Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation

Miroslav Mitev
School of CSEE
University of Essex
Colchester, UK
mm17217@essex.ac.uk

Arsenia Chorti
ETIS, Université Paris Seine, ENSEA
Université Cergy-Pontoise, CNRS
Cergy-Pontoise, France
arsenia.chorti@ensea.fr

E. Veronica Belmega
ETIS, Université Paris Seine, ENSEA
Université Cergy-Pontoise, CNRS
Cergy-Pontoise, France
belmega@ensea.fr

Martin Reed
School of CSEE
University of Essex
Colchester, UK
mjreed@essex.ac.uk

***Abstract*—Wireless secret key generation (W-SKG) from shared randomness (e.g., from the wireless channel fading realizations), is a well established scheme that can be used for session key agreement. W-SKG approaches can be of particular interest in delay constrained wireless networks and notably in the context of ultra reliable low latency communications (URLLC) in beyond fifth generation (B5G) systems. However W-SKG schemes are known to be malleable over the so called "advantage distillation" phase, during which observations of the shared randomness are obtained at the legitimate parties. As an example, an active attacker can act as a man-in-the-middle (MiM) by injecting pilot signals and/or can mount denial of service attacks (DoS) in the form of jamming. This paper investigates the impact of injection and reactive jamming attacks in W-SKG. First, it is demonstrated that injection attacks can be reduced to – potentially less harmful – jamming attacks by pilot randomization; a novel system design with randomized QPSK pilots is presented. Subsequently, the optimal jamming strategy is identified in a block fading additive white Gaussian noise (BF-AWGN) channel in the presence of a reactive jammer, using a game theoretic formulation. It is shown that the impact of a reactive jammer is far more severe than that of a simple proactive jammer.**

***Index Terms*—Wireless secret key agreement, shared randomness, injection attack, man-in-the-middle, denial of service attack, jamming.**

I. Introduction

In the past two decades a large number of studies and patents appeared on the topic of wireless secret key generation (W-SKG) schemes that exploit channel reciprocity as the source of shared randomness (see [1] for a comprehensive review and [2] for a tutorial on physical layer security including W-SKG). Additionally, W-SKG over unauthenticated channels has been proposed in [3], consolidating physical layer security technologies with standard authenticated encryption (AE) schemes [4], while a large number of practical demonstrators have provided "proof of concept" [5], [6]. A resurgence of interest in W-SKG has been witnessed recently as these technologies could be considered for application in B5G systems [1], in particular in the context of Internet of things (IoT) [7] and – potentially – URLLC applications. W-SKG could be a good fit in these systems as the limited computational resources and strict delay constraints can render challenging the use of standard security protocols such as the transport layer security protocol (TLS) protocol and it's IoT friendly version, the datagram transport layer security (DTLS) protocol.

In recent works it has been shown that building semantically secure AE protocols using the W-SKG procedure is straightforward, as long as the channel probing phase of the scheme is robust against active attacks [4], [8]. Therefore, an important next step is to study man-in-the-middle (MiM) and denial of service (DoS) attacks during the channel excitation phase of the W-SKG protocol, commonly referred to as "advantage distillation".[1] In this paper, two such active attacks, during channel probing are discussed.

Firstly, MiM attacks, referred to as "injection" attacks, are investigated in Section II: an active adversary tries to control part of the generated secret key by spoofing the channel estimation phase of the W-SKG scheme. We propose a simple approach to mount such a MiM attack, assuming that the adversary has one additional antenna with respect to the legitimate users. This is a very mild assumption with respect to the adversary's capabilities and reveals a critical vulnerability of W-SKG, that needs to be addressed. As a countermeasure, we propose a concrete pilot randomization scheme using quadrature amplitude phase shift keying (QPSK) modulated random pilots. We prove that the source of shared randomness remains Gaussian and that the adversary can no longer mount the MiM attack. An interesting conclusion of our analysis is that the MiM attack is reduced to a jamming attack when pilot randomization is employed.

Motivated by this result, in Sections III and IV, DoS in the form of reactive jamming is studied for BF-AWGN channels – used as an abstraction for orthogonal frequency division multiplexing (OFDM) modulation systems. The attacker's optimal strategies are derived. In the present contribution we assume that the legitimate users blindly adopt a uniform power allocation policy, the level of which we optimally iden-

[1] W-SKG schemes typically encompass three distinct phases: (i) the advantage distillation, during which observations of the shared randomness are obtained at the two legitimate parties; (ii) the reconciliation phase, during which side information, typically in the form of Slepian Wolf decoder cosets, is exchanged over a public channel; and, (iii) the privacy amplification phase, over which universal hash functions are employed to suppress the amount of information leaked during the reconciliation and also to ensure that the generated keys are of maximum entropy, i.e., uniformly distributed in the key space.

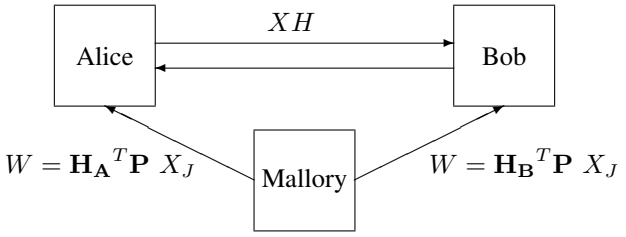

Fig. 1. Alice and Bob have single transmit and receive antennas and exchange pilot signals X over a Rayleigh fading channel with realization H. A MiM, Mallory, with multiple transmit antennas can inject a suitably pre-coded signal $\mathbf{P}X_J$, such that the received signal at both Alice and Bob coincide $W = \mathbf{H_A}^T\mathbf{P} = \mathbf{H_B}^T\mathbf{P}$.

tify; the more general case of an arbitrary power allocation for the legitimate parties will be investigated in the future. Our study demonstrates that a reactive jammer can have a far more serious impact on the W-SKG process compared to a simple proactive jammer. In the future, frequency hopping as well as energy harvesting approaches to mitigate the impact of reactive jammers [9] will be explored.

Finally, conclusions and further work are discussed in Section V.

II. MiM in W-SKG Systems: Injection Attacks

MiM in the form of injection attacks constitutes one of the most critical limitations in W-SKG systems that extract secret keys from received signal strength (RSS) measurements [10]–[12]. Recently, various possible approaches for injection attacks have been published: in [10], the attacker controlled the movement of objects in an indoor wireless network, thus generating predictable changes in the RSS, (e.g., by obstructing, or not, a line-of-sight). In [11], whenever similar channel envelope measurements in the links to the legitimate nodes were observed, the MiM spoofed the W-SKG process by injecting a strong signal. In the following we will prove that – even when full CSI is used to extract the keys – it suffices that the adversary has one additional antenna with respect to the legitimate users to be able to mount an injection MiM attack.

To capture the main components of MiM attacks in W-SKG systems, we employ the system model depicted in Fig. 1, comprising three nodes: a legitimate transmitter, its intended receiver, and a MiM, referred to as Alice, Bob and Mallory, respectively. Alice and Bob are assumed to have a single antenna each for simplicity, while Mallory has two transmit antennas.[2] The fading channel realization in the link Alice-Bob is denoted by the complex circularly symmetric Gaussian random variable $H \sim \mathcal{CN}(0, \sigma^2)$. To obtain estimates of H, Alice and Bob exchange pilot signals X with $\mathbb{E}[|X|^2] \leq P$. Furthermore, following [11], we assume Mallory has perfect knowledge of the channel vectors in the multiple input single output (MISO) links Mallory-Alice and Mallory-Bob. The channel coefficients are assumed to be independent and identically distributed (i.i.d.), i.e., $\mathbf{H_A} = [H_{A1}, H_{A2}]^T, \mathbf{H_B} = [H_{B1}, H_{B2}]^T$ with $(H_{A1}, H_{A2}, H_{B1}, H_{B2}) \sim \mathcal{CN}(\mathbf{0}, \sigma_J^2/2\ \mathbf{I}_4)$; this assumption is realistic since Mallory can estimate the channel vectors while Alice and Bob exchange pilot signals, as long as the channel's coherence time is respected (a plausible scenario in slow fading, low mobility environments).

To mount the attack, Mallory transmits a signal X_J, suitably precoded as $\mathbf{P}X_J$. The precoding matrix $\mathbf{P} = [P_1, P_2]^T$ is chosen such that the same signal is "injected" at both Alice and Bob, i.e.,

$$\mathbf{H_A}^T\mathbf{P}X_J = \mathbf{H_B}^T\mathbf{P}X_J \Rightarrow$$
$$P_1 = \frac{H_{B2} - H_{A2}}{H_{A1} - H_{B1}} P_2, \tag{1}$$

where, due to the i.i.d. assumption and to the continuous distribution of the channels, $H_{A1} \neq H_{B1}$ almost surely. As a result, Mallory can select a suitable precoding matrix (among infinite possibilities). Assuming a total power constraint $\mathbb{E}[|\mathbf{P}X_J|^2] \leq \Gamma$ for Mallory's transmission, P_2 should be chosen as

$$P_2 \leq \frac{\sqrt{\Gamma}}{\left|\frac{H_{B2}-H_{A2}}{H_{A1}-H_{B1}}\right|}. \tag{2}$$

This procedure, illustrated in Fig. 1, shows that it is possible to generalize the injection attack presented in [11], in which an attacker injected a strong signal whenever the RSS in the Mallory-Alice and Mallory-Bob links were similar. More importantly, the presented injection attack accounts not only for the RSS but for the full CSI, i.e., it includes the signal phase.

The observations at Alice and Bob, denoted by Z_A and Z_B, are

$$Z_A = XH + W + N_A \tag{3}$$
$$Z_B = XH + W + N_B, \tag{4}$$

where $W = \mathbf{H_A}^T\mathbf{P}X_J = \mathbf{H_B}^T\mathbf{P}X_J$ denotes the observed injected signal at Alice and Bob which is identical at both due the precoding matrix $\mathbf{P}$; and, N_A, N_B denote zero-mean unit variance i.i.d. complex circularly symmetric Gaussian random noise variables, i.e., $N_A, N_B \sim \mathcal{CN}(0, 1)$. The secret key rate controlled by Mallory is upper bounded by [8]

$$L \leq I(Z_A, Z_B; W). \tag{5}$$

Identifying the optimal injection signal W, corresponds to finding the capacity achieving input signal of the *two-look Gaussian channel* in (3)-(4). This signal is known to be Gaussian [13]; hence, a good choice for X_J is to be constant, so that, the overall injected signal is an optimal complex zero-mean circularly symmetric Gaussian signal, $W \sim \mathcal{CN}(0, \sigma_J^2\Gamma)$.

A countermeasure to injection attacks can be built by randomizing the pilot sequence exchanged between Alice and Bob [12], [8]. Here, we propose to randomize the pilots by

[2]It is straightforward to see that the scenario can easily be generalized to a multi-antenna setting in which Mallory has one more antenna than Alice and Bob.

drawing them from a (scaled) QPSK modulation, as follows: instead of transmitting the same probing signal X, Alice and Bob transmit independent, random probe signals X and Y, respectively, drawn from i.i.d. zero-mean discrete uniform distributions $\mathcal{U}(\{\pm r \pm jr\})$, where $j = \sqrt{-1}, r = \sqrt{P/2}$, so that, $\mathbb{E}[X] = \mathbb{E}[Y] = 0$, $\mathbb{E}\left[|X|^2\right] = \mathbb{E}\left[|Y|^2\right] = P$ and $\mathbb{E}[XY] = 0$, i.e., the pilots are randomly chosen QPSK signals. Alice's observation Z_A is modified accordingly as

$$Z_A = YH + W + N_A, \tag{6}$$

while Bob's observation is given in (4). To establish shared randomness in spite of the pilot randomization, Alice and Bob post-multiply Z_A and Z_B by their randomized pilots, obtaining local observations $\tilde{Z}_A$ and $\tilde{Z}_B$ (unobservable by Mallory), expressed as:

$$\tilde{Z}_A = XZ_A = XYH + XW + XN_A, \tag{7}$$
$$\tilde{Z}_B = YZ_B = XYH + YW + YN_B. \tag{8}$$

Lemma 1: The source of shared randomness, when the pilots are randomized QPSK symbols, is a circularly symmetric zero mean Gaussian random variable, $XYH \sim C\mathcal{N}(0, P^2\sigma^2)$.

Proof: We treat the two orthogonal axes (real and imaginary) independently. Looking only at the real values of the pilots and of the channel coefficient X, Y, H denoted here by $X_R = \mathrm{Re}(X)$, $Y_R = \mathrm{Re}(Y)$ and $H_R = \mathrm{Re}(H)$, we express the underlying discrete uniform pdf $f_{X_R}(x)$ and $f_{Y_R}(y)$ and the continuous pdf $f_{H_R}(h)$ as

$$f_{X_R}(x) = \frac{1}{2}\delta(x-r) + \frac{1}{2}\delta(x+r), \tag{9}$$
$$f_{Y_R}(y) = \frac{1}{2}\delta(y-r) + \frac{1}{2}\delta(y+r), \tag{10}$$
$$f_{H_R}(h) = \frac{1}{\sqrt{\pi}\sigma} e^{-\frac{h^2}{\sigma^2}}. \tag{11}$$

The pdf of the product $X_R H_R$ is given as

$$\begin{aligned} f_{X_R H_R}(z) &= \int_{-\infty}^{\infty} f_{X_R}(x) f_{H_R}(z/x) \frac{1}{|x|} \mathrm{d}x \\ &= \int_{-\infty}^{\infty} \frac{1}{2\sqrt{\pi}\sigma|x|} \delta(x-r) e^{-\frac{(z/x)^2}{\sigma^2}} \mathrm{d}x \\ &+ \int_{-\infty}^{\infty} \frac{1}{2\sqrt{\pi}\sigma|x|} \delta(x+r) e^{\frac{-(z/x)^2}{\sigma^2}} \mathrm{d}x \\ &= \frac{\sqrt{2} e^{-\frac{2z^2}{P\sigma^2}}}{\sqrt{\pi P}\sigma} \end{aligned} \tag{12}$$

by substituting $r = \sqrt{P/2}$ at the last derivation, i.e., $X_R H_R \sim \mathcal{N}(0, \frac{P\sigma^2}{4})$. A similar result holds for the products involving also the imaginary parts of X and H: $X_I H_I$, $X_I H_R$ and $X_R H_I$, so that $XH \sim \mathcal{CN}(0, P\sigma^2)$. Extending this result, we find that $XHY \sim \mathcal{CN}(0, P^2\sigma^2)$. ∎

Furthermore, due to the fact that X and Y are independent and have zero mean, the variables XW and YW are uncorrelated, circularly symmetric zero-mean Gaussian random variables, and, therefore independent, while the same holds for XN_A, YN_B, i.e., $(XW, YW) \sim \mathcal{CN}(\mathbf{0}, \sigma_J^2 P\Gamma \mathbf{I}_2)$ and $(XN_A, YN_B) \sim \mathcal{CN}(\mathbf{0}, P\mathbf{I}_2)$. Alice and Bob extract the common key from the modified source of common randomness XYH as opposed to XH. On the other hand, since XW, YW, XN_A, YN_B are i.i.d. complex circularly symmetric Gaussian random variables, the proposed scheme reduces injection attacks to uncorrelated jamming attacks, i.e., using Lemma 1 we get that

$$L \leq I\left(\tilde{Z}_A, \tilde{Z}_B; W\right) = 0. \tag{13}$$

III. Jamming Attacks on W-SKG

Building on the results of the previous section, we next examine in detail the scenario in which Mallory acts as a reactive jammer. Reactive jamming is a stealthy jamming approach in which the jammer first senses the spectrum and jams only when she detects an ongoing transmission. Due to the effectiveness and difficulty to be detected, reactive jammers are considered as the most harmful [14], [15]. Furthermore, as OFDM is used in many actual systems (and will be used at least in the first deployments of 5G), in our analysis we assume a BF-AWGN channel as in [9]. In this context, we assume that Alice and Bob perform W-SKG over a BF-AWGN channel with N parallel blocks (referred to as subcarriers for clarity). The notation introduced in Section II is extended with the introduction of a carrier index $i \in \{1, \ldots, N\}$, i.e., X_i, Y_i denote the randomized pilots on the i-th subcarrier, H_i denotes the channel coefficient in the link Alice-Bob, W_i the signal injected by Mallory on the i-th subcarrier and $N_{A,i}, N_{B,i}$ noise variables. As a reactive jammer, Mallory senses the spectrum and jams a specific subcarrier only when the power on it exceeds a certain threshold p_{th}. Two scenarios are considered: i) when p_{th} is fixed (determined in essence by the carrier sensing capability of Mallory's receiver); ii) when p_{th} is variable (its choice forms part of her strategy).

We can reformulate the expressions of Alice's and Bob's local observations on the i-th W-SKG subcarrier as follows:

$$\tilde{Z}_{A,i} = X_i Y_i H_i + X_i W_i + X_i N_{A,i} \tag{14}$$
$$\tilde{Z}_{B,i} = X_i Y_i H_i + Y_i W_i + Y_i N_{B,i} \tag{15}$$

for $i = 1, \ldots, N$ with $H_i \sim \mathcal{CN}(0, \sigma^2)$, $W_i \sim \mathcal{CN}(0, \sigma_J^2 \gamma_i)$, $N_{A,i} \sim \mathcal{CN}(0,1)$, $N_{B,i} \sim \mathcal{CN}(0,1)$. In this work, we assume that Alice and Bob use the same power p on all pilots, in agreement with common practice during the advantage distillation phase; the more general scenario of an arbitrary power allocation across the subcarriers will be investigated in the future. Based on this assumption we have that $\mathbb{E}[|X_i|^2] = \mathbb{E}[|Y_i|^2] = p$ with $p \in [0, P]$.

On the other hand, we let Mallory choose the power allocation vector to maximize the impact of her attack. The power Mallory uses on the i-th subcarrier is denoted by γ_i, so that $\mathbb{E}[|W_i|^2] = \sigma_J^2 \gamma_i$. Denoting the average available power for jamming by Γ and the power allocation of the jammer by $\underline{\boldsymbol{\gamma}} = (\gamma_1, \ldots, \gamma_N)$, we assume the following short-term power

constraint:

$$\underline{\gamma} \in \mathbb{R}_+^N, \quad \sum_{i=1}^{N} \gamma_i \leq N\Gamma. \tag{16}$$

Assuming that H_i is uncorrelated with $H_{A,i}, H_{B,i}$, $i = 1, \ldots, N$ and that the pilot randomization approach proposed in Section II is employed, the W-SKG rate $R(p, \gamma_i) = I\left(\tilde{Z}_{A,i}; \tilde{Z}_{B,i}\right)$ on the i-th subcarrier, can be expressed as a function of p and $\gamma_i, i = 1, \ldots, N$ as [9]:

$$R(p, \gamma_i) = \log_2 \left(1 + \frac{p\sigma^2}{2(1+\gamma_i\sigma_J^2) + \frac{(1+\gamma_i\sigma_J^2)^2}{p\sigma^2}} \right). \tag{17}$$

Note that the rate in (17) is independent of the instantaneous realizations of the fading coefficients; instead, the variations of the channel gains expressed through the variances σ^2, σ_J^2 determine the rate of the secret keys that can be extracted from the wireless medium. The overall W-SKG sum-rate can then be simply expressed as follows:

$$C_K(p, \underline{\gamma}) = \sum_{i=1}^{N} R(p, \gamma_i). \tag{18}$$

IV. Optimal Power Allocation Strategies

Alice and Bob's common objective is to maximize $C_K(p, \underline{\gamma})$ with respect to (w.r.t.) p, while Mallory wants to minimize $C_K(p, \underline{\gamma})$ w.r.t. $\underline{\gamma}$. Given the opposed objectives, a non-cooperative zero-sum game can be formulated to study the strategic interaction between the legitimate users and the jammer: $\mathcal{G} = (\{L, J\}, \{\mathcal{A}_\text{L}, \mathcal{A}_\text{J}(p)\}, C_K(p, \underline{\gamma}))$. The game $\mathcal{G}$ has three components. Firstly, there are two players: player L representing the legitimate users (Alice and Bob are considered to act as a single player) and player J representing the jammer (Mallory). Secondly, player L has a set of possible actions $\mathcal{A}_L = [0, P]$ while player J's set of actions is

$$\mathcal{A}_J(p) = \begin{cases} \{(0, \ldots, 0)\}, & \text{if } p \leq p_\text{th}, \\ \left\{\underline{\gamma} \in \mathbb{R}_+^N | \sum_{i=1}^{N} \gamma_i \leq N\Gamma\right\}, & \text{if } p > p_\text{th}. \end{cases} \tag{19}$$

At last, $C_K(p, \underline{\gamma})$, denotes the payoff function of player L.

Due to the fact that Mallory first observes the transmit power of the legitimate users on the subcarriers and then decides which strategy to choose (a consequence of player J being a reactive jammer), we study a hierarchical game in which player L is the leader and player J is the follower. In this hierarchical game, the solution is the Stackelberg equilibrium (SE) – rather than Nash – defined as a strategy profile $(p^\text{SE}, \underline{\gamma}^\text{SE})$ where player L chooses his optimal strategy first, by anticipating the strategic reaction of player J (i.e., its best response). This can be rigorously written as:

$$p^\text{SE} \triangleq \arg\max_{p \in \mathcal{A}_L} \sum_{i=1}^{N} R(p, \underline{\gamma}^*(p)), \text{ and } \underline{\gamma}^\text{SE} \triangleq \underline{\gamma}^*(p^\text{SE}), \tag{20}$$

where $\underline{\gamma}^*(p)$ denotes the jammer's best response (BR) function to any strategy $p \in \mathcal{A}_L$ chosen by player L, defined as follows:

$$\underline{\gamma}^*(p) \triangleq \arg\min_{\underline{\gamma} \in \mathcal{A}_J(p)} \sum_{i=1}^{N} R(p, \underline{\gamma}). \tag{21}$$

We also denote by $\gamma_i^*(p)$ the i-th component of $\underline{\gamma}^*(p)$.

A. Stackelberg equilibrium with fixed p_{th}

In the following, we evaluate the SE of the game $\mathcal{G}$ assuming that the threshold p_th is predefined and fixed. The case $P \leq p_\text{th}$ is trivial as $\underline{\gamma}^\text{SE} = (0, \ldots, 0)$, whereas, the legitimate users will optimally use the maximum available power so that $(p^\text{SE} = P)$. Indeed, because of the badly chosen threshold or low sensing capabilities of Mallory, the legitimate transmission will never be detected on any of the subcarriers and hence will not be jammed. In the following, we assume that: $P > p_\text{th}$.

Lemma 2: The BR of the jammer for any $p \in \mathcal{A}_L$ chosen by the leader defined in (21) is the uniform power allocation, such that:

$$\underline{\gamma}^*(p) \triangleq \begin{cases} (\Gamma, \ldots, \Gamma), & \text{if } p > p_\text{th}, \\ (0, \ldots, 0), & \text{if } p \leq p_\text{th}. \end{cases} \tag{22}$$

Proof: Note that $R(p, \gamma_i)$ is a monotonically decreasing convex function w.r.t γ_i, $i = 1, \ldots, N$ for any $p > 0$. We show that the jamming power should be equally distributed on all of the subcarriers. To prove this, we apply Jensen's inequality using $\delta_i > 0$, $\sum_{i=1}^{N} \delta_i = 1$, so that $R\left(p, \sum_{i=1}^{N} \delta_i x_i\right) \leq \sum_{i=1}^{N} \delta_i R(p, x_i)$. Substituting $\delta_i = 1/N$, $x_i = \Gamma/b_i$, we get:

$$R\left(p, \sum_{i=1}^{N} \frac{\Gamma}{N b_i}\right) \leq \sum_{i=1}^{N} \frac{1}{N} R\left(p, \frac{\Gamma}{b_i}\right) \Rightarrow$$
$$NR\left(p, \frac{1}{N} \sum_{i=1}^{N} \frac{\Gamma}{b_i}\right) \leq \sum_{i=1}^{N} R\left(p, \frac{\Gamma}{b_i}\right). \tag{23}$$

Applying the power constraint $\sum_{i=1}^{N} \Gamma/b_i \leq N\Gamma$ on the LHS of (23), for any $p > p_\text{th}$ we have:

$$NR(p, \Gamma) < \sum_{i=1}^{N} R\left(p, \frac{\Gamma}{b_i}\right) \Rightarrow C_K(p, (\Gamma, \ldots, \Gamma)) \leq C_K(p, \underline{\gamma}),$$

which shows that in order to minimize C_K, Mallory has to distribute her power equally on all subcarriers. ∎

In light of this result, the W-SKG sum rate can have two forms:

$$C_K(p, \underline{\gamma}^*(p)) = \begin{cases} NR(p, \Gamma), & \text{if } p > p_\text{th}, \\ NR(p, 0), & \text{if } p \leq p_\text{th}, \end{cases} \tag{24}$$

which simplifies the players' options. Next, we address the question of how Alice and Bob should choose their power p optimally.

Theorem 1: Depending on the available power P for W-SKG, player L will either transmit at P or p_th on all subcarriers. The SE point of the game is unique when $P \neq p_\text{th}(\sigma_J^2\Gamma + 1)$ and is given by

$$(p^\text{SE}, \underline{\gamma}^\text{SE}) = \begin{cases} \{(p_\text{th}, (0, \ldots, 0))\}, & \text{if } P < p_\text{th}(\sigma_J^2\Gamma + 1), \\ \{(P, (\Gamma, \ldots, \Gamma))\}, & \text{if } P > p_\text{th}(\sigma_J^2\Gamma + 1). \end{cases} \tag{25}$$

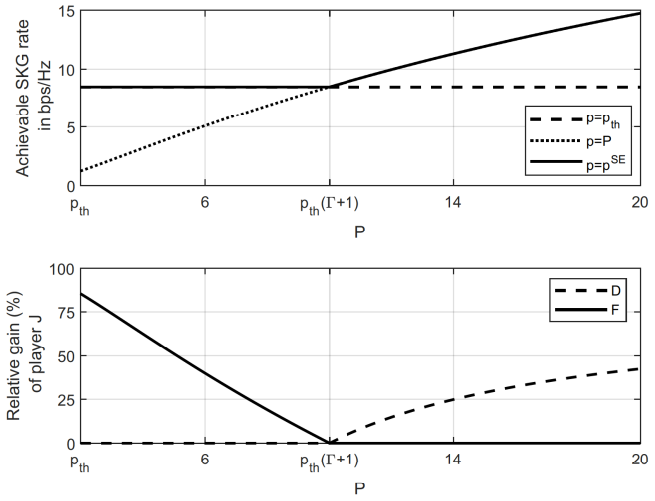

Fig. 2. UP: SE policy compared to always transmitting with either full power or with p_{th}. DOWN: Functions D and F vs P. In both sub-figures, $p_{\text{th}} = 2, \Gamma = 4, N = 10, \sigma^2 = \sigma_J^2 = 1$.

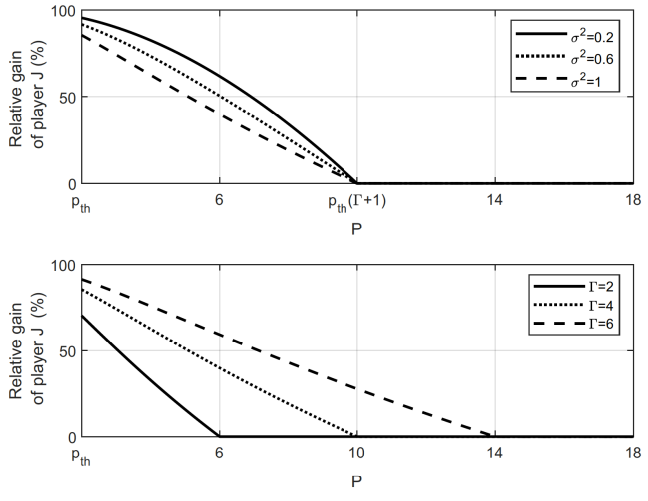

Fig. 3. Relative gain of player J, evaluated by function E, for strategic p_{th} and fixed $p_{\text{th}} = 2$ when $N = 10$, $\sigma_J^2 = 1$ and UP: $\Gamma = 4$, DOWN: $\sigma^2 = 1$.

When $P = p_{\text{th}}(\sigma_J^2\Gamma + 1)$, the game $\mathcal{G}$ has two SEs: $(p^{\text{SE}}, \underline{\gamma}^{\text{SE}}) \in \{(p_{\text{th}}, (0, \ldots, 0), (P, (\Gamma, \ldots, \Gamma)\}$.

Proof: Given the BR in (22) and the simplification in (24), player L wants to find the optimal $p \in \mathcal{A}_L$ that maximizes:

$$R(p, \gamma_i^*(p)) = \begin{cases} R(p, 0), & \text{if } p \leq p_{\text{th}}, \\ R(p, \Gamma), & \text{if } p > p_{\text{th}}. \end{cases} \tag{26}$$

Given that $R(p, \gamma)$ is monotonically increasing with p for fixed γ, two cases are distinguished: a) $p \in [0, p_{\text{th}}]$, b) $p \in (p_{\text{th}}, P]$. The optimal p in each case is given by

a) $\underset{p\in[0,p_{\text{th}}]}{\arg\max}\ R(p, \gamma_i^*(p)) = \underset{p\in[0,p_{\text{th}}]}{\arg\max}\ R(p, 0) = p_{\text{th}}$,

b) $\underset{p\in(p_{\text{th}},P]}{\arg\max}\ R(p, \gamma_i^*(p)) = \underset{p\in(p_{\text{th}},P]}{\arg\max}\ R(p, \Gamma) = P$.

From a) and b), we conclude that the overall solution is $p^{\text{SE}} = \underset{p\in\mathcal{A}_L}{\arg\max}\ R(p, \gamma_i^*(p)) = \begin{cases} p_{\text{th}}, & \text{if } R(P,\Gamma) < R(p_{\text{th}}, 0), \\ P, & \text{if } R(P,\Gamma) > R(p_{\text{th}}, 0), \\ \{p_{\text{th}}, P\}, & \text{if } R(P,\Gamma) = R(p_{\text{th}}, 0). \end{cases}$

To specify clearly the three possibilities in function of the system parameters, we can focus on the case $R(P, \Gamma) = R(p_{\text{th}}, 0)$. Using this equality, and by substituting appropriately into (17), we obtain a quadratic equation in P:

$$P^2(2\sigma^2 p_{\text{th}}+1) - P(2{p_{\text{th}}}^2\sigma^2 + 2\sigma_J^2\Gamma{p_{\text{th}}}^2\sigma^2) - (1+\sigma_J^2\Gamma)^2{p_{\text{th}}}^2 = 0,$$

which has a unique positive root equal to $p_{\text{th}}(\sigma_J^2\Gamma + 1)$. Given that $(2\sigma^2 p_{\text{th}} + 1) \geq 0$ and that $P > 0$ the inequalities $R(P, \Gamma) > R(p_{\text{th}}, 0)$ and $R(P, \Gamma) < R(p_{\text{th}}, 0)$ are equivalent to $P > p_{\text{th}}(\sigma_J^2\Gamma + 1)$ and $P < p_{\text{th}}(\sigma_J^2\Gamma + 1)$, respectively. ■

Some numerical results are presented in Fig. 2 for a total number of SKG subcarriers $N = 10$ (pertinent to narrowband IoT applications), $p_{\text{th}} = 2$, $\Gamma = 4$, and $\sigma^2 = \sigma_J^2 = 1$. The top figure compares the achievable rates of the SE strategy and of two alternative strategies consisting in transmitting with fixed $p = P$ or $p = p_{\text{th}}$. The bottom figure depicts the following quantities:

$$F = \frac{C_K(p^{\text{SE}}, \underline{\gamma}^{\text{SE}}) - C_K(P, (\Gamma, \ldots, \Gamma))}{C_K^{SE}}, \tag{27}$$

$$D = \frac{C_K(p^{\text{SE}}, \underline{\gamma}^{\text{SE}}) - C_K(p_{\text{th}}, (0, \ldots, 0))}{C_K^{SE}}, \tag{28}$$

where F and D represent the jammer's gain (or legitimate users' loss) if player L deviates from the SE point (indeed, if player L transmits at $P > p_{th}$, the jammer will jam at $\gamma_i^*(P) = \Gamma$; and if player L transmits at p_{th} the jammer will not detect it and will remain silent). Both figures show that deviating from the SE point can decrease the achievable sum-rates by up to 85%.

B. Stackelberg equilibrium with strategic p_{th}

Finally, we investigate how Mallory could optimally adjust p_{th} and how her choice will impact Alice's and Bob's strategies. Allowing p_{th} to vary modifies the game under study as follows $\hat{\mathcal{G}} = (\{L, J\}, \{\mathcal{A}_L, \hat{\mathcal{A}}_J(p)\}, C_K(p, \underline{\gamma}, p_{\text{th}}))$, where:

$$\hat{\mathcal{A}}_J(p) \triangleq \begin{cases} \{((0, \ldots, 0), p_{\text{th}}),\ p_{\text{th}} \geq 0\}, & \text{if } p_{\text{th}} \geq p, \\ \left\{(\underline{\gamma}, p_{\text{th}}) \in \mathbb{R}_+^{N+1} \mid \sum_{i=1}^N \gamma_i \leq N\Gamma\right\}, & \text{if } p_{\text{th}} < p. \end{cases} \tag{29}$$

The BR of jammer can then be defined as:

$$(\widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}^*(p)) \triangleq \underset{(\underline{\gamma}, p_{\text{th}}) \in \hat{\mathcal{A}}_J(p)}{\arg\min}\ C_K(p, \underline{\gamma}, p_{\text{th}}). \tag{30}$$

Lemma 3: The best response of player J in this case is a set of strategies:

$$(\widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}^*(p)) \in \{\ ((\Gamma, \ldots, \Gamma), \epsilon),\ \epsilon \in [0, p)\}. \tag{31}$$

Proof: The problem that the jammer wants to solve is: $\min_{(\underline{\gamma}, p_{\text{th}}) \in \hat{\mathcal{A}}_J(p)} C_K(p, \underline{\gamma}, p_{\text{th}})$, which can be split as follows:

$$\min_{p_{\text{th}} \geq 0}\ \min_{\underline{\gamma} \in \hat{\mathcal{A}}_J(p)} C_K(p, \underline{\gamma}(p), p_{\text{th}}). \tag{32}$$

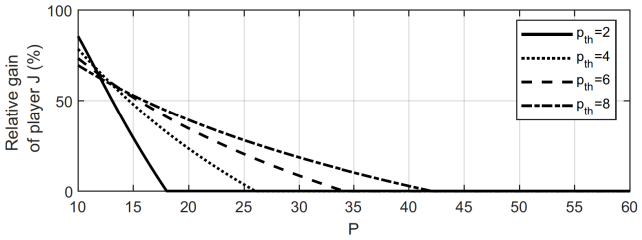

Fig. 4. Relative gain of player J, evaluated by function E, for different values of p_{th} for $N = 10$, $\sigma_J^2 = 1$ and $\Gamma = 4$.

The solution of the inner minimization is already known from (22). For the outer problem we have to find the optimal $p_{\text{th}} \geq 0$ that minimizes $C_K(p, \widehat{\underline{\gamma}}^*(p), p_{\text{th}})$. Given that:

$$\min_{p_{\text{th}} \geq 0} C_K(p, \widehat{\underline{\gamma}}^*(p), p_{\text{th}}) = \begin{cases} NR(p, \Gamma, p_{\text{th}}), & \text{if } p_{\text{th}} < p, \\ NR(p, 0, p_{\text{th}}), & \text{if } p_{\text{th}} \geq p, \end{cases} \tag{33}$$

and that $R(p, \Gamma, p_{\text{th}}) < R(p, 0, p_{\text{th}})$ the jammer can optimally choose any threshold such that $p_{\text{th}} = \epsilon, \quad \forall \epsilon < p$. ■

Theorem 2: The game $\hat{\mathcal{G}}$ has an infinite number of SEs:

$$(\widehat{p}^{\text{SE}}, \widehat{\underline{\gamma}}^{\text{SE}}, \widehat{p_{\text{th}}}^{\text{SE}}) \in \{ \ (P, (\Gamma, \ldots, \Gamma), \epsilon), \quad \forall \epsilon < P \}. \tag{34}$$

Proof: Given the BR of player J, we will now evaluate the SE of the game $\hat{\mathcal{G}}$. The definition for $\widehat{p}^{\text{SE}}$ is given as:

$$\widehat{p}^{\text{SE}} \triangleq \underset{p \in \mathcal{A}_L}{\arg} \max C_K(p, \widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}(p)^*). \tag{35}$$

Since the jammer will act as in (31), we have:

$$C_K(p, \widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}(p)^*) = NR(p, \Gamma, \epsilon), \ \forall \epsilon < p, \tag{36}$$

and the fact that $R(p, \Gamma, \epsilon)$ is monotonically increasing with p results in $\widehat{p}^{\text{SE}} = P$. ■

Fig. 3 and Fig. 4 illustrate the gain of the jammer (or the loss in W-SKG rate) when p_{th} is part of her strategy, with utility function $C_K(p, \underline{\gamma}, p_{\text{th}})$, compared to the case when it is not, with utility function $C_K(p, \underline{\gamma})$. We evaluate this gain by:

$$E = \frac{C_K(p^{SE}, \underline{\gamma}^{SE}) - C_K(\widehat{p}^{SE}, \widehat{\underline{\gamma}}^{SE}, \widehat{p_{\text{th}}}^{SE})}{C_K(p^{SE}, \underline{\gamma}^{SE})}. \tag{37}$$

As in Fig. 2 the total number of subcarriers is $N = 10$ and $\sigma_J^2 = 1$. The non-strategic threshold on Fig. 3 is set to $p_{\text{th}} = 2$ and the quantity E is evaluated for different values of σ^2 and Γ. The numerical results demonstrate that when p_{th} is part of Mallory's strategy, she can be a significantly more effective opponent, compared to the case when p_{th} is fixed, confirming that reactive jammers can indeed pose a serious threat. This is also confirmed by the results on Fig. 4 where the relative gain of the jammer is presented for different p_{th}. As expected with decreasing the threshold her gain increases.

V. Conclusions

In this study, injection and reactive jamming attacks were analyzed in W-SKG systems and optimal power allocation policies were investigated in BF-AWGN channels. It was shown that pilot randomization can reduce injection MiM attacks to less harmful jamming attacks. An intelligent reactive jammer should optimally jam with equal power on the whole spectrum. Furthermore, a strategically chosen jamming threshold just below the power level used by the legitimate users, allows the adversary to launch a much more effective attack. In this case, the legitimate users have no choice but to transmit at full power.

Acknowledgements

M. Mitev is supported by the Doctoral Training Programme of CSEE, University of Essex, A. Chorti and E.V. Belmega are supported by the ELIOT ANR-18-CE40-0030 and FAPESP 2018/12579-7 project and M.J. Reed is supported by the project SerIoT which has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 780139.

References

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, 2018.

[2] E. Jorswieck, S. Tomasin, and A. Sezgin, "Boradcasting into the uncertainty: authentication and confidentiality by physical layer processing," *Proc. IEEE, invited paper*, vol. 103, pp. 1702–1724, Oct. 2015.

[3] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[4] C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness," in *Proc. IEEE Conf. CNS*, IT, Sep. 2015, pp. 113–118.

[5] S. Premnath, J. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthyn, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, pp. 917–930, 2013.

[6] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *IEEE 14th Workshop SPAWC*, Darmastd, DE, Jun. 2013, pp. 669–673.

[7] W. Xu, S. Jha, and W. Hu, "LoRa-key: Secure key generation system for LoRa-based network," *IEEE Internet Things J.*, 2019 (early access).

[8] A. Chorti, "A study of injection and jamming attacks in wireless secret sharing systems," *Springer, L. Notes El. Eng.*, pp. 1–14, Jan. 2018.

[9] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, Nov. 2017.

[10] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annual Int. Conf. Mobile Comput. Netw.* ACM, 2009, pp. 321–332.

[11] S. Eberz, M. Strohmeier, M. Wilhelm and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Proc. 17th ESORICS*, 2012, pp. 235–252.

[12] J. Rong and Z. Kai, "Physical layer key agreement under signal injection attacks," in *IEEE Conf. CNS*, 2015, pp. 254–262.

[13] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ: John Wiley and Sons, Inc., 2006.

[14] S. Fang, Y. Liu and P. Ning , "Wireless communications under broadband reactive jamming attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 3, pp. 394 – 408, May 2016.

[15] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1593 – 1603, May 2014.