Uncoordinated Frequency Hopping for Wireless Secrecy Against Non-degraded Eavesdroppers

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

***Abstract*— Current physical-layer security techniques typically 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 consider employing a spread spectrum uncoordinated frequency hopping scheme aided by friendly jammers for improved secrecy. We characterize the secrecy level of this spread spectrum scheme, by devising a stochastic geometry mathematical model to assess the secure packet throughput (probability of secure communication) of devices operating under Uncoordinated Frequency Hopping that accommodates the impact of friendly jammers. We further implement and evaluate these techniques in a real-world test-bed of software-defined radios. Results show that although Uncoordinated Frequency Hopping with jamming leads to low secure packet throughput values, by exploiting frequency diversity these methods may be used for establishing secret keys. We propose a method for secret-key establishment that builds on the advantage provided by Uncoordinated Frequency Hopping and jamming to establish secret-keys, notably against non-degraded adversary eavesdroppers that may appear in advantageous situations.**

Keywords — physical layer security, non-degraded eavesdroppers, jamming, uncoordinated frequency hopping, secret-key agreement.

I. Introduction

Physical-layer security has its roots in a contribution by Wyner [1] that showed in 1975 that there exist codes (wiretap codes) simultaneously guaranteeing reliable communication to the receiver and secrecy against the adversary eavesdropper (Eve). Wyner's work was based on the assumption of Eve observing a degraded version of the information being transmitted. Recent works on physical-layer security [2] show that the physical characteristics of wireless channels can be used to enhance the secrecy level of these networks. These works typically assume that Eve 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 [3] that can possibly be removed at the legitimate receiver [4], or (c) using relays to improve the quality of information available at the receiver [5]. 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 [6], 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 [7], 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 packet throughput* (i.e. probability of a transmission being received by the legitimate receiver without being received by any eavesdropper) with increased number of eavesdroppers [8].

A. Physical-layer Security with Non-degraded Eavesdroppers

A substantial body of literature focus on so called *cooperative jamming* [9] to warrant some advantage over eavesdroppers. This security mechanism tries to combat eavesdroppers by combining the efforts of external helpers, jammers, in order to enhance the system's security level. Jammers are in this sense friendly, although they can also harm legitimate communication and must, therefore, be chosen/activated with care [3].

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). A few articles consider enhanced eavesdroppers and analyze their impact on secure communication. For example, without jammers, the effect of colluding eavesdroppers [10] 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 [11] using secrecy graphs [12] 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 [13]. In this case, each eavesdropper

This work was partially funded through project PTDC/EEI-TEL/3684/2014 (SWING2 - Securing Wireless Networks with Coding and Jamming), a project co-funded by COMPETE 2020, Portugal 2020 - Programa Operacional Competitividade e Internacionalização (POCI), European Union through Fundo Europeu de Desenvolvimento Regional (FEDER) and Fundação para a Ciência e Tecnologia (FCT).

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.

Under this challenging setup of non-degraded eavesdroppers, most of current physical-layer security techniques become hard to administer and new dimensions to establish advantageous periods of communication are needed. This calls for new approaches for physical-layer security, such as using channel characteristics to perform secret-key agreement and exploring diversity on the frequency domain.

B. Uncoordinated Frequency Hopping

Uncoordinated Frequency Hopping (UFH) [14], [15] enables communication between transmitter and receiver through a set of randomly chosen frequency channels unknown to the receiver. Both nodes randomly and independently hop between a set of frequencies, briefly transmitting chunks of data that are exchanged successfully when both of them land in the same channel. Since adversaries are unaware of the random hopping sequence, this enables adversary-free periods of communication whenever the transmitter and receiver lie in the same frequency without the adversary doing so. This scheme acts, in some way, like regular FH, although it tries to offer a key-independent service (no previous hopping scheme is established between nodes). This leads to a significant reduction of the average throughput and, consequently, significantly decreases its performance at the benefit of adversarial-free information exchange. Originally thought out for protection against DoS jammers, these periods of adversary-free communication can then be used for exchanging a secret key or a hopping sequence for regular FH communication, with higher performance levels.

The randomness associated with UFH, and the fact that it does not entail any pre-established sequences, makes it a good choice for also improving secrecy of wireless communications, most notably when combined with jamming for secret-key exchange in setups where an eavesdropper may have an advantage (e.g. a better location/signal quality).

C. Physical-layer Secret-key Generation

Physical-layer secret-key generation exploits wireless channel characteristics such as reciprocity and inherent randomness to derive shared secret keys. This process typically includes the following steps [16]: channel probing, randomness extraction, quantization, reconciliation, and privacy amplification.

1) Channel probing consists on collecting channel measurements, such as channel state information (CSI) and received signal strength (RSS), from probes that are exchanged between legitimate devices. These devices are expected to observe highly correlated signals due to channel reciprocity;
2) Randomness extraction retrieves information from the exchanged signals that may be used to generate shared keys. This step usually disregards large-scale components that may be easily determined by the attacker;
3) Quantization is the process that transforms the extracted signal measurements into a stream of bits;
4) Information reconciliation is performed to ensure that the keys generated at both legitimate sides are identical. Although they are expected to be highly similar, differences can occur due to imperfect channel reciprocity and/or channel measurements. In this process error correction parity-bit information is usually exchanged, thus possibily leaking some information to the adversary eavesdropper;
5) The privacy amplification phase aims to reduce/eliminate the partial information that Eve is able to obtain by overhearing information in the channel probing and reconciliation stages. The choice usually lies in an universal hash function to compress the information exchanged by legitimate devices, thus reducing the correlation with Eve's obtained information.

Typical measures for secret-key generation are the secret key rate and capacity, as well as statistical measures such as the bit mismatch rate (BMR). The secret key rate and its capacity supremum is obtained from the mutual information between legitimate devices given Eve's observation [17], while BMR measures the bit mismatch between the two sequences generated at the legitimate devices. A major challenge in this process is measuring the information leaked to passive eavesdroppers that provide no sign/information on their presence.

In this work, we consider the joint use of UFH and jamming for secrecy against non-degraded eavesdropper adversaries that may overhear communication from advantageous situations. In this case, the aforementioned physical-layer secret-key generation approaches do not apply because eavesdroppers may observe highly correlated versions of the exchanged information, even if located at a distance greater than the commonly assumed half-wavelength [18]. For that, we explore different approaches based on frequency hopping and jamming to establish periods of advantageous communication for secret-key generation against non-degraded eavesdroppers.

In particular, resorting to a spatial stochastic model, we characterize the level of secrecy provided by UFH against adversary eavesdroppers spread out in space. We also consider the use of jammer devices to further enhance the secrecy level provided by UFH alone. We show that it is possible to optimize the secrecy level by adjusting the number of frequencies employed and demonstrate the practical benefits of UFH and jamming for secrecy by implementing and evaluating these schemes in a real-world software-defined radio test-bed. Finally, we propose a secret-key agreement mechanism that builds on the advantage provided by UFH and jamming against a non-degraded adversary, to exchange a key that can then be used to secure regular communication without the inherently low rates of UFH.

Part of this work was presented in [19], [20], where we characterize the secrecy level of UFH and jamming resorting to a much simpler combinatorial model that does not consider propagation phenomena, and [21] where the secrecy level of UFH alone (without jamming) is characterized resorting to a simplified spatial stochastic model where devices are considered within range if they are at a given distance from the receiver (unit-disk alike). The work presented here considers a more realistic spatial stochastic model for both UFH and jamming based on the signal-to-interference-plus-noise ratio (SINR) concept, implements and evaluates these schemes in a real-world testbed, and further proposes a secret key agreement mechanism.

II. Secure Packet Throughput of UFH with Jamming

In this section, we characterize the secure packet throughput (probability of secure communication) of communication under UFH. For that, we consider a spatial stochastic network model based on the SINR concept, that takes into account all the essential physical parameters that affect the aggregate interference by adding stochastic geometry to account for the randomness of both eavesdroppers' and jammers' locations, as well as their arbitrary number.

The SINR model represents interference, whether originated from other devices (e.g. jammers) or from propagation effects (e.g. path loss), based on the following signal quality formula.

$$SINR = \frac{S}{I + N_x}, \tag{1}$$

where S is the received power, N_x is the constant noise power, and I is the aggregate interference power that captures the impact from jammers/interferers. This model can be used to determine the throughput, $\mathcal{T}$, of a link that is affected by interference from multiple devices as [22]: $\mathcal{T} = \mathbb{P}\{SINR \geq \theta^*\}$, where θ^* is a predetermined threshold that ensures reliable reception (i.e. related to the sensitivity of the receiver). The inlaid structure of this model was proposed by Win et al. [22], but multiple changes/extensions were made to model our setup. In particular, our model considers communication under the UFH paradigm, as well as the coexistence of the legitimate receiver with multiple other receivers (eavesdroppers) in a network with interfering devices (jammers). For that, we consider the notion of secure packet throughput

Definition 1 (Secure Packet Throughput)**.** *The secure packet throughput from the transmitter Tx to the receiver Rx is the probability of Rx receiving the message from Tx (Tx→Rx) without any eavesdropper e_i doing so,*

$$\mathcal{T}_s \triangleq \mathbb{P}\left\{ Tx \rightarrow Rx \wedge \bigwedge_{e_i} Tx \nrightarrow e_i \right\}. \tag{2}$$

This metric admits an outage interpretation. In fact, it measures the probability that (1) the system is not in outage to the legitimate receiver *Rx*, and (2) the system is in outage to all possible eavesdroppers.

The notation and symbols used throughout this section are summarized in Table I. The concept of reception of a message (*Tx→Rx*) according to the SINR level will be clearly defined in Section II-C.

Symbol	Usage
$\mathbb{E}\{\cdot\}$	Expectation operator
$\mathbb{P}\{\cdot\}$	Probability operator
$F(\cdot)$	CDF operator
$\Gamma(\cdot)$	Gamma function operator
$b, 2b$	Amplitude/Power loss exponent
θ^*	SINR threshold
$\Pi_e = \{e_i\}, \Pi_j = \{j_i\}$	Poisson processes of eavesdroppers and jammers
λ_e, λ_j	Spatial densities of eavesdroppers and jammers
P_{tx}, P_I	Transmit power of transmitter and jammers
r_0, r_e	Pair-wise distances between $Tx - Rx$ and $Tx - e_i$
$r_{tx,e}$	Radius of the circle around the transmitter
N_e	Expected number of eavesdroppers
N	Available number of frequencies
N_x	Constant noise power
$\mathcal{B}_x(\rho)$	Ball centered at x with radius ρ
$\mathcal{T}_s$	secure packet throughput
$\mathcal{T}_{rx}$,$\mathcal{T}_e$	Throughput at *Rx* and Eve, respectively
$\mathcal{T}'_e$	Reverse throughput at Eve ($\mathcal{T}'_e = 1 - \mathcal{T}_e$)
μ_e	Average # of eavesdroppers inside $\mathcal{B}_{tx}(r_{tx,e})$

TABLE I: Notation and Symbols.

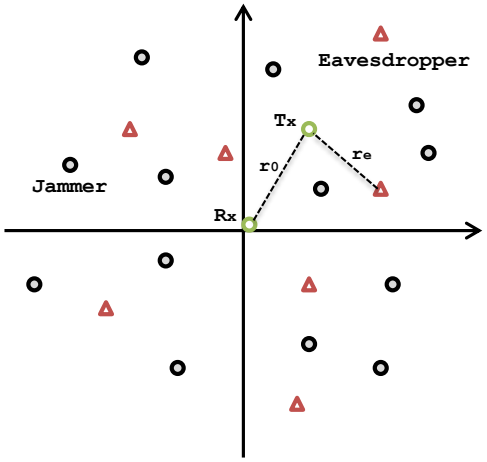

Fig. 1: Transmitter and receiver communicate in the presence of eavesdroppers (triangles) and jammer defenders (circles), which are randomly distributed according to homogeneous Poisson point processes with different spatial densities.

A. System and Attacker Model

We consider the following scenario depicted in Figure 1, where a legitimate user - transmitter (*Tx*) - tries to communicate with another user - receiver (*Rx*) - without a set of eavesdroppers having access to transmitted messages. With the aim of improving the secrecy of communication, multiple jammers can transmit in cooperation with legitimate devices.

Without loss of generality, *Tx* is placed deterministically anywhere on the two-dimensional plane, while *Rx* is located at the origin (at distance r_0 from *Tx*). The set of eavesdroppers

is $\Pi_e = \{e_i\} \subset \mathbb{R}^2$, with the set of jammers represented by $\Pi_j = \{j_i\} \subset \mathbb{R}^2$.

The spatial location of nodes can be modeled either deterministically or stochastically. In many cases, node positions are unknown to the network designer a priori, so they may be treated as completely random (uniform) according a Poisson Point Process (PPP) [23]. Thus, both eavesdroppers and jammers are spatially distributed according to a homogeneous PPP on $\mathbb{R}^2$ with spatial densities λ_e and λ_j, respectively. This way, results are averaged over many possible spatial realizations, providing a measure of the system that encompasses both favorable setups (e.g. jammers on top of eavesdroppers), as well as unfavorable situations (e.g. eavesdroppers without interference very close to the source).

The transmitter and receiver employ UFH as their multiple-access technique, attempting to evade eavesdroppers by randomly jumping among frequencies. The remaining terminals (jammers and eavesdroppers) hop between frequencies uniformly at random as well, as they try to protect or overhear the communication. Adversary eavesdroppers hop between frequencies at the same rate as the remaining devices. If eavesdroppers could hop between frequencies much faster than other devices, this would allow them to rapidly detect legitimate communication on a given frequency and remain on that frequency overhearing communication until the *Tx* jumps to another frequency. However, the same kind of reasoning can be applied to jammers, in the sense that if jammers were able to hop between frequencies much faster this would allow them to affect eavesdroppers more frequently with corresponding security benefits.

1) Non-degraded eavesdroppers: We consider non-degraded eavesdroppers, that possess equal or better capabilities (e.g. number of antennas, location) than legitimate receivers. In this work, that is modeled in two ways:

a) on the simulations, non-degraded eavesdroppers correspond to the case in which the number/density of eavesdroppers surpasses the number/density of available defensive jammers, thus increasing the probability that eavesdroppers are able to overhear communication (i.e. lie in the same frequency as *Rx* without suffering interference from jammers);
b) on the test-bed evaluation, since we are limited in terms of number of eavesdroppers to deploy, a non-degraded eavesdropper corresponds to the situation in which the eavesdropper is closer to the transmitter than the legitimate receiver.

2) Jamming for secrecy: We consider the presence of jammers that cause interference (extra additive white Gaussian noise) with transmit power P_I. Jammers hop between frequencies at the same rate as all other devices, and cause interference during their stay in a given channel/frequency. While there exist synchronization mechanisms to reduce the negative effect of jammers on legitimate communication [3], that is out of scope for this work. In that sense, jammers can cause interference to eavesdroppers as well as legitimate receivers. Our goal here is to assess the benefit of the joint effect of uncoordinated frequency hopping and jamming for secrecy, without the need for tight synchronization.

B. Wireless Propagation and Interference

We consider that the power P_x received at distance r from the transmitter is given by

$$P_x = \frac{P_{tx} \prod_k Z_k}{r^{2b}} \tag{3}$$

where P_{tx} is the transmission power, b is the amplitude loss exponent, r is the distance between source and destination and Z_k is a random variable (r.v.) that can represent the different propagation effects that influence communication (e.g. shadowing and multipath fading). Far-field path loss is modeled by means of the term $1/r^{2b}$, that accounts for the loss of signal-power as it travels through the medium and is related with the distance between source and destination, as well as the other environmental dependent aspects hereby represented by the amplitude loss exponent b. For ease of analysis, we consider the effect of pathloss only (i.e. $\prod_k Z_k = 1$). While some works [22] do consider the effect of channel fading with stochastic geometry, they do so in a simpler scenario without randomly located eavesdroppers. The addition of eavesdroppers that, unlike the fixed receiver in [22], are randomly distributed in space makes the problem more difficult with respect to the characterization of interference of randomly located jammers over also randomly located eavesdroppers (Proposition 1), thus making it hard to obtain closed-form expressions and provide meaningful insights. We do, however, complement these results with a real-world testbed implementation and evaluation in Section III, which naturally encompasses all propagation phenomena of wireless networks.

Relating this to the SINR concept in (1), we have

$$S = \frac{P_{tx}}{r^{2b}} \tag{4}$$

where P_{tx} is the transmitter power and r is the distance between source and destination. For *Rx*, r has the deterministic value of r_0 (see Figure 1), while for the eavesdroppers, r is a random value (R_e) because of the stochastic distribution in space of these devices. Similarly, I can be written as

$$I = \sum_{i=1}^{\infty} \frac{P_I}{{R_i}^{2b}} \tag{5}$$

where R_i is the distance between interferer and receiver, and P_I is the interference power of all interferers/jammers (considered the same for all jammers). Since jammers' positions are random (spatially distributed by a PPP), R_i is a r.v. and, consequently, so is I. This is valid for both receiver and eavesdroppers.

For the static legitimate receiver, the interference can be characterized [22] as a *skewed stable distribution* - $\mathcal{S}$ - with parameters α, β, γ.

$$I \sim \mathcal{S}\left(\alpha = \frac{1}{b}, \beta = 1, \gamma = \frac{\pi \lambda_j \Gamma(2-\alpha) \cos\left(\frac{\pi\alpha}{2}\right) P_I^{\frac{1}{b}}}{1-\alpha}\right) \tag{6}$$

where Γ denotes the gamma function. This then allows us to

determine the throughput as $\mathcal{T} = \mathbb{P}\{SINR \geq \theta^*\}$, where θ^* is the reception sensitivity threshold at *Rx*.

To expand this formulation for our setup, we need to (1) incorporate the effect of randomly hopping through frequencies of UFH, and (2) characterize the interference distribution to eavesdroppers that, unlike the legitimate receiver, are randomly distributed in space so that (6) does not apply.

To model the effect of UFH, we have to account for the fact that channel hopping jammers do not continuously affect a given receiver (*Rx* or Eve). Therefore, only a set of these may actually be interfering with the devices at a given time. The effect of UFH can be added to (6) by considering the splitting property of Poisson processes [23], so that the effective density of jammers is scaled down by the probability p_i of a jammer landing on the communication frequency as follows

$$I \sim \mathcal{S}\left(\alpha = \frac{1}{b}, \beta = 1, \gamma = \frac{\pi\lambda_j p_i \Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right) P_I^{\frac{1}{b}}}{1-\alpha}\right) \quad (7)$$

where $p_i = 1/N$, with N the number of available frequencies. We now proceed to the characterization of interference for randomly deployed eavesdroppers, which will allow us to determine the secure packet throughput according to (2).

C. Secure Packet Throughput

The secure packet throughput under UFH corresponds to the probability that a packet from *Tx* is successfully received by *Rx*, without being received by any eavesdropper. This happens if *Tx* and *Rx* land in the same frequency, and *Rx* is not in outage, i.e. its SINR exceeds a given threshold. For eavesdroppers to be incapable of overhearing legitimate communication, they have to either land on different frequencies, or suffer from a low SINR. The secure packet throughput is then affected by the density of jammers and eavesdroppers, the power of *Tx* and jammers, and the number of available frequencies as presented in Proposition 1.

The upcoming Proposition 1, relies on the following results and assumptions.

- The stable variable I that represents the interference power of all jammers has a set of parametrizations that we can chose from, that allows us to clearly define this variable's density and distribution functions [24]. Given the proximity with our characteristic function, we chose one of Levy's stable distribution parametrizations with $\alpha = \frac{1}{2},\ \beta = 1$, thus corresponding to a typical power loss exponent of $2b = 4$;
- The probability of *Rx* receiving the message from *Tx* (*Tx* $\rightarrow$ *Rx*) comes from the SINR concept and interference representation, such that [22]

$$\mathbb{P}\{Tx \rightarrow Rx\} = F_I\left(\frac{P_{tx}}{r^{2b}\theta^*} - N_x\right) \quad (8)$$

with $F_I(x)$[1] being the CDF of I, and r being the distance r_0 between *Tx* and *Rx*;

- We restrict the spatial distribution of the eavesdroppers inside a specific region, a circle, $\mathcal{B}$, around the transmitter - $\Pi_e \cap \mathcal{B}_{tx}(r_{tx,e})$. If we consider a large enough area, we can have a perfect approximation for the secure packet throughput, even if we have eavesdroppers placed outside this circle's borders. To do that, we adjust the radius of the circle to accommodate eavesdroppers that can overhear communication (those such that SINR$\geq$ θ^*). From $\mathbb{P}\{Tx \rightarrow Rx\} = F_I(x)$, we can determine an upper-bound for the radius when $x = 0$, i.e. $r_{tx,e} = \left(\frac{P_{tx}}{N_x\theta^*}\right)^{\frac{1}{2b}}$, where r in (8) represents the distance between *Tx* and eavesdropper, i.e. the r.v. R_e.

Proposition 1. The secure packet throughput for a setup with one *Tx*-*Rx* pair deterministically located in $\mathbb{R}^2$ hopping uniformly at random through N frequencies and with a set of eavesdroppers, $\Pi_e = \{e_i\} \subset \mathbb{R}^2$, and jammers, $\Pi_j = \{j_i\} \subset \mathbb{R}^2$ spatially distributed according to a PPP with densities λ_e and λ_j respectively, is given by

$$\mathcal{T}_s = \frac{1}{N} F_I\left(\frac{P_{tx}}{r_0^{2b}\theta^*} - N_x\right) \times \exp\left(-\frac{2\pi\lambda_e}{N}\int_0^{r_{tx,e}} F_I\left(\frac{P_{tx}}{r_e^{2b}\theta^*} - N_x\right) r_e \, \mathrm{d}r_e\right) \quad (9)$$

with

$$I \sim \mathcal{S}\left(\alpha = \frac{1}{b}, \beta = 1, \gamma = \frac{\frac{\pi\lambda_j}{N}\Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right) P_I^{\frac{1}{b}}}{1-\alpha}\right) \quad (10)$$

where F_I (characterized as mentioned in the assumptions) represents the cumulative distribution function (cdf) of the stable variable I, r_e is the distance between the transmitter and each eavesdropper and $r_{tx,e}$ is the radius of a sphere centered over the transmitter where eavesdroppers are able to overhear, determined as mentioned in the assumptions.

Proof: From the definition of secure packet throughput, and considering N_e as the number of eavesdroppers, $\#\Pi_e$, we can write

$$\mathcal{T}_s = \mathbb{P}\left\{Tx \rightarrow Rx \wedge \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} = \mathbb{P}\left\{Tx \rightarrow Rx \,\middle|\, \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} \times \mathbb{P}\left\{\bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\}$$

From the law of total probability[2], we have

$$\mathcal{T}_s = \mathbb{P}\left\{Tx \rightarrow Rx \,\middle|\, \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} \times \sum_{n=0}^{\infty} \mathbb{P}\left\{\bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i \,\middle|\, N_e = n\right\} \cdot \mathbb{P}\{N_e = n\} \quad (11)$$

We now make two approximations whose validity we will evaluate in Section II-D: i) the event $\{Tx \rightarrow Rx\}$ is indepen-

[1] $F_I(x) = \begin{cases} 0 & x < 0 \\ y & 0 \leq x < 1 \\ 1 & x \geq 1 \end{cases}$, y depends on the distribution of r.v. I

[2] $\mathbb{P}\{A\} = \mathbb{E}_X\{\mathbb{P}\{A|X\}\} = \sum_x \mathbb{P}\{A|x\} \times \mathbb{P}(x)$.

dent of $\left\{\bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\}$; and ii) the events $\{Tx \nrightarrow e_i | N_e = n\}$ are independent identically distributed (IID) for different i. Then, (11) becomes

$$\mathcal{T}_s \approx \mathbb{P}\{Tx \rightarrow Rx\} \times \sum_{n=0}^{\infty} (1-\omega)^n \cdot \mathbb{P}\{N_e = n\} \qquad (12)$$

where $\omega = \mathbb{P}\{Tx \rightarrow e_i | N_e = n\}$, with $\mathbb{P}\{Tx \rightarrow Rx\}$ defined as in (8).

Knowing that the number of eavesdroppers, N_e inside circle $\mathcal{B}$ is a Poisson random variable with mean $\mu_e = \lambda_e \pi r_{tx,e}^2$ [25], we have $\mathbb{P}\{N_e = n\} = \frac{\mu_e^n}{n!} e^{-\mu_e}$, and the summation in (12) can be expressed as,

$$\begin{aligned}\sum_{n=0}^{\infty} (1-\omega)^n \cdot \mathbb{P}\{N_e = n\} &= \sum_{n=0}^{\infty} (1-\omega)^n \cdot \frac{\mu_e^n e^{-\mu_e}}{n!} \\ &= e^{-\mu_e} e^{\mu_e (1-\omega)} \underbrace{\sum_{n=0}^{\infty} \frac{(\mu_e (1-\omega))^n e^{-\mu_e (1-\omega)}}{n!}}_{=1} \\ &= \exp\left(-\mu_e \cdot \omega\right). \qquad (13)\end{aligned}$$

Finally, we conclude our proof by working out $\omega = \mathbb{P}\{Tx \rightarrow e_i | N_e = n\}$ – the probability that an eavesdropper is not in outage, i.e. able to receive the message by having a large enough SINR. Note that we have to take into account the possible position of each eavesdropper and correspondent distance to the transmitter R_e, which is a r.v.. By assuming that each of these distances are independent from one another[3], we can calculate its expected value, $\mathbb{E}$, from the law of total probability as follows,

$$\omega = \mathbb{E}_{R_e}\{\omega | R_e\}.$$

From (8), this is equivalent to

$$\omega = \mathbb{E}_{R_e}\left\{F_I\left(\frac{P_{tx}}{R_e^{2b}\theta^*} - N_x\right)\right\},$$

which, from the expectation value of a function[4], leads to

$$\omega = \frac{2}{r_{tx,e}^2} \int_0^{r_{tx,e}} F_I\left(\frac{P_{tx}}{r_e^{2b}\theta^*} - N_x\right) r_e \, \mathrm{d}r_e. \qquad (14)$$

□

D. Evaluation

We now assess the secrecy impact of UFH with and without jamming. We start by placing a transmitter and receiver distanced one unit/meter away from each other (i.e. $(x_{tx}, y_{tx}) = (0,0)$ and $(x_{rx}, y_{rx}) = (0,1)$), as well as a random set of jammers and eavesdroppers on a circular region centered on the origin with a radius of $L = 4$ meters, which represents the boundaries of the simulation space.

[3]Property of PPP: for a fixed region and fixed number of nodes (in this case $N_e = n$), the location of nodes/eavesdroppers is independent.

[4]Expectation value of a function: $\mathbb{E}_x(f(x)) = \int f(x) pdf(x) \, \mathrm{d}x$; probability density function (pdf) of the distances between the eavesdropper and the transmitter is given by: $pdf(x) = \frac{2r_e}{r_{tx,e}^2}$.

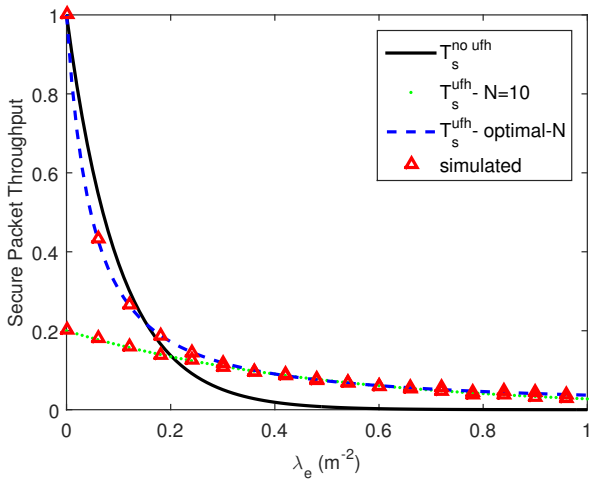

Fig. 2: Comparison of strategies for varying λ_e (no UFH, optimal UFH, UFH with 10 frequency channels). Values used also in the remaining plots of this section are $P_{tx} = P_I = 40$mW, constant noise power $N_x = 4$mW and SINR threshold $\theta^* = 1$. So as not to overwhelm the plot, the triangles correspond to the simulated values for the curve/scenario on top of which they appear.

The number of devices is picked at random from a Poisson distribution (mean $= \lambda \pi L^2$) and each of them is placed uniformly at random in the circle. Knowing that a node can successfully communicate if $\mathbb{P}\{SINR \geq \theta^*\}$, we determine the secure packet throughput by averaging over 10000 repetitions, with different spatial realizations[5]. We compare these simulated results with our analytical results for the secure packet throughput in (9), showing that the analytical results match with the simulated ones. So as not to overhelm the plots, the triangles correspond to the simulated values for the simulation case of the curve on top of which they appear.

1) UFH-only ($\lambda_j = 0$): Figure 2 depicts the secure packet throughput (y-axis) for varying density of overhearing eavesdroppers (x-axis) with and without UFH. This plot shows us that for densities of eavesdroppers, above ~ 0.2, UFH can provide a positive secure packet throughput, while the secure packet throughput without UFH rapidly tends to 0. This happens because UFH adds diversity to the system by providing frequency channels where *Tx-Rx* can possibly communicate without an eavesdropper being able to overhear, which would otherwise not happen if only a single channel was available. Note that the secure packet throughput of UFH also decreases with the density of eavesdroppers, albeit at a lower pace than for the case without UFH. UFH then provides a relevant advantage when compared to the single frequency case, specially against *non-degraded eavesdroppers* with high density/number of devices in the network.
If an estimate of the number of eavesdroppers is available, the number of frequencies can be adjusted accordingly to

[5]This will encompass both favorable setups (e.g. jammers on top of eavesdroppers), as well as unfavorable situations (e.g. eavesdroppers without interference very close to the source).

maximize the secure packet throughput. This corresponds to the case $\mathcal{T}_s^{ufh}$-optimal-N, where the number of frequencies is adjusted to the optimal value [19] of $\#\Pi_e + 1$. However, in the more likely case of not having information about the eavesdroppers, a non-optimal UFH (in this case $\mathcal{T}_s^{ufh}$-N=10) still provides a secrecy advantage for a large range of number/density of eavesdroppers.

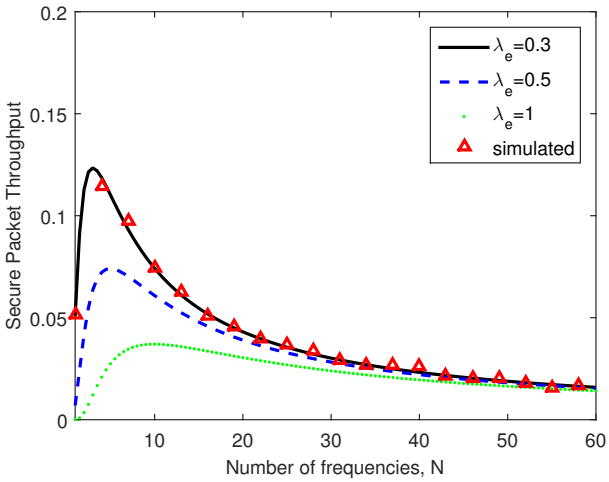

Fig. 3: secure packet throughput (T_s) with UFH versus the number of available frequencies, for various eavesdroppers' spatial densities, $\lambda_e = 0.3$, $\lambda_e = 0.5$ and $\lambda_e = 1$.

In Figure 3 we vary instead the number of frequencies (x-axis) for three different densities of eavesdroppers. This graph highlights the fact that the number of frequencies can be adjusted to improve the secure packet throughput [19]. Note that the secure packet throughput first increases and then decreases. This happens because the secure packet throughput in (2) is a function of the throughput to *Rx* and the throughput to Eve. At first the secure packet throughput increases as more frequencies will reduce the probability of eavesdroppers overhearing information, and then decreases as a result of a greater loss of throughput to Rx, that surpasses the beneficial effect over Eve. We can also see that for different numbers/densities of eavesdroppers, the maximum can be obtained through a reasonable number of employed frequencies, irrespectively of the density of eavesdroppers.

2) UFH+Jamming: In Figure 4 we consider the joint effect of UFH and jammers that are available to cause interference to eavesdroppers, but can also, as consequence, cause interference to the legitimate receiver. This plot shows that jammers with different densities ($\lambda_j = \{0.2, 0.6\}$) can improve the secure packet throughput when compared to the case without jamming after a certain density of adversary eavesdroppers, $\lambda_e \sim 0.24$ for $\lambda_j = 0.2$, and $\lambda_e \sim 0.42$ for $\lambda_j = 0.6$. Below these densities of eavesdroppers, jamming is harmful and actually reduces the secure packet throughput when compared to the case without jammers. This is expected because with fewer eavesdroppers, jammers can harm the legitimate receiver more than eavesdroppers, thus showing the need to adjust the

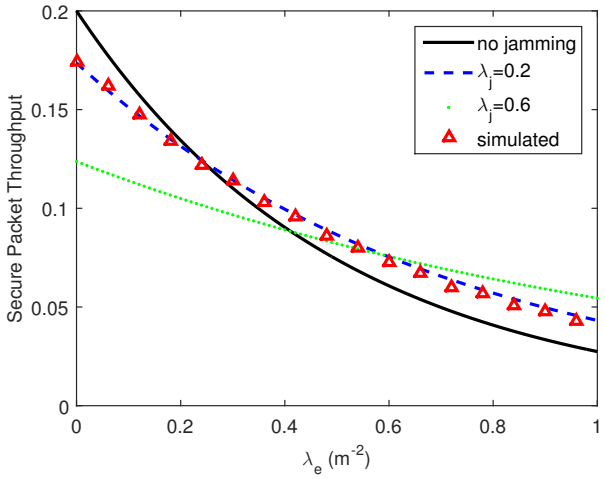

Fig. 4: secure packet throughput with UFH ($N = 5$ available frequencies) for varying density of eavesdroppers λ_e with jammers ($\lambda_j = \{0.2, 0.6\}$) and without jammers (no jamming, $\lambda_j = 0$).

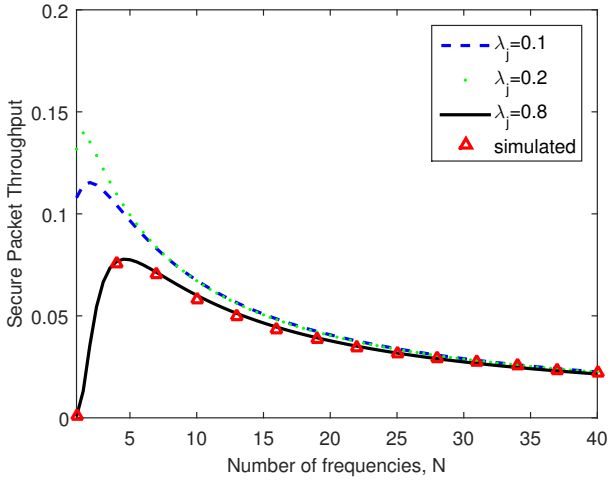

Fig. 5: secure packet throughput (T_s) with UFH and friendly jamming versus the number of available frequencies, for various jammers' spatial densities, $\lambda_j = 0.1$, $\lambda_j = 0.2$ and $\lambda_j = 0.8$, for a fixed $\lambda_e = 0.4$.

number of jammers to the expected number of eavesdroppers in the system, and employ jammer selection strategies [3].

Figure 5 shows the secure packet throughput with UFH and jamming for a varying number of frequencies. We compare three different settings with distinct λ_j values for a fixed $\lambda_e = 0.4$. This plot depicts the existence of a maximum secure packet throughput as a function of the number of frequencies also for the case of UFH and jamming, thus indicating that the maximization of the secure packet throughput under this setup depends on the joint optimization over the density of jammers and the available number of frequencies. This plot also shows that increasing the density of jammers does not necessarily lead to an increase in the secure packet throughput for the overall system. In particular, for this setup we can see that the secure packet throughput first increases when the

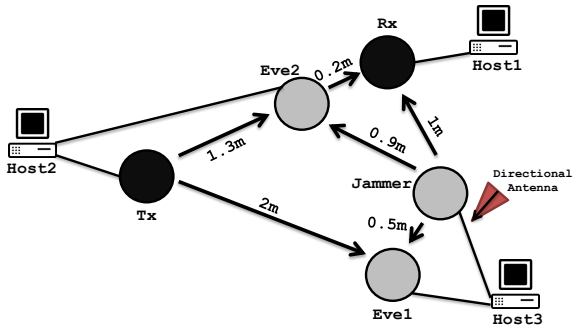

Fig. 6: Test-bed setup. The scenarios are organized in the following way, *Setup I: Tx*, *Rx* and *Eve1*; *Setup II: Tx*, *Rx*, *Eve1* and Jammer; *Setup III: Tx*, *Rx*, *Eve1*, *Eve2* and Jammer; *Setup IV: Tx*, *Rx*, *Eve1* and Jammer (directional antenna steered towards Eve).

density of jammers goes from $\lambda_j = 0.1$ to $\lambda_j = 0.2$, but then decreases when the density of jammers is set to $\lambda_j = 0.8$. This decrease in the secure packet throughput for $\lambda_j = 0.8$ happens because jammers can also harm the legitimate receiver *Rx* and, in the case of $\lambda_j = 0.8$ the harmful effect of jammers over *Rx* surpasses the beneficial effect of jammers over the eavesdroppers.

These results indicate that the number of jammers and frequencies must be adjusted to the expected number of eavesdroppers in the system. Actually, for lower numbers of eavesdroppers, jammers may cause more harm to legitimate communication than desired. However, it is realistic to assume that the information on the number of (silent) eavesdroppers may not be available. In such case, steering jammers away from legitimate receivers is a possibility that we will consider in the test-bed evaluation.

III. Test-bed Implementation and Evaluation

This section introduces and describes our test-bed implementation using software defined radios (SDRs). These experiments are performed to validate our analytical results, by comparing different setups, but mostly, as a tool to evaluate the performance of our security mechanisms when *realistically deployed*.

A. System Setup

Our test-bed is setup through Gnuradio and SDRs, more specifically five ettus USRPs B210 boards, which can operate on a continuous frequency coverage from 70 MHz – 6 GHz. We have devised three setups with different nodes, each representing a specific experiment. Figure 6 portrays each of these scenarios, as well as the disposition of the nodes and distances. Each of these devices corresponds to a single USRP and are hooked to a single host computer, responsible for retrieving and analyzing the data.

Our *first setup* includes a transmitter, *Tx*, and a receiver, *Rx*, distanced 1.5m from each other and an eavesdropper, *Eve1*, 2m away from *Tx*. The reason for placing the receiver and eavesdropper with dissimilar distances to the transmitter is to allow the analysis of two different situations in the same setup: a favorable situation [6] (a) in which *Rx* is closer than Eve to *Tx*, and an unfavorable (non-degraded eavesdropper) situation (b) in which Eve is closer to *Tx* than *Rx*. The later can be easily obtained by simply swapping the roles of *Rx* and Eve, without any other change to the system.

The *second setup* is similar to the first one except that we add another device, notably, an omnidirectional interferer which aims to defend legitimate communication.

The *third setup* features another eavesdropper, *Eve2*, placed near the legitimate receiver (at 0.2m), and distanced 1.3m from the transmitter.

Finally, the *fourth setup* incorporates a single eavesdropper (*Eve1*), but this time the jammer is deployed with a directional antenna which allows it to define a specific direction in which it will interfere (opposed to *Rx* and targeting an eavesdropper).

VARIABLE	Tx	Rx	Jammer	Eavesdroppers
antenna	Tx/Rx	Rx	Tx/Rx	Rx
bandwidth (Hz)	10e6	10e6	10e6	10e6
amplitude	0.6		0.6	
gain(db)	60	40	50	40
modulation	BPSK	BPSK	BPSK	BPSK
num_channels	[2,9]	[2,9]	[2,9]	[2,9]
run	[1,10]	[1,10]	[1,10]	[1,10]

TABLE II: System variables and their values.

For every setup we ran a 2-minute experiment 10 times for each number of available frequencies, between 2 and 9, ensuing no less than $10 \times 8 = 80$ tests. The USRP system variables and values employed are depicted in Table II. Because of time and hardware constraints, we opted to use between 2 and up to 9 different frequency channels with bandwidth of 1 MHz ranging from [2450 MHz, 2458 MHz], with a 1 Hz hop rate. The range of frequencies is also adequate and works with both types of antennas, omnidirectional and directional. After collecting the data, we calculate the secure packet throughput as

$$\frac{\#\text{packets received } (Rx) - \#\text{packets compromised (Eves)}}{\#\text{packets sent } (Tx)}$$

and determine the mean value and correspondent 95% confidence interval.

SETUP	I	II	III	IV
Devices	*Tx*, *Rx*, *Eve1*	*Tx*, *Rx*, *Eve1*, J	*Tx*, *Rx*, *Eve1*,2	... , *Eve1*, J*
a)	*Rx*→ *Tx*	*Eve1* → J	No Jamming	*Eve1* → J*
b)	*Eve1* → *Tx*	*Rx*→ J	Jamming	*Rx*→ J*

TABLE III: Setup's summary. *Tx*: Transmitter, *Rx*: Receiver, Eve: Eavesdropper, J: Jammer with omnidirectional antenna and J*: Jammer with directional antenna steered towards Eve. The → is interpreted as "closer to"; a) corresponds to the favorable scenario, while b) to the unfavorable.

[6] from a security perspective

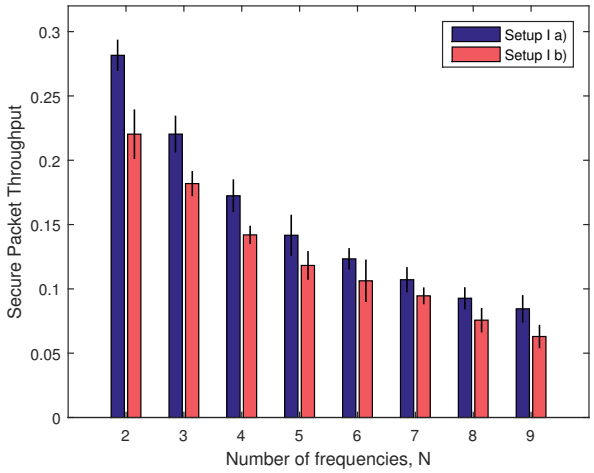

Fig. 7: Setup I - *Tx*, *Rx* and *Eve1*. In setup a) *Eve1* is closer, while in setup b) it is more distanced from *Rx*.

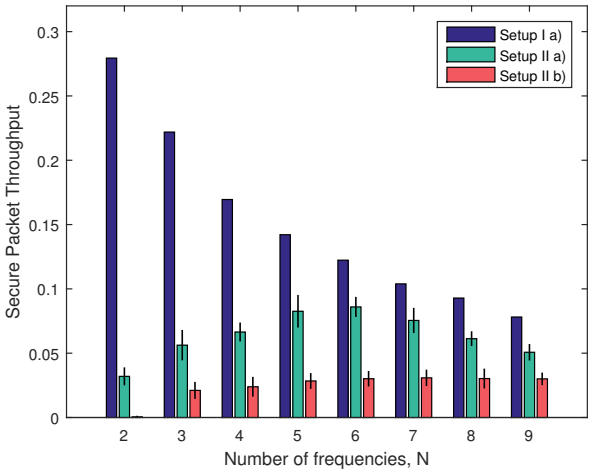

Fig. 8: Setup II - *Tx*, *Rx*, *Eve1* and an omnidirectional Jammer. In setup a) the jammer is closer to *Eve1*, while in setup b) it is closer to *Rx*. Setup I-a) is presented for comparison.

B. Results and Discussion

We now evaluate the four setups proposed, that are summarized in Table III, each setup with a corresponding favorable (a) and unfavorable (b) version. The unfavorable setups model non-degraded eavesdroppers by having eavesdroppers with the advantage of (1) being closer to *Tx* or (2) more distanced to a jammer than *Rx*. These unfavorable setups are, therefore, the most relevant to evaluate the effectiveness of this scheme against non-degraded eavesdroppers.

1) Setup I: Figure 7 plots the secure packet throughput (y-axis) with varying number of available frequencies (x-axis) for settings I-a) and I-b). We can see that the favorable (I-a) scenario leads to higher secure packet throughput than its unfavorable (I-b) counterpart, which is expected since *Rx* is closer to *Tx* than Eve. However, even when Eve is closer (unfavorable scenario I-b), there are still acceptable levels of secure packet throughput that result from the benefit of UFH against a non-degraded adversary eavesdropper.

2) Setup II: Figure 8 plots the secure packet throughput (y-axis) with varying number of available frequencies (x-axis) for settings II-a) and II-b). This setup is similar to the previous one except that we add an omnidirectional jammer. Results are in line with our theoretical analysis in the sense that an added jammer does not necessarily improve the secure packet throughput when compared with a similar scenario without jamming (setup I-a), specially for lower numbers/density of eavesdroppers. This was previously observed in Figure 4 and further reiterates the need to adjust the number of jammers to the number of eavesdroppers in the system. In particular, jammers may only be useful upon a higher number of eavesdroppers in the system. A higher number of eavesdroppers will also reduce the secure packet throughput without jamming as depicted in Figure 3, thus making the need for jammers more evident.

3) Setup III: In Figure 9 we can see that the addition of an extra eavesdropper (setup III-a) severely affects the secure packet throughput when compared to the case with a single eavesdropper (setup I-a). In such case, the addition of a friendly jammer (setup III-b) can in some cases (number of frequencies N=7) improve the secure packet throughput. However, the gain is, in this case, still limited, as a result of the negative impact of jammers on legitimate communication, thus calling for techniques to reduce the impact of jamming on legitimate communication [3]. Our analytical results indicate that the secure packet throughput gain due to jamming and UFH becomes more relevant as the number of adversary eavesdroppers is increased (see also Figures 2 and 4).

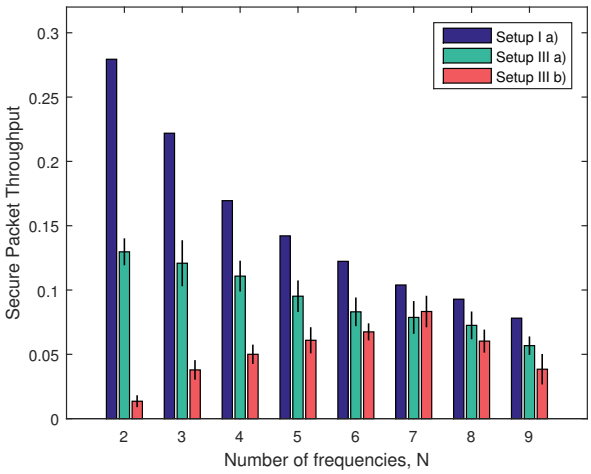

Fig. 9: Setup III - *Tx*, *Rx*, *Eve1*, *Eve2* and Jammer (in setup b) only).

Note that the secure packet throughput values of the test-bed experiments do not exactly match the analytical/simulated results of Section II-D. This is expected because (1) the test-bed includes the effect of other environmental effects

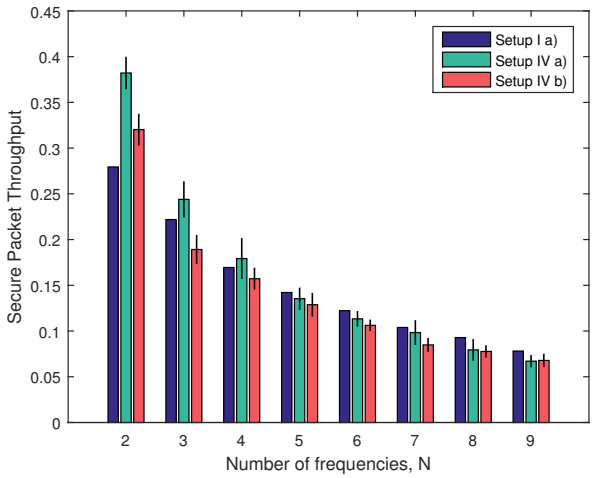

Fig. 10: Setup IV - *Tx*, *Rx*, *Eve1* and jammer with directional antenna steered towards Eve. In setup a) *Eve1* is closer, while in setup b) it is more distanced from the jammer. Setup I-a) is presented for comparison.

(e.g. fading, shadowing) that are not considered in the analytical model, and (2) the analytical stochastic model considers densities of devices other than a discrete number of nodes, as in the test-bed. However, the general behavior holds, in particular the fact that the secure packet throughput can be maximized by adjusting the number of frequencies to the number of devices in the system (Figures 5 and 9).

We have seen so far that the secure packet throughput with non-degraded eavesdroppers can be improved via UFH and jamming. These eavesdroppers are non-degraded by either being closer to the *Tx* than *Rx* (setup I-b in *Figure 7*) or having a numerical advantage over *Rx* (setup III-a in *Figure 9*). While jamming can help (setup III-b in *Figure 9*), its benefit is still limited due to the negative impact on legitimate communication. To address this issue, we now consider a different setup with a jammer employing a directional antenna to steer away from legitimate communication. This setup is valid if there is some information about possible locations of eavesdroppers, e.g. eavesdroppers lie outside a protected region such as a warehouse [6].

4) Setup IV: We now consider a setup where the jammer resorts to a directional antenna to steer interference towards Eve1 and away from *Rx*, with Eve1 closer (favorable scenario IV-a) or more distanced to the jammer (unfavorable scenario IV-b: *Rx*$\rightarrow J^*$ is equivalent to Eve1 being further away from J^* in Figure 6).

Figure 10 shows that directional-antenna jammers can improve the secure packet throughput when oriented towards Eve and away from *Rx*. Naturally, the benefit is higher when Eve is closer to the jammer (IV-a) than when more distanced (IV-b). In both cases jamming can lead to relevant gains when compared to the scenario without jammers of setup I-a (also depicted in the figure), notably for lower numbers of frequencies.

IV. Secret Key Agreement with UFH and Jamming

We have seen that the secure packet throughput in our scenarios is, at best, close to 40%, that is less than half of the transmissions are being secured. This is clearly insufficient for secure communication in many scenarios, even against a non-degraded adversary. In this section we describe a methodology for secret-key establishment that benefits from the advantage provided by UFH to provide higher levels of security. In particular, we devise a scheme for secret key agreement that builds on the advantage provided by UFH and jamming to exchange a key that can then be used for secure communication with higher performance levels. This key is exchanged by taking advantage of UFH and jamming against a non-degraded eavesdropper, after which the system can fallback to regular (non-UFH) communication with higher communication/throughput levels.

We start by noting that under UFH with a secure packet throughput of $\mathcal{T}_\mathrm{s}$, the probability of having at least one secure packet can be made arbitrarily close to 1 as follows.

Lemma 1. (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 t transmitted packets is given by

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

and this can be made arbitrarily close to 1 with increasing number of transmissions t, at the cost of added delay.

We then assume that we have at least one secure packet out of r packets that were received by *Rx* (i.e. this one packet was not received by eavesdroppers), with probability as determined by Lemma 1.

A. Secret-key Agreement by Hashing over Received Packets

Consider that *Tx* sent t packets $P_{tx} = \{p_1, \ldots, p_t\}$ into the network. From these, a set of r packets $P_{rx} = \{p_1, \ldots, p_r\}$ are received by *Rx*, such that $P_{rx} \subset P_{tx}$. By employing the aforementioned UFH mechanism, according to Lemma 1, if we wait long enough (i.e. transmit enough packets) we will have a high probability that from these P_{rx} packets, at least one was not received by eavesdroppers with set of packets $P_{eves} = \{p_1, \ldots, p_e\} \subset P_{tx}$.

Consider $H(\cdot)$ a one-way hash function that maps data of arbitrary size (e.g. concatenated payloads of packets) to data of fixed size, that we shall use as a key. *Rx* can then apply this hash function over the set of received packets, thus producing $H(P_{rx}) = H(\{p_1, \ldots, p_r\})$. Following the assumption from Lemma 1 that at least one of these packet was received securely (i.e. eavesdroppers did not get it), a one-way hash function of these packets can serve as a key $\mathcal{K}_r = H(P_{rx})$ that can be used to communicate securely with *Tx*.

For *Tx* to have access to the same key, *Rx* can simply inform *Tx* of the ids $\{i, \ldots, r\}$ (e.g. sequence numbers) of its received packets P_{rx}. This information can be sent in clear and will be of no use to eavesdroppers, because eavesdroppers missed at least one of the packets, therefore being unable to derive the same key (hash over all received packets from *Rx*). Finally,

by knowing only the set (ids) of packets that *Rx* sucessfully received and requiring no information about the eavesdroppers, *Tx* can derive a shared key for secret communication with *Rx* by hashing over the set of packets with ids sent from *Rx*, thus producing the shared key $\mathcal{K}_r = H(P_{rx})$. The whole process is presented in Algorithm 1.

Algorithm 1 Secret Key Agreement

1: $P_{tx} \leftarrow$ set of packets $\{p_1, \ldots, p_t\}$ sent by *Tx*
2: $P_{rx} \leftarrow$ set of packets $\{p_1, \ldots, p_r\}$ received by *Rx*
3: $H(\cdot) \leftarrow$ one-way hash function that maps data of arbitrary size to data of fixed size
4: *Tx* sends set P_{tx} of packets to *Rx*
5: *Rx* receives a set P_{rx} of those packets
6: *Rx* derives a key $\mathcal{K}_r = H(P_{rx})$ from the packets received from *Tx*
7: *Rx* sends the ids of the received packets $\{1, \ldots, r\}$ to *Tx*
8: *Tx* selects from P_{tx} the set of packets received by *Rx*, using the received ids
9: *Tx* generates a key $\mathcal{K}_t = H(P_{rx}) = \mathcal{K}_r$ (shared key with *Rx*)
10: *Tx* and *Rx* communicate securely using the shared key

Note that although our scheme and [14] both rely on UFH for secret-key establishment, our scheme differs from [14] because of the different nature of the adversary and the different approaches to secret-key establishment. Our adversary is a passive eavesdropper that aims to break confidentiality, while the adversary in [14] is an active jammer that wants to compromise/prevent legitimate communication. Our approach for secret-key establishment relies on hashing over a set of packets, from which at least one shall not be received by Eve, while Diffie-Hellman is used in [14]. From our understanding, these two elements combined make it unfeasible to compare the two proposals. In fact, our results in Section IV-C focus on the probability that at least one message is not received by eavesdroppers, whereas [14] looks at the probability that a message is successfully received under active jammers, considering specific parameters with respect to the jammer adversary that are not applicable in our case.

B. Determining the System Secure Packet Throughput

One important aspect in this process is determining the expected secure packet throughput, for establishing the amount of packets t that are required to transmit so as to achieve a given probability of eavesdroppers not receiving at least one packet according to Lemma 1. Since it is reasonable to assume availability of information about the legitimate receiver, deciding the secure packet throughput then depends on the information one is able to determine about Eve. A first step towards that goal is being able to detect the presence of a passive eavesdropper. While there are some works that may help by trying to detect Eve's presence from the local oscillator power that is leaked from its RF front end [26], we consider that this is a challenging goal on its own that is out of the scope of this paper.

This aspect can be more easily addressed if there is some restriction to eavesdroppers, e.g. a protected area such as the inside of a warehouse where eavesdroppers cannot appear [6]. In this restricted case, a lower-bound estimate for the secure packet throughput can be obtained through real-world measurements considering eavesdroppers in the best possible location in the outside of the protected area. For the more general case in which eavesdroppers can appear everywhere, other solutions shall be required, possibly involving user cooperation, and are left as future work.

C. Information Leakage to Eve

Measuring information leakage to a passive eavesdropper is a major challenge of secret-key agreement schemes. This can be approached in two manners:

- Conceptually: several works [16], [27] measure leakage to Eve as the mutual information (or some variant thereof) between the information at Eve and the original information from the transmitter *Tx*. This requires knowing what information Eve has received;
- In practice: determining the information that is received by Eve so as to measure what was leaked. This is a difficult problem, most notably against passive/silent eavesdroppers. While there are works that aim to detect Eve based on the power leaked from its RF front end [26], this is still insufficient to determine what Eve has received.

Measuring leaked information in practice is a very challenging goal on its own that is out of the scope of this paper. However, by following the first (conceptual) approach above, we can determine information leakage to Eve as a function of transmitted packets for several scenarios as follows.

Definition 2 (Leakage Rate)**.** *The leakage rate from* Tx *to the eavesdroppers (Eves) is the number of packets compromised by the eavesdroppers over the number of packets received by* Rx*,*

$$\mathcal{L}_r = \frac{\#\text{packets compromised (Eves)}}{\#\text{packets received (}Rx\text{)}}. \tag{15}$$

Leakage occurs when a packet that is sucessfully received by *Rx* is also received by the eavesdroppers. Therefore, the number of packets compromised by the eavesdroppers is the number of packets that eavesdroppers received from those received by *Rx*.

Figure 11 shows the leakage rate for a set of selected scenarios from Table III. To avoid overcrowding the plot, we select only the favorable scenarios, i.e. version a) of each setup. For a fair comparison among setups, we run each setup for the same time duration and select the optimal system configuration, i.e. the number of frequencies N that optimizes the secure packet throughput for each setup as shown in the legend. Two behaviours warrant extra explanation: (a) the initial erratic behavior of the leakage rate is due to a low number of received packets, leading to more abrupt variations

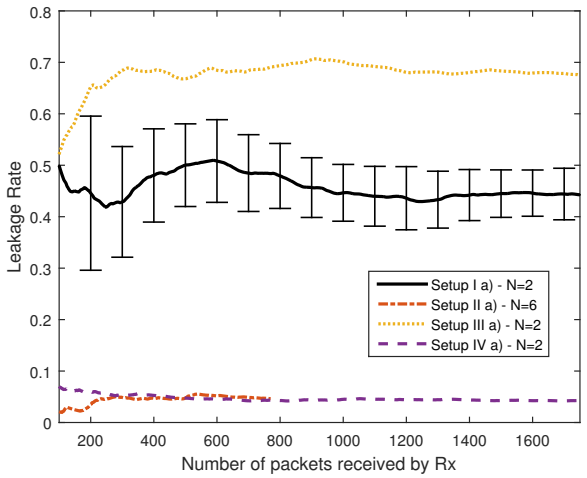

Fig. 11: Leakage rate with varying number of packets for the advantageous settings considered in the testbed setups of Table III. We decided to include the confidence intervals for a single setup to avoid overcrowding the plot.

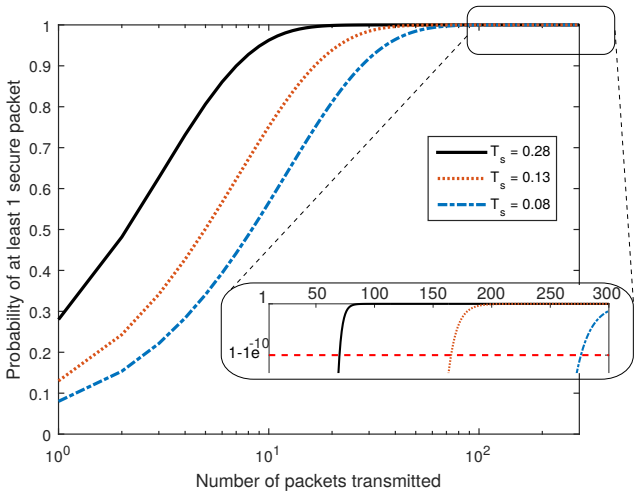

Fig. 12: Probability of at least one packet not being received by an eavesdropper with a varying number of packets transmitted. We considered three different secure packet throughput values, $\mathcal{T}_{\rm s} = 0.28$, $\mathcal{T}_{\rm s} = 0.13$, $\mathcal{T}_{\rm s} = 0.08$, corresponding respectively to the optimal secure packet throughput results of Setups I-a, III-a, and II-a in the testbed. The zoomed area at larger number of transmitted packets shows the number of packet transmissions needed for each setup for a probability of receiving at least one secure packet of $1 - 1e^{10}$.

in the leakage rate formula (15), and (b) depending on the setup, for the same duration of experiments fewer packets may be received, as result of a higher number of frequencies being employed (which reduces the probability of landing in the same frequency) and the effect of interference from jammers on *Rx*, as seen for Setup II-a whose results terminate at nearly 800 packets. This makes the leakage rate results more relevant to analyze in terms of its convergence with growing number of packets.

From *Figure 11*, it is clear the benefit of jamming and adjusting the number of frequencies to reduce the leakage rate. In particular, Setup II-a with one omnidirectional jammer and $N = 6$ as well as Setup IV-a with one directional jammer and $N = 2$ both lead to the lowest leakage results. The negative effect of added eavesdroppers is also apparent with the leakage rate increase from Setup I-a (1 eavesdropper) to Setup III-a (2 eavesdroppers), both without jamming.

Note that in our case, secret key agreement is successful even with a non-zero leakage rate, as long as the eavesdroppers fail to compromise at least one packet that was received by *Rx* (i.e. leakage rate is not 1). However, the leakage rate fails to capture the effect of the probability of *Rx* receiving a packet, which is needed for secret key agreement. In particular, adding jammers and/or increasing the number of frequencies can reduce the probability of *Rx* receiving packets, as seen in the lower number of received packets (below 800) for Setup II-a in *Figure 11* for the same duration of experiments.

Knowingly of the probabilistic nature of our scheme and the difficulty to determine the secure packet throughput in practice, it does provide us a way to assess the probability of secret-key agreement success (i.e. of having at least one packet received by *Rx* and not Eve) according to the number of packet transmissions and the secure packet throughput as shown in Lemma 1. The probability that a packet is successfully received depends not only on the system setup (i.e. relative location of devices and number of frequencies), but also on the number of packet transmissions, as depicted in *Figure 12*. Based on this information, we can define a threshold τ for the probability that *Rx* receives at least one packet without Eve doing so. This helps us determining the minimum number of packet transmissions so that a prescribed level of secrecy τ is achieved. For example, with $\mathcal{T}_{\rm s} = 0.08$ (the optimal result for Setup II-a), for a probability that at least one packet is received by *Rx* without being received by Eve $\tau = 1 - 1e^{-10}$, one would have to transmit nearly 277 packets, as depicted in the zoomed part of *Figure 12*.

V. Conclusion

We characterized the secure packet throughput (probability of secure communication) of a wireless system operating under Uncoordinated Frequency Hopping (UFH), a frequency hopping scheme in which devices hop uniformly at random between a set of frequencies. Through a spatial stochastic geometry approach and aggregate interference model, we proposed a mathematical model for evaluation of UFH combined with jamming, that takes into account propagation effects combined with random disposition of devices in space. Results showed that jamming coupled with UFH can provide secrecy benefits when fending off multiple/non-degraded eavesdropper adversaries, and secrecy gains can be maximized by adjusting the number of frequencies to maximize the secure packet throughput. We also implemented and realistically evaluated these schemes in a software-defined radio test-bed, with results showing compliance with our analytical model. Finally, we have proposed a secret-key establishment methodology that builds on the advantage provided by UFH and jamming to establish secret keys against a non-degraded eavesdropper

adversary.

Future directions for this work entail being able to detect passive eavesdroppers as a step to determine the secure packet throughput in practice. Additionally, in the line of recent advances on full-duplex communications, other directions include having a receiver generate its own noise, thus being able to interfere with eavesdroppers while performing auto-cancellation of the effect of its own noise in received signals.

VI. Acknowledgments

We would like to thank useful discussions with Pedro C. Pinto, Marco Gomes, and Dinis Sarmento.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] 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.

[3] 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, no. 3, pp. 616–627, September 2011.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] J. P. Vilela and J. S. Sousa, "Physical-layer security against non-degraded eavesdroppers," in *IEEE Global Communications Conference (Globecom)*, San Diego, CA, USA, December 2016.

[9] 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, no. 6, pp. 2735–2751, June 2008.

[10] P. C. Pinto, J. Barros, and M. Z. Win, "Techniques for enhanced physical-layer security," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Miami, Florida, USA, December 2010, pp. 1–5.

[11] ——, "Wireless physical-layer security: The case of colluding eavesdroppers," in *IEEE International Symposium on Information Theory*, Seoul, South Corea, July 2009, pp. 2442–2446.

[12] ——, "Physical layer security in stochastic wireless networks," in *IEEE International Conference on Communication Systems (ICCS)*, Guangzhou, China, November 2008, pp. 974–979.

[13] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in mimo wiretap channels," in *Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, California, USA, November 2011, pp. 265–269.

[14] M. Strasser, C. Pöpper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *IEEE Symposium on Security and Privacy*, Oakland, California, USA, 2008, pp. 64–78.

[15] 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.

[16] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[17] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[18] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proceedings of the Fourth European Workshop on System Security*, Salzburg, Austria, 2011.

[19] 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.

[20] ——, "Uncoordinated frequency hopping for secrecy with broadband jammers and eavesdroppers," in *IEEE International Conference on Communications (ICC)*, London, UK, June 2015.

[21] J. P. Vilela and J. S. Sousa, "Physical-layer security against non-degraded eavesdroppers," in *IEEE Global Communications Conference (Globecom)*, San Diego, USA, December 2015.

[22] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its application," *Proceedings of the IEEE*, vol. 97, no. 2, no. 2, pp. 205–230, February 2009.

[23] J. F. C. Kingman, *Poisson Processes*. Oxford University Press, 1993.

[24] J. P. Nolan, *Stable Distributions - Models for Heavy Tailed Data*. Boston, USA: Birkhauser, 2015.

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

[26] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the mimo wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Pacific Grove, California, USA, 2012, pp. 2809–2812.

[27] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on pid controller," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1842–1852, 2013.

João Sá Sousa is a Security/Privacy Software Engineer at the LCA1 laboratory of EPFL (École Polytechnique Fédérale de Lausanne), under the direction of professor Jean-Pierre Hubaux. He received his Master's degree in Computer Science in 2015 from the University of Coimbra and was a visiting student at the University of Bern for 3 months. His Master's thesis was entitled "Spread Spectrum and Jamming for Wireless Secrecy" and focused on the research of new defensive PHY schemes to provide protection in wireless networks. He also did a 3-month internship at Carnegie Mellon (CMU-SV), working on new ways of enhancing privacy in android based systems. More recently, João Sá Sousa has been working with genome privacy, applied cryptography and trusted hardware.

João P. Vilela is an assistant professor at the Department of Informatics Engineering of the University of Coimbra, Portugal. He received his Ph.D. in Computer Science in 2011 from the University of Porto, Portugal. In recent years, he has been a Coordinator and Team Member of several national, bilateral, and European-funded projects in security and privacy. His main research interests are in security and privacy of computer and communication systems, with focus on wireless networks, mobile devices and cloud computing. Other research interests include anticipatory networks and intelligent transportation systems.