entropy

Article

Protecting Physical Layer Secret Key Generation from Active Attacks

Miroslav Mitev [1,*], Arsenia Chorti [2], E. Veronica Belmega [2] and H. Vincent Poor [3]

[1] Barkhausen Institut gGmbH, Würzburger Str. 46, 01187 Dresden, Germany
[2] ETIS, UMR 8051 CY Cergy Paris Université, ENSEA, CNRS, 95000 Cergy, France; arsenia.chorti@ensea.fr (A.C.); veronica.belmega@ensea.fr (E.V.B.)
[3] School of Engineering and Applied Science, Princeton University, Princeton, NJ 08544, USA; poor@princeton.edu
* Correspondence: Miroslav.Mitev@barkhauseninstitut.org

Abstract: Lightweight session key agreement schemes are expected to play a central role in building Internet of things (IoT) security in sixth-generation (6G) networks. A well-established approach deriving from the physical layer is a secret key generation (SKG) from shared randomness (in the form of wireless fading coefficients). However, although practical, SKG schemes have been shown to be vulnerable to active attacks over the initial "advantage distillation" phase, throughout which estimates of the fading coefficients are obtained at the legitimate users. In fact, by injecting carefully designed signals during this phase, a man-in-the-middle (MiM) attack could manipulate and control part of the reconciled bits and thus render SKG vulnerable to brute force attacks. Alternatively, a denial of service attack can be mounted by a reactive jammer. In this paper, we investigate the impact of injection and jamming attacks during the advantage distillation in a multiple-input–multiple-output (MIMO) system. First, we show that a MiM attack can be mounted as long as the attacker has one extra antenna with respect to the legitimate users, and we propose a pilot randomization scheme that allows the legitimate users to successfully reduce the injection attack to a less harmful jamming attack. Secondly, by taking a game-theoretic approach we evaluate the optimal strategies available to the legitimate users in the presence of reactive jammers.

Keywords: physical layer security; secret key generation; injection attacks; jamming attacks; pilot randomization

check for updates

Citation: Mitev, M.; Chorti, A.; Belmega, E.V.; Poor, H.V. Protecting Physical Layer Secret Key Generation from Active Attacks. *Entropy* **2021**, *23*, 960. https://doi.org/10.3390/e23080960

Academic Editor: Ivan B. Djordjevic

Received: 15 June 2021
Accepted: 23 July 2021
Published: 27 July 2021

1. Introduction

The increasing interest in physical layer security (PLS) has been stimulated by many practical needs, particularly in the context of Internet of things (IoT) applications [1]. For example, in [2,3], secret key generation (SKG) from wireless fading coefficients was analyzed, showing its potential as a lightweight alternative to standard security schemes. In fact, the SKG scheme allows two legitimate parties (Alice and Bob) to extract on-the-fly secret keys, without the need for significant infrastructure. Furthermore, it has been information-theoretically proven that by following the SKG process, Alice and Bob can extract a shared secret over unauthenticated channels [4–6]. Building on that, numerous practical experiments have demonstrated the feasibility of the scheme [7,8]. Moreover, it has been shown that SKG can be combined with authenticated encryption (AE) schemes [9,10] in order to overcome trivial man-in-the-middle (MiM) attacks, similarly to known MiM attacks on unauthenticated Diffie–Hellman schemes.

The success of the SKG scheme relies on the reciprocity and variability of wireless channels. On the one hand, the reciprocity property allows both Alice and Bob to measure an identical channel impulse response during the coherence time of the channel [11–13], while on the other hand, the variability property of the wireless channel directly affects the key generation rates [14–17].

However, the exchange of pilots during the channel estimation phase between Alice and Bob could allow an adversary (Mallory) to estimate the channels Alice–Mallory and Bob–Mallory. Having this information, Mallory could inject suitably precoded signals during the SKG process and could potentially control a significant part of the reconciled sequence while remaining undetected. To overcome this, instead of transmitting publicly known pilot signals, we propose a two-way randomized pilot transmission between Alice and Bob. An earlier work studied this problem for an orthogonal frequency-division multiplexing (OFDM) system [18]. Here, we investigate the scenario of a multiple-input–multiple-output (MIMO) system. We prove that if Mallory has one extra antenna with respect to Alice and Bob, she could always launch an injection attack. Next, through theoretical analysis, we show that the proposed pilot randomization scheme successfully reduces an injection attack to a less harmful uncorrelated jamming attack, ensuring that the extracted key bits are secret from both active and passive adversaries.

In the second part of this paper, we delve deeper into jamming attacks over MIMO systems. In particular, we focus on denial of service (DoS) in the form of reactive jamming. We derive the optimal strategies for both the attacker and the legitimate users. Through numerical evaluation, we demonstrate that, depending on their capabilities, reactive jammers could provoke legitimate users to transmit at full power in order to achieve a positive SKG rate.

2. System Model

In this work, we consider a time-division duplex MIMO (TDD–MIMO) system consisting of two legitimate nodes and an active adversary, namely, Alice, Bob, and Mallory, respectively. On the one hand, Alice and Bob are generating secret keys using the wireless SKG procedure, while on the other hand, Mallory performs an injection attack on the MIMO links Mallory–Alice and Mallory–Bob. The number of antennas at Alice N_A and Bob N_B are assumed to be equal, i.e., $N_A = N_B = N$. To better illustrate the considered scenario, we give a brief overview of the SKG procedure, and show how an injection attack could affect the process.

2.1. Secret Key Generation from Fading Coefficients

As illustrated in Figure 1, the standard SKG procedure consists of three phases [19]: (1) advantage distillation: the legitimate nodes exchange pilot signals, each using N transmit and N receive antenna elements, in order to estimate their reciprocal channel state information (CSI).

$$\mathbf{z}_A = \mathbf{H}\mathbf{x} + \mathbf{n}_A \tag{1}$$

$$\mathbf{z}_B = \mathbf{H}^T\mathbf{x} + \mathbf{n}_B, \tag{2}$$

where $\mathbf{H}$ represents the channel matrix of size $N_r \times N_t = N \times N$ such that its (i,j) entry represents the channel linking the i-th receive antenna, and the j-th transmit antenna, $\mathbf{z}$ represents the received vector of length N_r, $\mathbf{x}$ denotes the transmitted vector consisting of $N_t = N_r = N$ elements, $\mathbf{n}_A$ and $\mathbf{n}_B$ are the received noise vectors at Alice and Bob, each of length N_r, respectively. Note that, due to the reciprocity of the wireless channel, Alice and Bob observe $\mathbf{H}$ and $\mathbf{H}^T$, respectively. To conclude this step, $\mathbf{z}_A$ and $\mathbf{z}_B$ are passed through suitable quantizers [20], generating binary vectors $\mathbf{r}_A$ and $\mathbf{r}_B$, respectively; (2) information reconciliation: discrepancies, due to imperfect channel estimation in the quantizer local outputs, are reconciled through a public exchange of helper data $\mathbf{s}_A$ (see Figure 1), e.g., by using Slepian–Wolf reconciliation techniques [10,21]; (3) privacy amplification: the legitimate nodes apply universal hash functions to the reconciled information $\mathbf{r}_A$ and obtain key $\mathbf{k}$. This step ensures that the generated key $\mathbf{k}$ is uniformly distributed and completely unpredictable by an adversary.

During the process above, an eavesdropping adversary could obtain channel observations, given as follows:

$$\mathbf{z}_{AM} = \mathbf{H}_{AM}\mathbf{x} + \mathbf{n}_{AM}, \tag{3}$$
$$\mathbf{z}_{BM} = \mathbf{H}_{BM}\mathbf{x} + \mathbf{n}_{BM}, \tag{4}$$

where the channel matrices in the links Alice–Mallory and Bob–Mallory are denoted by $\mathbf{H}_{AM}$ and by $\mathbf{H}_{BM}$, respectively, while the received noise vectors are demoted by $\mathbf{n}_{AM}$ and $\mathbf{n}_{BM}$. Afterward, the SKG capacity between Alice and Bob is expressed as the conditional mutual information between the observations of Alice, Bob, and Mallory.

$$I(\mathbf{z}_A; \mathbf{z}_B | \mathbf{z}_{AM}, \mathbf{z}_{BM}). \tag{5}$$

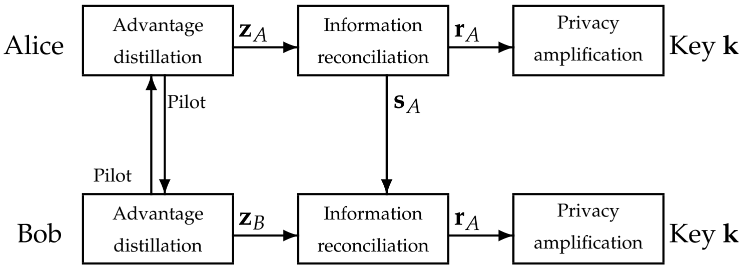

Figure 1. Secret key generation process between Alice and Bob.

2.2. Injection Attacks during SKG

One of the most critical threats to the SKG model, given in Figure 1, is MiM in the form of an injection attack [11,22,23]. The main components of the injection attack are captured in Figure 2. While, the legitimate nodes Alice and Bob exchange pilot signals during the advantage distillation phase, Mallory injects signals $\mathbf{p}$. Based on the results in [22], we assume that Mallory has perfect knowledge of the channel vectors in the MIMO links Mallory–Alice, $\mathbf{H}_{MA} = \mathbf{H}_{AM}^T$ and Mallory–Bob, $\mathbf{H}_{MB} = \mathbf{H}_{BM}^T$. This is a reasonable assumption 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). Finally, Mallory chooses the vector $\mathbf{p}$ such that the same signal is "injected" at both Alice and Bob, i.e., $\mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}$.

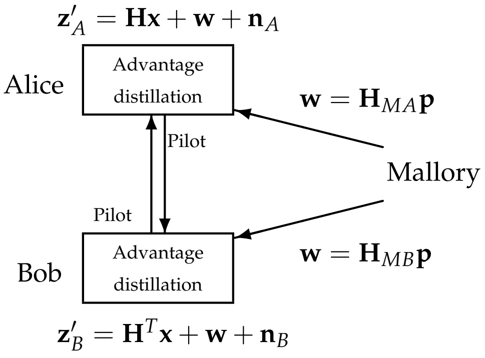
$\mathbf{z}'_A = \mathbf{H}\mathbf{x} + \mathbf{w} + \mathbf{n}_A$
Alice
Advantage distillation
$\mathbf{w} = \mathbf{H}_{MA}\mathbf{p}$
Pilot
Mallory
Pilot
Bob
Advantage distillation
$\mathbf{w} = \mathbf{H}_{MB}\mathbf{p}$
$\mathbf{z}'_B = \mathbf{H}^T\mathbf{x} + \mathbf{w} + \mathbf{n}_B$

Figure 2. Injection attack performed by Mallory: While Alice and Bob exchange pilot signals $\mathbf{x}$ over a Rayleigh fading channel with realization $\mathbf{H}$, Mallory injects a signal $\mathbf{p}$ such that the received signals at both Alice and Bob coincide $\mathbf{w} = \mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}$.

3. Analysis of Injection Attacks in MIMO SKG

In this section, we first prove that if Mallory has one extra antenna, with respect to Alice and Bob, she could always launch an injection attack. Next, we propose a pilot randomization scheme and show that when employed, legitimate users could successfully reduce the attack to a jamming attack.

Lemma 1. *While Alice and Bob perform advantage distillation using N antennas, Mallory could always launch an injection attack, as long as she has at least $N+1$ antennas.*

Proof. The precoding vector of Mallory $\mathbf{p}$ of size $(N+1)\times 1$ is represented as

$$\mathbf{p} = \begin{bmatrix} p_1 \\ \vdots \\ p_{N+1} \end{bmatrix}. \tag{6}$$

The channel matrices $\mathbf{H}_{MA}$ and $\mathbf{H}_{MB}$ have size $N \times (N+1)$, such that

$$\mathbf{H}_{MA} = \begin{bmatrix} H_{MA_{1,1}} & \cdots & H_{MA_{1,N+1}} \\ \vdots & \dots & \vdots \\ H_{MA_{N,1}} & \cdots & H_{MA_{N,N+1}} \end{bmatrix}, \tag{7}$$

and

$$\mathbf{H}_{MB} = \begin{bmatrix} H_{MB_{1,1}} & \cdots & H_{MB_{1,N+1}} \\ \vdots & \dots & \vdots \\ H_{MB_{N,1}} & \cdots & H_{MB_{N,N+1}} \end{bmatrix}. \tag{8}$$

Next, we can represent the equation

$$\mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}, \tag{9}$$

as

$$(\mathbf{H}_{MA} - \mathbf{H}_{MB})\mathbf{p} = 0, \tag{10}$$

where $\mathbf{H}_M = \mathbf{H}_{MA} - \mathbf{H}_{MB}$ is equal to:

$$\mathbf{H}_M = \begin{bmatrix} H_{MA_{1,1}} - H_{MB_{1,1}} & \cdots & H_{MA_{1,N+1}} - H_{MB_{1,N+1}} \\ \vdots & \dots & \vdots \\ H_{MA_{N,1}} - H_{MB_{N,1}} & \cdots & H_{MA_{N,N+1}} - H_{MB_{N,N+1}} \end{bmatrix}. \tag{11}$$

Given the above, Equation (10) can be rewritten as $\mathbf{H_M}\mathbf{p} = 0$, where $\mathbf{H_M}$ is given in Equation (11). The equality $\mathbf{H_M}\mathbf{p} = 0$ is equivalent to solving the following linear system of equations:

$$\begin{cases} H_{M_{1,1}}p_1 + H_{M_{1,2}}p_2 + \cdots + H_{M_{1,N+1}}p_{N+1} & = \quad 0 \\ \qquad \vdots & \\ H_{M_{N,1}}p_1 + H_{M_{N,2}}p_2 + \cdots + H_{M_{N,N+1}}p_{N+1} & = \quad 0. \end{cases} \tag{12}$$

Due to the fact that Mallory has an additional degree of freedom (one extra antenna), as compared to Alice and Bob, she can treat one of the elements in $\mathbf{p}$ as a constant and solve for the others in terms of it. Based on this, we let p_{N+1} be a constant and rewrite the system in (12) as

$$\begin{cases} H_{M_{1,1}}p_1 + H_{M_{1,2}}p_2 + \cdots + H_{M_{1,N}}p_N & = \quad -H_{M_{1,N+1}}p_{N+1} \\ \qquad \vdots & \\ H_{M_{N,1}}p_1 + H_{M_{N,2}}p_2 + \cdots + H_{M_{N,N}}p_N & = \quad -H_{M_{N,N+1}}p_{N+1}. \end{cases} \tag{13}$$

The system of equations in (13) can be represented as $\mathbf{A}\mathbf{x} = \mathbf{b}$, where the $N \times N$ matrix $\mathbf{A}$ is the $N \times N$ matrix containing the first N lines and N columns of $\mathbf{H}_M$, $\mathbf{x} = (p_1, p_2, \ldots, p_N)^T$, and $\mathbf{b}$ contains the right-hand side of the system, i.e., $\mathbf{b} = (-H_{M_{1,N+1}}p_{N+1}, \ldots, -H_{M_{N,N+1}}p_{N+1})^T$.

Finally, since $\det(\mathbf{A}) \neq 0$ almost surely, (i.e., under the assumptions in Section 2, $\det(\mathbf{A})$ is a continuous random variable, hence $\det(\mathbf{A}) \neq 0$ with probability 1) and therefore the system's solution is unique and given by

$$(p_1, p_2, \ldots, p_N)^T = \mathbf{A}^{-1}\mathbf{b}. \tag{14}$$

Note that if Mallory has the same number of antennas as Alice and Bob, she will not have one extra degree of freedom and the transition from the system in Equation (12) to the system in Equation (13) would not be possible. However, as shown here, if Mallory has one extra antenna, with respect to Alice and Bob, she can treat one of the elements in $\mathbf{p}$ as constant, which allows her to find the rest of the elements as in Equation (14). This concludes the proof of Lemma 1. □

Based on Lemma 1, the observations of Alice and Bob are now given by

$$\mathbf{z}_A = \mathbf{H}\mathbf{x} + \mathbf{w} + \mathbf{n}_A \tag{15}$$

$$\mathbf{z}_B = \mathbf{H}^T\mathbf{x} + \mathbf{w} + \mathbf{n}_B, \tag{16}$$

where $\mathbf{w} = \mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}$ denotes the observed injected signals at Alice and Bob, which are identical due to the precoding vector $\mathbf{p}$. By injecting $\mathbf{w}$, Mallory controls the secret key rate, which is now upper bounded by [18,24]

$$L \leq I(\mathbf{z}_A, \mathbf{z}_B; \mathbf{w}). \tag{17}$$

Pilot Randomization as a Countermeasure to Injection Attacks

It has been shown that a countermeasure to injection attacks can be built by randomizing the pilot sequence exchanged between Alice and Bob [18,23,24]. In this work, we propose a MIMO pilot randomization scheme in which pilots are drawn from a (scaled) QPSK modulation. Specifically, Alice and Bob do not transmit the same pilot signal $\mathbf{x}$; instead, they transmit independent, random pilot signals $\mathbf{x}$ and $\mathbf{y}$ drawn from i.i.d. zero-mean discrete uniform distributions in which the individual elements of the vectors have probability mass functions as $\mathcal{U}(\{\pm r \pm jr\}, \ldots, \{\pm r \pm jr\})$, where $j = \sqrt{-1}, r = \sqrt{P/2}$, so that $\mathbb{E}[\mathbf{x}] = \mathbb{E}[\mathbf{y}] = (0, \ldots, 0)^T$, $(\mathbb{E}[|x_1|^2], \ldots, \mathbb{E}[|x_N|^2])^T = (\mathbb{E}[|y_1|^2], \ldots, \mathbb{E}[|y_N|^2])^T = (P, \ldots, P)^T$ and $(\mathbb{E}[x_1 y_1], \ldots, \mathbb{E}[x_N y_N])^T = (0, \ldots, 0)^T$, i.e., the pilots are randomly chosen QPSK signals. Given that Alice's and Bob's observation $\mathbf{z}_A$ and $\mathbf{z}_B$ are modified as

$$\mathbf{z}_A = \mathbf{H}\mathbf{y} + \mathbf{w} + \mathbf{n}_A, \tag{18}$$

$$\mathbf{z}_B = \mathbf{H}^T\mathbf{x} + \mathbf{w} + \mathbf{n}_B. \tag{19}$$

Finally, to generate shared randomness, Alice and Bob post-multiply $\mathbf{z}_A$ and $\mathbf{z}_B$ by their own randomized pilot signals, such as $\tilde{z}_A = \mathbf{x}^T\mathbf{z}_A$ and $\tilde{z}_B = \mathbf{y}^T\mathbf{z}_B$ (unobservable by Mallory). Given this, the modified observations are expressed as

$$\tilde{z}_A \;=\; \mathbf{x}^T\mathbf{H}\mathbf{y} + \mathbf{x}^T\mathbf{w} + \mathbf{x}^T\mathbf{n}_A, \tag{20}$$

$$\tilde{z}_B \;=\; \mathbf{y}^T\mathbf{H}^T\mathbf{x} + \mathbf{y}^T\mathbf{w} + \mathbf{y}^T\mathbf{n}_B, \tag{21}$$

where the shared randomness between Alice and Bob is now represented by $\mathbf{x}^T\mathbf{H}\mathbf{y} = \mathbf{x}\mathbf{H}^T\mathbf{y}^T$. Furthermore, the independence of $\mathbf{x}$ and $\mathbf{y}$ ensures the following:

$$L \leq I(\tilde{z}_A, \tilde{z}_B; \mathbf{w}) = 0. \tag{22}$$

4. Jamming Attacks on SKG

In this section, we focus on reactive jamming attacks in SKG systems and examine the scenario in which Mallory reactively jams Alice (note that the scenario in which Mallory jams Bob is identical). A reactive jamming attack is an intelligent approach in which the jammer initially senses the spectrum and jams only if a transmission is detected. Due to the difficulty to be detected, reactive jamming attacks are considered to be a great threat to legitimate transmission [25,26]. Next, we assume that Alice and Bob perform SKG in a TDD–MIMO system with a spatially uncorrelated channel. It has been proven that the optimal power strategy for Alice and Bob in this scenario is to employ equal power distribution [27], which is also assumed for this study, i.e.,

$$\left(\mathbb{E}\left[|x_1|^2\right],\ldots,\mathbb{E}\left[|x_N|^2\right]\right)^T = (p,\ldots,p)^T \text{ with } p \in [0,P]. \tag{23}$$

In the following, we assume that Mallory has N antennas, and as a reactive jammer, she senses the spectrum and jams in the link Mallory–Alice only if she detects a power greater than a certain threshold p_{th}. Thus, instead of considering Mallory's power allocation matrix, we work with the sum jamming power for all antennas, which can be represented as a power allocation vector $\underline{\gamma} = (\gamma_1,\ldots,\gamma_N)$. By denoting the available jamming power by $N\Gamma$, the following short-term power constraint is considered:

$$\underline{\gamma} \in \mathbb{R}_+^N, \quad \sum_{i=1}^{N} \gamma_i \leq N\Gamma. \tag{24}$$

Assuming that $\mathbf{H}$ is uncorrelated with $\mathbf{H}_{AM}, \mathbf{H}_{BM}$ and that all channel matrices have independent and identically distributed elements that are drawn from circularly symmetric zero-mean Gaussian distributions of variances σ^2 and σ_J^2, respectively, then the SKG capacity can be expressed as [27]

$$C_K(p,\underline{\gamma}) = N\sum_{i=1}^{N} \log\left(1 + \frac{p\sigma^2}{2(1+\gamma_i\sigma_J^2) + \frac{(1+\gamma_i\sigma_J^2)^2}{p\sigma^2}}\right). \tag{25}$$

4.1. Optimal Power Allocation Strategies

In the following, we take a game-theoretic approach in order to evaluate the optimal strategies of Alice, Bob and Mallory. Throughout the following 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. $\underline{\gamma}$. Due to the reversed objectives, we formulated a noncooperative zero-sum game, which studies 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: (i) there are two players, namely, L, denoting the legitimate users (Alice and Bob act as a single player), and J being the jammer (Mallory); (ii) player L has a set of possible actions $\mathcal{A}_L = [0,P]$, while player J's set of actions is

$$\mathcal{A}_J(p) = \begin{cases} \{(0,\ldots,0)\}, & \text{if } p \leq p_{\text{th}}, \\ \left\{\underline{\gamma} \in \mathbb{R}_+^N \,|\, \sum_{i=1}^N \gamma_i \leq N\Gamma\right\}, & \text{if } p > p_{\text{th}}. \end{cases} \tag{26}$$

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

Given the fact that player J is a reactive jammer, i.e, first observes the transmit power of player L and subsequently chooses a strategy, we study a hierarchical game in which player L is the leader, and player J is the follower. In this game, the solution is the Stackelberg equilibrium (SE)—rather than Nash—and it is defined as a strategy profile $(p^{\text{SE}},\underline{\gamma}^{\text{SE}})$ where player L chooses their optimal strategy first, by anticipating the strategic reaction of player J (i.e., its best response). This is expressed as:

$$p^{\text{SE}} \triangleq \arg\max_{p\in\mathcal{A}_L} C_K(p,\underline{\gamma}^*(p)), \text{ and } \underline{\gamma}^{\text{SE}} \triangleq \underline{\gamma}^*(p^{\text{SE}}), \tag{27}$$

where $\underline{\gamma}^*(p)$ defines the best response (BR) of player J to any strategy $p \in \mathcal{A}_L$ chosen by player L, and it is defined as follows:

$$\underline{\gamma}^*(p) \triangleq \underset{\underline{\gamma} \in \mathcal{A}_J(p)}{\arg\min} C_K(p, \underline{\gamma}). \tag{28}$$

Finally, based on the detection capabilities at player L, two scenarios are considered: (i) when the detection threshold p_{th} is fixed (defined by the sensing capability of Mallory's receiver); (ii) when p_{th} is part of player L's strategy and could vary.

4.2. Stackelberg Equilibrium with Fixed Detection Threshold

In this section, we evaluate SE, when player J's detection threshold p_{th} is predefined and constant. Note that the case $P \leq p_{\text{th}}$ is trivial as $\underline{\gamma}^{\text{SE}} = (0, \ldots, 0)$, and the legitimate users will optimally use their maximum available power, i.e., $(p^{\text{SE}} = P)$. Indeed, due to the poorly chosen threshold p_{th} or low sensing capabilities of Mallory, the legitimate transmission will not be detected and therefore will not be jammed. In the following, we assume that $P > p_{\text{th}}$.

Lemma 2. *The BR of player J for any $p \in \mathcal{A}_L$ chosen by player L defined in (28) is the uniform power allocation, given as*

$$\underline{\gamma}^*(p) \triangleq \begin{cases} (\Gamma, \ldots, \Gamma), & \text{if } p > p_{th}, \\ (0, \ldots, 0), & \text{if } p \leq p_{th}. \end{cases} \tag{29}$$

Proof. Note that $C_K(p, \gamma_i)$ is a monotonically decreasing convex function w.r.t γ_i, $i = 1, \ldots, N$ for any $p > 0$. Based on the principles of convexity in order to minimize C_K, Mallory has to transmit with full power from all antennas. The detailed proof can be found in [18]. □

Based on the result from Lemma 1, the SKG rate can have the following two forms:

$$C_K(p, \underline{\gamma}^*(p)) = \begin{cases} C_K(p, (0, \ldots, 0)), & \text{if } p \leq p_{\text{th}}, \\ C_K(p, (\Gamma, \ldots, \Gamma)), & \text{if } p > p_{\text{th}}, \end{cases} \tag{30}$$

which simplifies the players' options.

Theorem 1. *Depending on their available power P for SKG, Alice and Bob will either transmit at P or p_{th}. The SE point of the game is unique when $P \neq p_{th}(\Gamma\sigma_J^2 + 1)$ and is given by*

$$(p^{SE}, \underline{\gamma}^{SE}) = \begin{cases} \{(p_{th}, (0, \ldots, 0))\}, & \text{if } P < p_{th}(\sigma_J^2\Gamma + 1), \\ \{(P, (\Gamma, \ldots, \Gamma))\}, & \text{if } P > p_{th}(\sigma_J^2\Gamma + 1). \end{cases} \tag{31}$$

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

Proof. Given the BR of player J defined in (29), the legitimate users want to identify their optimal $p \in \mathcal{A}_L$ that maximizes

$$C_K(p, \underline{\gamma}^*(p)) = \begin{cases} C_K(p, (0, \ldots, 0)), & \text{if } p \leq p_{\text{th}}, \\ C_K(p, (\Gamma, \ldots, \Gamma)), & \text{if } p > p_{\text{th}}, \end{cases} \tag{32}$$

Given the fact that $C_K(p, \underline{\gamma})$ is monotonically increasing with p for fixed $\underline{\gamma}$, 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) $\underset{p \in [0, p_{\text{th}}]}{\arg\max}\, C_K(p, \underline{\gamma}^*(p)) = \underset{p \in [0, p_{\text{th}}]}{\arg\max}\, C_K(p, (0, \ldots, 0) = p_{\text{th}}$,

(b) $\underset{p \in (p_{\text{th}}, P]}{\arg\max}\, C_K(p, \underline{\gamma}^*(p)) = \underset{p \in (p_{\text{th}}, P]}{\arg\max}\, C_K(p, (\Gamma, \ldots, \Gamma) = P$.

From (a) and (b), it can be concluded that the overall solution is $p^{\text{SE}} =$

$$\arg\max_{p\in\mathcal{A}_L} C_K(p,\underline{\gamma}^*(p)) = \begin{cases} p_{\text{th}}, & \text{if } C_K(P,\Gamma) < C_K(p_{\text{th}},0), \\ P, & \text{if } C_K(P,\Gamma) > C_K(p_{\text{th}},0), \\ \{p_{\text{th}},P\}, & \text{if } C_K(P,\Gamma) = C_K(p_{\text{th}},0). \end{cases}$$

To simplify the above possibilities, we focus on the case when the utility function $C_K(P,\Gamma)$, i.e., being detected and jammed, equals the utility function when player L is transmitting at threshold p_{th} (player J is silent), i.e., $C_K(P,\Gamma) = C_K(p_{\text{th}},0)$. Using this equality, by substituting appropriately into (25), we obtain a quadratic equation in P.

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

Note that Equation (33) has a unique positive root equal to $p_{\text{th}}(\sigma_J^2\Gamma+1)$. Furthermore, due to the fact that the leading coefficient of (33): $(2\sigma^2 p_{\text{th}}+1) \geq 0$ and $P > 0$, we can state that the inequalities $C_K(P,\Gamma) > C_K(p_{\text{th}},0)$ and $C_K(P,\Gamma) < C_K(p_{\text{th}},0)$ are equivalent to $P > p_{\text{th}}(\sigma_J^2\Gamma+1)$ and $P < p_{\text{th}}(\sigma_J^2\Gamma+1)$, respectively. □

A numerical evaluation of the SKG rate is presented in Figure 3. The parameters used are $N = 10$, $p_{\text{th}} = 2$, $\Gamma = 3$, and $\sigma^2 = \sigma_J^2 = 1$. Figure 3 compares the achievable SKG rates of the SE strategy, i.e., $p = p^{SE}$ with the two alternative strategies, i.e., $p = P$ or $p = p_{\text{th}}$. It can be seen that if player L deviates from the SE point the achievable SKG rate can decrease by up to 40%.

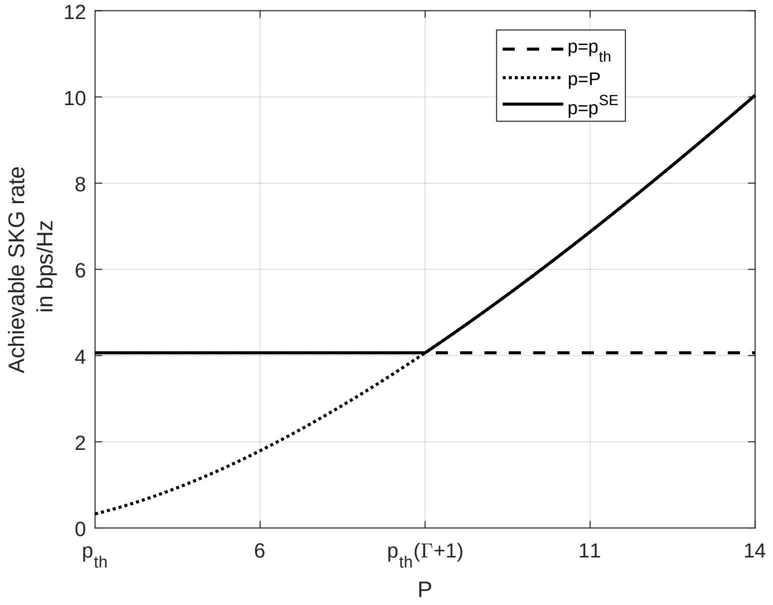

Figure 3. SE policy, compared to always transmitting with either full power or with p_{th}. Used parameters $p_{\text{th}} = 2, \Gamma = 3, N = 10, \sigma^2 = \sigma_J^2 = 1$.

4.3. Stackelberg Equilibrium with Strategic p_{th}

Finally, we investigate the case when Mallory could optimally adjust p_{th} and show how her choice impacts 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

$$\hat{\mathcal{A}}_J(p) \triangleq \begin{cases} \{((0,\ldots,0),p_{\text{th}}),\ p_{\text{th}} \geq 0\}, & \text{if } p_{\text{th}} \geq p, \\ \left\{(\underline{\gamma},p_{\text{th}}) \in \mathbb{R}_+^N \mid \sum_{i=1}^N \gamma_i \leq N\Gamma\right\}, & \text{if } p_{\text{th}} < p. \end{cases} \tag{33}$$

The BR of the jammer can then be defined as

$$(\widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}^*(p)) \triangleq \underset{(\underline{\gamma}, p_{\text{th}}) \in \hat{\mathcal{A}}_J(p)}{\arg\min} \; C_K(p, \underline{\gamma}, p_{\text{th}}). \tag{34}$$

Lemma 3. *Mallory's BR in this scenario is a set of strategies as follows:*

$$(\widehat{\underline{\gamma}}^*(p), \widehat{p_{th}}^*(p)) \in \{ \, ((\Gamma, \ldots, \Gamma)\epsilon), \; \epsilon \in [0, p)\}. \tag{35}$$

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

$$\min_{p_{\text{th}} \geq 0} \; \min_{\underline{\gamma} \in \hat{\mathcal{A}}_J(p)} C_K(p, \underline{\gamma}(p), p_{\text{th}}). \tag{36}$$

The solution of the inner minimization is known from (29). 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

$$\min_{p_{\text{th}} \geq 0} C_K(p, \widehat{\underline{\gamma}}^*(p), p_{\text{th}}) = \begin{cases} C_K(p, \Gamma, p_{\text{th}}), & \text{if } p_{\text{th}} < p, \\ C_K(p, 0, p_{\text{th}}), & \text{if } p_{\text{th}} \geq p, \end{cases} \tag{37}$$

and that $C_K(p, \Gamma, p_{\text{th}}) < C_K(p, 0, p_{\text{th}})$, player J can optimally choose any p_{th} such that $p_{\text{th}} = \epsilon, \;\; \forall \epsilon < p$. This allows the jammer to detect any ongoing transmission and to perform a jamming attack. □

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

$$(\widehat{p}^{SE}, \widehat{\underline{\gamma}}^{SE}, \widehat{p_{th}}^{SE}) \in \{ \, (P, (\Gamma, \ldots, \Gamma)\epsilon), \;\; \forall \epsilon < P\}. \tag{38}$$

Proof. Given Mallory's BR, we evaluate the SE of the game $\hat{\mathcal{G}}$. The definition for $\widehat{p}^{\text{SE}}$ is given as follows:

$$\widehat{p}^{\text{SE}} \triangleq \underset{p \in \mathcal{A}_L}{\arg} \; \max C_K(p, \widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}(p)^*). \tag{39}$$

Since Mallory will act as in (35), we have

$$C_K(p, \widehat{\underline{\gamma}}^*(p), \widehat{p_{\text{th}}}(p)^*) = C_K(p, \Gamma, \epsilon), \; \forall \epsilon < p, \tag{40}$$

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

Figure 4 illustrates the achievable SKG rate when p_{th} is part of player J's strategy. As in Figure 3, the parameters are chosen as $\Gamma = 3$, $N = 10$ and $\sigma_J^2 = 1$. It can be seen that due to a strategically chosen threshold from player J the legitimate users have no other choice but to transmit at full power $p = P = p^{\text{SE}}$. In fact, if the legitimate users deviate from the SE strategy and transmit with low power $p = p_{\text{th}}$, player J could successfully disrupt their SKG process and decrease their achievable SKG rate by up to 97%.

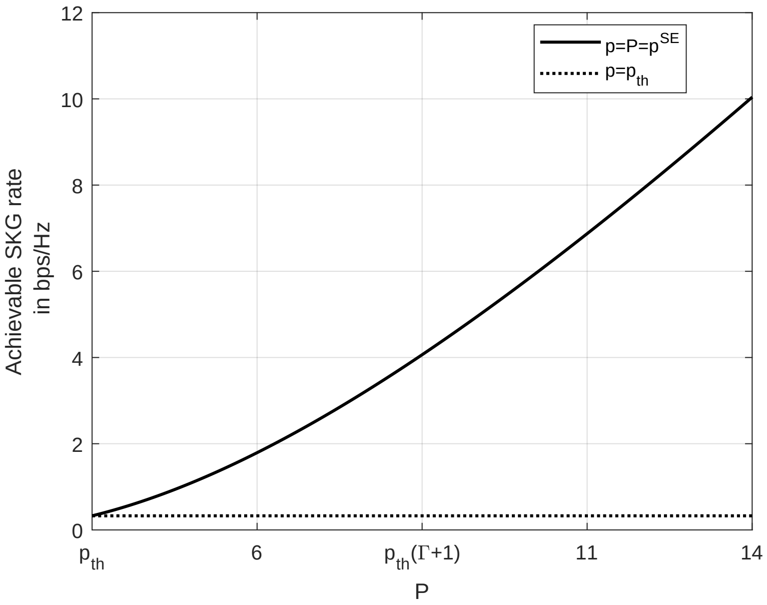

Figure 4. The effect to the SE policy when p_{th} is part of player J strategy. Comparison of the achievable SKG rate when player L chooses $p = p^{\text{SE}}$ with the case when transmitting with power p_{th}. Used parameters $\Gamma = 3, N = 10, \sigma^2 = \sigma_J^2 = 1$.

5. Conclusions

In this study, injection and reactive jamming attacks were analyzed in MIMO SKG systems. With respect to injection attacks, the study demonstrated that a trivial advantage in the form of one extra antenna allows a MiM to mount such an attack. As a countermeasure, we showed that a pilot randomization scheme can successfully reduce injection attacks to jamming attacks. With respect to jamming attacks, using a game-theoretic approach, we showed that an intelligent reactive jammer should optimally jam with full power when a transmission is sensed. Finally, by strategically choosing her jamming threshold, i.e., just below the power level used by the legitimate users, Mallory could perform a much more effective attack. In fact, our theoretical analysis suggests that in this case, Alice and Bob have no choice but to use their full power available for SKG. An important topic for further research in this area is an examination of these initial findings in practical scenarios.

Author Contributions: Conceptualization, M.M., A.C., E.V.B. and H.V.P.; Methodology, M.M., A.C., E.V.B. and H.V.P.; Software, M.M.; Validation, M.M., A.C., E.V.B. and H.V.P.; Supervision, A.C., E.V.B. and H.V.P.; Writing—review and editing, M.M., A.C., E.V.B. and H.V.P. All authors have read and agreed to the published version of the manuscript.

Funding: H.V. Poor was supported in part by the U.S. National Science Foundation under Grant CCF-1908308. E.V. Belmega and A. Chorti were supported by the ELIOT ANR-18-CE40-0030 and FAPESP 2018/12579-7 project. A. Chorti was also supported by CYU Initiative of Excellence (INEX) funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xu, W.; Jha, S.; Hu, W. LoRa-key: Secure Key Generation System for LoRa-based Network. *IEEE Internet Things J.* **2019**, *6*. [CrossRef]
2. Mitev, M.; Chorti, A.; Reed, M. Subcarrier Scheduling for Joint Data Transfer and Key Generation Schemes in Multicarrier Systems. In Proceedings of the IEEE Global Communications Conference (GLOBECOM , Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.

3. Mitev, M.; Chorti, A.; Reed, M. Optimal Resource Allocation in Joint Secret Key Generation and Data Transfer Schemes. In Proceedings of the 15th International Wireless Communications Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 360–365.
4. Maurer, U.; Wolf, S. Secret-key Agreement Over Unauthenticated Public Channels-Part I: Definitions and a Completeness Result. *IEEE Trans. Inf. Theory* **2003**, *49*, 822–831. [CrossRef]
5. Maurer, U.; Wolf, S. Secret-key Agreement Over Unauthenticated Public Channels-Part II: The Simulatability Condition. *IEEE Trans. Inf. Theory* **2003**, *49*, 832–838. [CrossRef]
6. Maurer, U.; Wolf, S. Secret-key Agreement Over Unauthenticated Public Channels-Part III: Privacy Amplification. *IEEE Trans. Inf. Theory* **2003**, *49*, 839–851. [CrossRef]
7. Premnath, S.N.; Jana, S.; Croft, J.; Gowda, P.L.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S. Secret Key Extraction from Wireless Signal Strength in Real Environments. *IEEE Trans. Mob. Comput.* **2013**, *12*, 917–930. [CrossRef]
8. Pierrot, A.J.; Chou, R.A.; Bloch, M.R. Experimental Aspects of Secret Key Generation in Indoor Wireless Environments. In Proceedings of the IEEE 14th Workshop Signal Processing Advances in Wireless Communications (SPAWC), Darmstadt, Germany, 16–19 June 2013; pp. 669–673.
9. Mitev, M.; Chorti, A.; Reed, M.; Musavian, L. Authenticated Secret Key Generation in Delay-Constrained Wireless Systems. *EURASIP J. Wirel. Commun. Netw.* **2020**, *122*. [CrossRef]
10. Saiki, C.; Chorti, A. A Novel Physical Layer Authenticated Encryption Protocol Exploiting Shared Randomness. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015.
11. Jana, S.; Premnath, S.N.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S. On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments. In Proceedings of the 15th Annual International Conference on Mobile Computing and Networking ACM, Beijing, China, 20–25 September 2009; pp. 321–332.
12. Rappaport, T. *Wireless Communications: Principles and Practice*, 2nd ed.; Prentice Hall PTR: Upper Saddle River, NJ, USA, 2001.
13. Wan, J.; Lopez, A.B.; Al Faruque, M.A. Exploiting Wireless Channel Randomness to Generate Keys for Automotive Cyber-Physical System Security. In Proceedings of the IEEE 7th nternational Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016; pp. 1–10.
14. Zoli, M.; Barreto, A.N.; Köpsell, S.; Sen, P.; Fettweis, G. Physical-Layer-Security Box: A Concept for Time-Frequency Channel-Reciprocity Key Generation. *EURASIP J. Wirel. Commun. Netw.* **2020**, *114*. [CrossRef]
15. Xiao, L.; Greenstein, L.J.; Mandayam, N.B.; Trappe, W. Using the Physical Layer for Wireless Authentication in Time-Variant Channels. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2571–2579. [CrossRef]
16. Chorti, A.; Hollanti, C.; Belfiore, J.-C.; Poor, H.V. *Physical Layer Security: A Paradigm Shift in Data Confidentiality*; Springer, Lect. Notes Electr. Eng.: Cham, Switzerland, 2015; pp. 1–15
17. Shakiba, M.; Chorti, A.; Poor, V. Physical Layer Security: Authentication, Integrity, and Confidentiality. In *Physical Layer Security*; Le, K., Ed.; Springer: Cham, Switzerland, 2021.
18. Mitev, M.; Chorti, A.; Belmega, E.V.; Reed, M. Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation. In Proceedings of the IEEE Global Communication Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
19. Maurer, U. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
20. Wang, Q.; Su, H.; Ren, K.; Kim, K. Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks. In Proceedings of the IEEE International Conference on Computer Communication (INFOCOM), Shanghai, China, 10–15 April, 2011.
21. Ye, C.; Reznik, A.; Shah, Y. Extracting Secrecy from Jointly Gaussian Random Variables. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Seattle, WA, USA, 9–14 July 2006.
22. Eberz, S.; Strohmeier, M.; Wilhelm, M.; Martinovic, I. *A Practical Man-in-the-Middle Attack on Signal-Based Key Generation Protocols*; Springer, Lect. Notes Comput. Sci.: Berlin/Heidelberg, Germany, 2012; pp. 235–252.
23. Rong, J.; Kai, Z. Physical Layer Key Agreement Under Signal Injection Attacks. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015; pp. 254–262.
24. Chorti, A. *A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems*; Springer, Lect. Notes in Electr. Eng.: Cham, Switzerland, 2018; pp. 1–14.
25. Fang, S.; Liu, Y.; Ning, P. Wireless Communications Under Broadband Reactive Jamming Attacks. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 394–408. [CrossRef]
26. Spuhler, M.; Giustiniano, D.; Lenders, V.; Wilhelm, M.; Schmitt, J.B. Detection of Reactive Jamming in DSSS-based Wireless Communications. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1593–1603. [CrossRef]
27. Jorswieck, E.; Wolf, A.; Engelmann, S. Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels. In Proceedings of the IEEE Global Communication Workshops, (GLOBECOM Workshops), Atlanta, GA, USA, 9–13 December 2013; pp. 1245–1250.