new approaches to attain periods of advantageous communication that can be relied upon to enhance the security of the system. We characterize the secrecy level of two techniques against strong

eavesdroppers: Uncoordinated Frequency Hopping, although low-throughput, is shown suitable for secret key establishment without added costs; higher secure throughput rates can be attained through a jamming receiver with self-interference cancellation, albeit at the cost of extra transmission power.

Appendix A
Derivation of (3)

$$\begin{aligned}\mathcal{T}_{\mathrm{s}} &= \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \wedge \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &= \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \,\middle|\, \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \times \mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &= \mathbb{P}\left\{ \mathrm{a} \to \mathrm{b} \,\middle|\, \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \right\} \\ &\quad \times \sum_{n=0}^{\infty} \mathbb{P}\left\{ \bigwedge_{e_i \in \mathcal{E}} \mathrm{a} \nrightarrow e_i \,\middle|\, N_{\mathrm{a,e}} = n \right\} \cdot \mathbb{P}\{N_{\mathrm{a,e}} = n\}. \end{aligned} \quad (5)$$

Since the are no dependencies between collisions on the eavesdroppers and Bob,

$$\mathcal{T}_{\mathrm{s}} = \mathbb{P}\{\mathrm{a} \to \mathrm{b}\} \times \sum_{n=0}^{\infty} (1 - p_{\mathrm{a,e}})^n \cdot \mathbb{P}\{N_{\mathrm{a,e}} = n\}, \quad (6)$$

where $p_{\mathrm{a,e}} \triangleq \mathbb{P}\{\mathrm{a} \to e_i |\, N_{\mathrm{a,e}} = n\}$.

Under UFH, Alice and Bob can only communicate when landing on the same frequency out of the N frequencies available and, thus, $\mathcal{T}_{\mathrm{b}} = \mathbb{P}\{\mathrm{a} \to \mathrm{b}\} = \frac{1}{N}$.

Since $N_{\mathrm{a,e}}$ is a Poisson RV with mean $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \cdot \pi r_{\mathrm{a,e}}^2$, the summation in (6) gives [19, Appendix A]:

$$\sum_{n=0}^{\infty} (1 - p_{\mathrm{a,e}})^n \cdot \mathbb{P}\{N_{\mathrm{a,e}} = n\} = \exp\left(-\mu_{\mathrm{a,e}} \cdot p_{\mathrm{a,e}}\right), \quad (7)$$

where $p_{\mathrm{a,e}}$ is the probability of communication between Alice and an eavesdropper. Under UFH, this is the probability of Eve lying in the same frequency as Alice, $p_{\mathrm{a,e}} = \frac{1}{N}$.

This concludes the proof.

Appendix B
Derivation of (4)

From (6) and (7), we have that

$$\mathcal{T}_{\mathrm{s}} = \mathbb{P}\{\mathrm{a} \to \mathrm{b}\} \cdot \exp\left(-\mu_{\mathrm{a,e}} \cdot p_{\mathrm{a,e}}\right), \quad (8)$$

with $\mu_{\mathrm{a,e}} = \lambda_{\mathrm{e}} \cdot \pi r_{\mathrm{a,e}}^2$ and $p_{\mathrm{a,e}} \triangleq \mathbb{P}\{\mathrm{a} \to e_i |\, N_{\mathrm{a,e}} = n\}$.

Since Bob is within communication range of Alice and we assume that it is able to perform self-interference cancellation [15], $\mathbb{P}\{\mathrm{a} \to \mathrm{b}\} = 1$. The eavesdroppers are able to overhear Alice if they lie in the region $\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})$ without suffering interference from the jamming receiver (i.e. outside the region $\mathcal{B}_{x_{\mathrm{b}}}(r_{\mathrm{b,e}})$). In that case, we have

$$p_{\mathrm{a,e}} = \frac{\mathbb{A}\{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \backslash \mathcal{B}_{x_{\mathrm{b}}}(r_{\mathrm{b,e}})\}}{\mathbb{A}\{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})\}} = 1 - \frac{\mathbb{A}\{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \cap \mathcal{B}_{x_{\mathrm{b}}}(r_{\mathrm{b,e}})\}}{\mathbb{A}\{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})\}}.$$

Applying the formula for the area of a circular segment of radius r and triangular height d,

$$\mathbb{A}(r, d) = r^2 \cos^{-1}(d/r) - d\sqrt{r - d^2}.$$

for the both circular segments that compose $\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \cap \mathcal{B}_{x_{\mathrm{b}}}(r_{\mathrm{b,e}})$, we get

$$\mathbb{A}\{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}}) \cap \mathcal{B}_{x_{\mathrm{b}}}(r_{\mathrm{b,e}})\} = \mathbb{A}(r_{\mathrm{a,e}}, d_1) + \mathbb{A}(r_{\mathrm{b,e}}, d_2),$$

where $d_1 = \dfrac{d_{\mathrm{a,b}}^2 - r_{\mathrm{b,e}}^2 + r_{\mathrm{a,e}}^2}{2d_{\mathrm{a,b}}}$, $d_2 = \dfrac{d_{\mathrm{a,b}}^2 + r_{\mathrm{b,e}}^2 - r_{\mathrm{a,e}}^2}{2d_{\mathrm{a,b}}}$, $\mathbb{A}\{\mathcal{B}_{x_{\mathrm{a}}}(r_{\mathrm{a,e}})\} = \pi r_{\mathrm{a,e}}^2$, and the result follows.

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based Jamming for Enhanced Wireless Secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, September 2011.

[3] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1568–1571, 2013.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[5] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," *Mobile Networks and Applications*, vol. 19, no. 1, pp. 45–60, February 2014.

[6] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *IEEE Conference on Computer Communications (INFOCOM)*, Miami, USA, 2005, pp. 1940–1951.

[7] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[8] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *IEEE International Symposium on Information Theory*, July 2009, pp. 2442–2446.

[9] ——, "Secure communication in stochastic wireless networks—part ii: Maximum rate and collusion," *IEEE Transactions on Inf. Forensics and Security*, vol. 7, no. 1, pp. 139–147, February 2012.

[10] ——, "Physical layer security in stochastic wireless networks," in *IEEE Int. Conf. on Communication Systems*, November 2008, pp. 974–979.

[11] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in mimo wiretap channel," in *Proc. IEEE ICASSP*, March 2012, pp. 2809–2812.

[12] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and harq for the awgn wire-tap channel: A security gap analysis," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883–894, 2012.

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

[14] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/ region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, October 2012.

[15] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, October 2013.

[16] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, April 2011.

[17] C. Pöpper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, June 2010.

[18] J. S. Sousa and J. P. Vilela, "A characterization of uncoordinated frequency hopping for wireless secrecy," in *IEEE/IFIP Wireless and Mobile Networking Conference*, Vilamoura, Portugal, May 2014.

[19] P. C. Pinto and M. Z. 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.