



**HAL**  
open science

# Protecting Physical Layer Secret Key Generation From Active Attacks

Miroslav Mitev, Arsenia Chorti, E Veronica Belmega, Vincent Poor

► **To cite this version:**

Miroslav Mitev, Arsenia Chorti, E Veronica Belmega, Vincent Poor. Protecting Physical Layer Secret Key Generation From Active Attacks. *Entropy*, 2021, 23 (8), pp.960. 10.3390/e23080960 . hal-03833914

**HAL Id: hal-03833914**


**<https://hal.science/hal-03833914>**

Submitted on 28 Oct 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Protecting Physical Layer Secret Key Generation From Active Attacks

Miroslav Mitev<sup>1,\*</sup> , Arsenia Chorti<sup>2</sup>, E. Veronica Belmega<sup>2</sup> and Vincent Poor<sup>3</sup>

<sup>1</sup> Barkhausen Institut gGmbH, Würzburger Str. 46, 01187 Dresden, Germany; Miroslav.Mitev@barkhauseninstitut.org

<sup>2</sup> ETIS, UMR 8051 CY Cergy Paris Université, ENSEA, CNRS F-95000, France; {arsenia.chorti, veronica.belmega}@ensea.fr

<sup>3</sup> School of Engineering and Applied Science, Princeton University, Princeton, NJ, 08544; 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 coming from the physical layer is 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) 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.

**Citation:** Mitev, M.; Chorti, A.; Belmega, E. V.; Poor, V. Protecting Physical Layer Secret Key Generation From Active Attacks. *Entropy* **2021**, *1*, 0. <https://doi.org/>

Received:

Accepted:

Published:

**Publisher’s Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2022 by the authors. Submitted to *Entropy* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 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 analysed, 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 one hand, the reciprocity property allows both Alice and Bob to measure

34 an identical channel impulse response during the coherence time of the channel,<sup>1</sup> while  
 35 on the other hand, the variability property of the wireless channel directly affects the  
 36 key generation rates [14–17].

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

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

## 56 2. System model

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

### 65 2.1. Secret key generation from fading coefficients

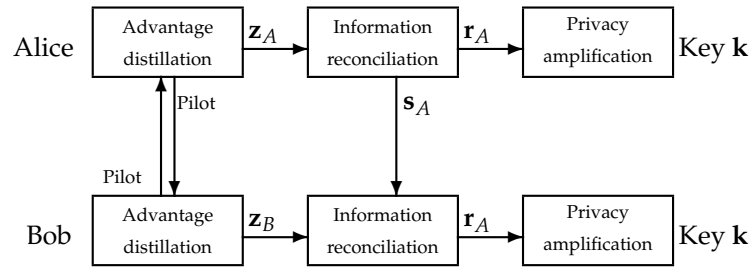
66 As illustrated in Fig. 1, the standard SKG procedure consist of three phases [19]: 1)  
 67 *advantage distillation*: the legitimate nodes exchange pilot signals, each using  $N$  transmit  
 68 and  $N$  receive antenna elements, in order to estimate their reciprocal channel state  
 69 information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

$$70 \quad \mathbf{z}_A = \mathbf{H}\mathbf{x} + \mathbf{n}_A \quad (1)$$

$$71 \quad \mathbf{z}_B = \mathbf{H}^T\mathbf{x} + \mathbf{n}_B, \quad (2)$$

72 where  $\mathbf{H}$  represents the channel matrix of size  $N_r \times N_t = N \times N$  such that its  $(i, j)$  entry  
 73 represents the channel linking the  $i$ -th receive antenna and the  $j$ -th transmit antenna,  $\mathbf{z}$   
 74 represents the received vector of length  $N_r$ ,  $\mathbf{x}$  denotes the transmitted vector consisting of  
 75  $N_t = N_r = N$  elements,  $\mathbf{n}_A$  and  $\mathbf{n}_B$  are the received noise vectors at Alice and Bob, each of  
 76 length  $N_r$ , respectively. Note that, due to the reciprocity of the wireless channel Alice and  
 77 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

<sup>1</sup> The coherence time indicates the interval during which the multipath properties of wireless channels (channel gains, signal phase, delay) remain stable [11–13].



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

78 outputs, are reconciled through a public exchange of helper data  $\mathbf{s}_A$  (see Fig. 1), e.g.,  
 79 by using Slepian Wolf reconciliation techniques [10,21]; 3) *privacy amplification*: the  
 80 legitimate nodes apply universal hash functions to the reconciled information  $\mathbf{r}_A$  and  
 81 obtain key  $\mathbf{k}$ . This step ensures that the generated key  $\mathbf{k}$  is uniformly distributed and  
 82 completely unpredictable by an adversary.

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

$$\mathbf{z}_{AM} = \mathbf{H}_{AM}\mathbf{x} + \mathbf{n}_{AM}, \quad (3)$$

$$\mathbf{z}_{BM} = \mathbf{H}_{BM}\mathbf{x} + \mathbf{n}_{BM}. \quad (4)$$

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 denoted by  $\mathbf{n}_{AM}$  and  $\mathbf{n}_{BM}$ . Following from that, the SKG capacity between Alice and Bob is expressed as the conditional mutual information between the observations of Alice, Bob and Mallory:

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

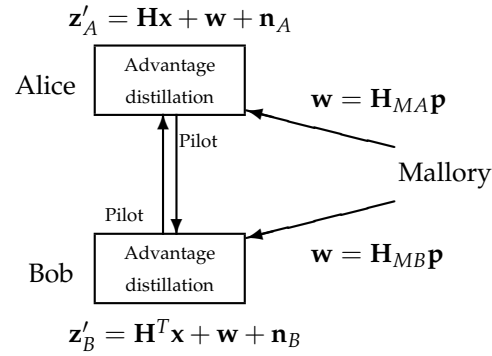
### 83 2.2. Injection attacks during SKG

84 One of the most critical threats to the SKG model, given in Fig. 1, is MiM in the  
 85 form of injection attack [11,22,23]. The main components of the injection attack are  
 86 captured in Fig. 2. While, the legitimate nodes Alice and Bob exchange pilot signals  
 87 during the advantage distillation phase, Mallory injects signals  $\mathbf{p}$ . Based on the results in  
 88 [22], we assume that Mallory has perfect knowledge of the channel vectors in the MIMO  
 89 links Mallory-Alice,  $\mathbf{H}_{MA} = \mathbf{H}_{AM}^T$  and Mallory-Bob,  $\mathbf{H}_{MB} = \mathbf{H}_{BM}^T$ . This is a reasonable  
 90 assumption since Mallory can estimate the channel vectors while Alice and Bob exchange  
 91 pilot signals, as long as the channel's coherence time is respected (a plausible scenario  
 92 in slow fading, low mobility environments). Finally, Mallory chooses the vector  $\mathbf{p}$  such  
 93 that the same signal is "injected" at both Alice and Bob, i.e.,  $\mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}$ .

### 94 3. Analysis of injection attacks in MIMO SKG

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

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



**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  $\mathbf{w} = \mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}$ .

101 **Proof.** The pre-coding vector of Mallory  $\mathbf{p}$  of size  $(N + 1) \times 1$  is represented as:

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

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

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

and

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

Next we can represent the equation

$$\mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}, \quad (9)$$

as

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

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

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

Given that, Eq. (10) can be re-written as  $\mathbf{H}_M\mathbf{p} = \mathbf{0}$ , where  $\mathbf{H}_M$  is given in Eq. (11). The equality  $\mathbf{H}_M\mathbf{p} = \mathbf{0}$  is equivalent to solving the following linear system of equations:

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

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 that, we let  $p_{N+1}$  to be a constant, and re-write the system in (12) as:

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

The system of equations in (13) can be represented as  $\mathbf{Ax} = \mathbf{b}$ , where the  $N \times N$  matrix  $\mathbf{A}$  is the  $N \times N$  matrix containing the first  $N$  lines and  $N$  columns of  $\mathbf{H}_M$ ,  $\mathbf{x} = (p_1, p_2, \dots, p_N)^T$ , and  $\mathbf{b}$  contains the right hand side of the system, i.e.,  $\mathbf{b} = (-H_{M_{1,N+1}}p_{N+1}, \dots, -H_{M_{N,N+1}}p_{N+1})^T$ . Finally, since  $\det(\mathbf{A}) \neq 0$  almost surely<sup>2</sup>, the system's solution is unique and given by:

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

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

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

$$\mathbf{z}_A = \mathbf{H}\mathbf{x} + \mathbf{w} + \mathbf{n}_A \quad (15)$$

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

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 the pre-coding vector  $\mathbf{p}$ . By injecting  $\mathbf{w}$  Mallory controls the secret key rate which is now upper bounded by [18,24]:

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

### 108 3.1. Pilot randomization as a countermeasure to injection attacks

In 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 where with pilots are drawn from a (scaled) QPSK modulation. In detail, 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  $\mathcal{U}(\{\pm r \pm jr\}, \dots, \{\pm r \pm jr\})$ , where  $j = \sqrt{-1}$ ,  $r = \sqrt{P/2}$ , so that,  $\mathbb{E}[\mathbf{x}] = \mathbb{E}[\mathbf{y}] = (0, \dots, 0)^T$ ,  $(\mathbb{E}[|x_1|^2], \dots, \mathbb{E}[|x_N|^2])^T = (\mathbb{E}[|y_1|^2], \dots, \mathbb{E}[|y_N|^2])^T = (P, \dots, P)^T$  and  $(\mathbb{E}[x_1y_1], \dots, \mathbb{E}[x_Ny_N])^T = (0, \dots, 0)^T$ , 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

$$\mathbf{z}_A = \mathbf{H}\mathbf{y} + \mathbf{w} + \mathbf{n}_A, \quad (18)$$

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

<sup>2</sup> Under the wireless channels assumptions in Sec. 2,  $\det(\mathbf{A})$  is a continuous random variable, hence  $\det(\mathbf{A}) \neq 0$  with probability 1.

109 Finally, to generate a shared randomness, Alice and Bob post-multiply  $\mathbf{z}_A$  and  $\mathbf{z}_B$  by  
 110 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  
 111 by Mallory). Given that, the modified observations are expressed as:

$$\tilde{z}_A = \mathbf{x}^T \mathbf{H} \mathbf{y} + \mathbf{x}^T \mathbf{w} + \mathbf{x}^T \mathbf{n}_A, \quad (20)$$

$$\tilde{z}_B = \mathbf{y}^T \mathbf{H}^T \mathbf{x} + \mathbf{y}^T \mathbf{w} + \mathbf{y}^T \mathbf{n}_B, \quad (21)$$

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 that:

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

#### 112 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). 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 the legitimate transmission [25,26]. Next, we assume that Alice and Bob perform SKG in a TDD-MIMO system with 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.:

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

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  $p_{\text{th}}$ . Due to that, 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  $\underline{\gamma} = (\gamma_1, \dots, \gamma_N)$ . By denoting the available jamming power by  $N\Gamma$  the following short-term power constraint is considered:

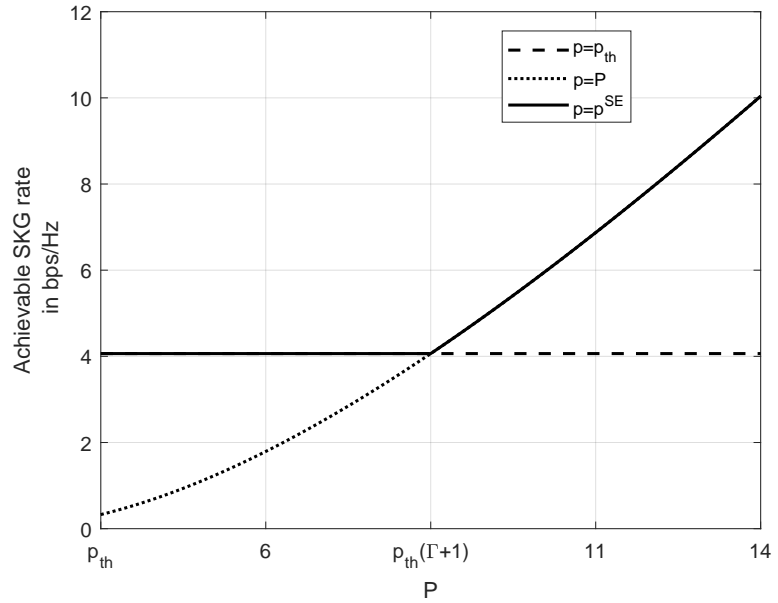
$$\underline{\gamma} \in \mathbb{R}_+^N, \quad \sum_{i=1}^N \gamma_i \leq N\Gamma. \quad (24)$$

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  $\sigma^2$  and  $\sigma_J^2$ , respectively, then the SKG capacity can be expressed as [27]:

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

##### 113 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 non-cooperative zero-sum game which studies the strategic interaction between the legitimate users and the jammer:  $\mathcal{G} = (\{L, J\}, \{\mathcal{A}_L, \mathcal{A}_J(p)\}, C_K(p, \underline{\gamma}))$ . The game  $\mathcal{G}$  has three components: i) there are two players:  $L$  denoting the legitimate users (Alice and Bob act



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

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

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

114 At last,  $C_K(p, \underline{\gamma})$ , 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  $(p^{SE}, \underline{\gamma}^{SE})$  where player  $L$  chooses his optimal strategy first, by anticipating the strategic reaction of player  $J$  (i.e., its best response). This is expressed as:

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

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 :

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

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

#### 118 4.2. Stackelberg equilibrium with fixed detection threshold

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



**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:

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

125 **Proof.** Note that  $C_K(p, \gamma_i)$  is a monotonically decreasing convex function w.r.t  $\gamma_i$ ,  $i =$   
 126  $1, \dots, N$  for any  $p > 0$ . Based on the principles of convexity in order to minimize  $C_K$ ,  
 127 Mallory has to transmit with full power from all antennas. The detailed proof can be  
 128 found in [18].  $\square$

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

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

129 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  $P \neq p_{th}(\sigma_f^2\Gamma + 1)$  and is given by

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

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

**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:

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

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

$$\begin{aligned} 133 \quad & \text{a) } \arg \max_{p \in [0, p_{th}]} C_K(p, \underline{\gamma}^*(p)) = \arg \max_{p \in [0, p_{th}]} C_K(p, (0, \dots, 0)) = p_{th}, \\ 134 \quad & \text{b) } \arg \max_{p \in (p_{th}, P]} C_K(p, \underline{\gamma}^*(p)) = \arg \max_{p \in (p_{th}, P]} C_K(p, (\Gamma, \dots, \Gamma)) = P. \end{aligned}$$

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

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

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.,  $C_K(P, \Gamma) = C_K(p_{th}, 0)$ . Using this equality, by substituting appropriately into (25), we obtain a quadratic equation in  $P$ :

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

135 Note that Eq. (33) has a unique positive root equal to  $p_{th}(\sigma_f^2\Gamma + 1)$ . Furthermore, due  
 136 to the fact that the leading coefficient of (33):  $(2\sigma^2 p_{th} + 1) \geq 0$  and  $P > 0$ , we can say  
 137 that the inequalities  $C_K(P, \Gamma) > C_K(p_{th}, 0)$  and  $C_K(P, \Gamma) < C_K(p_{th}, 0)$  are equivalent to  
 138  $P > p_{th}(\sigma_f^2\Gamma + 1)$  and  $P < p_{th}(\sigma_f^2\Gamma + 1)$ , respectively.  $\square$

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

#### 144 4.3. Stackelberg equilibrium with strategic $p_{\text{th}}$

Finally, we investigate the case when Mallory could optimally adjust  $p_{\text{th}}$  and show how her choice impacts Alice's and Bob's strategies. Allowing  $p_{\text{th}}$  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:

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

The BR of jammer can then be defined as:

$$(\hat{\underline{\gamma}}^*(p), \hat{p}_{\text{th}}^*(p)) \triangleq \arg \min_{(\underline{\gamma}, p_{\text{th}}) \in \hat{\mathcal{A}}_J(p)} C_K(p, \underline{\gamma}, p_{\text{th}}). \quad (34)$$

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

$$(\hat{\underline{\gamma}}^*(p), \hat{p}_{\text{th}}^*(p)) \in \{((\Gamma, \dots, \Gamma)\epsilon), \epsilon \in [0, p)\}. \quad (35)$$

**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:

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

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  $C_K(p, \hat{\underline{\gamma}}^*(p), p_{\text{th}})$ . Given that:

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

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

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

$$(\hat{p}^{\text{SE}}, \hat{\underline{\gamma}}^{\text{SE}}, \hat{p}_{\text{th}}^{\text{SE}}) \in \{(P, (\Gamma, \dots, \Gamma)\epsilon), \forall \epsilon < P\}. \quad (38)$$

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

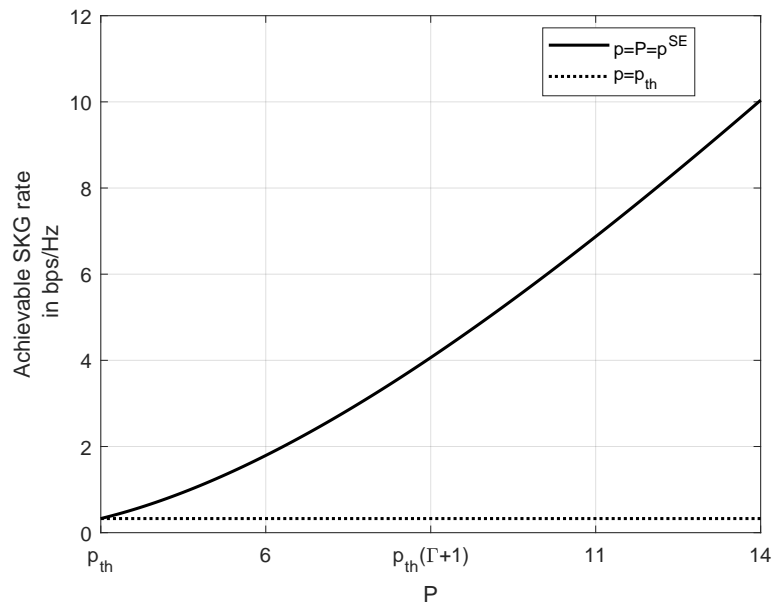
$$\hat{p}^{\text{SE}} \triangleq \arg \max_{p \in \mathcal{A}_L} C_K(p, \hat{\underline{\gamma}}^*(p), \hat{p}_{\text{th}}(p)^*). \quad (39)$$

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

$$C_K(p, \hat{\underline{\gamma}}^*(p), \hat{p}_{\text{th}}(p)^*) = C_K(p, \Gamma, \epsilon), \forall \epsilon < p, \quad (40)$$

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

149 Figure 4 illustrates the achievable SKG rate when  $p_{\text{th}}$  is part player  $J$ 's strategy. As  
 150 in Figure 3, the parameters are chosen as  $\Gamma = 3$ ,  $N = 10$  and  $\sigma_j^2 = 1$ . It can be seen that



**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  $p = p^{SE}$  with the case when transmitting with power  $p_{th}$ . Used parameters  $\Gamma = 3, N = 10, \sigma^2 = \sigma_j^2 = 1$ .

151 due to a strategically chosen threshold from player  $J$  the legitimate users have no other  
 152 choice but to transmit at full power  $p = P = p^{SE}$ . In fact, if the legitimate users deviate  
 153 from the SE strategy and transmit with low power  $p = p_{th}$  player  $J$  could successfully  
 154 disrupt their SKG process and decrease their achievable SKG rate by up to 97%.

## 155 5. Conclusions

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

- 168 **Author Contributions:** All authors contributed and edited the manuscript. All authors read and  
169 approved the final manuscript.
- 170 **Funding:** This research was funded by DIM RFSI, project SAFEST and the ELIOT ANR-18-CE40-  
171 0030 and FAPESP 2018/12579-7 project. A. Chorti was also supported by CYU Initiative of  
172 Excellence (INEX) funding.
- 173 **Institutional Review Board Statement:** Not applicable.
- 174 **Informed Consent Statement:** Not applicable.
- 175 **Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. W. Xu, S. Jha, W. Hu. LoRa-key: secure key generation system for LoRa-based network. *IEEE Internet of Things Journal* **2019**.
2. M. Mitev, A. Chorti, M. Reed. Subcarrier scheduling for joint data transfer and key generation schemes in multicarrier systems. Proceedings of the IEEE Global Communications Conference, 2019, pp. 1–6.
3. M. Mitev, A. Chorti, M. Reed. Optimal resource allocation in joint secret key generation and data transfer schemes. Proceedings of the 15th International Wireless Communications and Mobile Computing Conference, 2019, pp. 360–365.
4. U. Maurer, S. Wolf. Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result. *IEEE Transactions on Information Theory* **2003**, *49*, 822–831.
5. U. Maurer, S. Wolf. Secret-key agreement over unauthenticated public channels-part II: the simulatability condition. *IEEE Transactions on Information Theory* **2003**, *49*, 832–838.
6. U. Maurer, S. Wolf. Secret-key agreement over unauthenticated public channels-part III: privacy amplification. *IEEE Transactions on Information Theory* **2003**, *49*, 839–851.
7. S. Premnath, J. Jana, J. Croft, P. Gowda, M. Clark, S. Kasera, N. Patwari, S. Krishnamurthy. Secret key extraction from wireless signal strength in real environments. *IEEE Transactions on Mobile Computing* **2013**, *12*, 917–930.
8. A. Pierrot, R. Chou, M. Bloch. Experimental aspects of secret key generation in indoor wireless environments. Proceedings of the IEEE 14th Workshop on Signal Processing Advances in Wireless Communications; , 2013; pp. 669–673.
9. M. Mitev, A. Chorti, M. Reed, L. Musavian. Authenticated secret key generation in delay-constrained wireless systems. *EURASIP Journal on Wireless Communications and Networking* **2020**.
10. C. Saiki, A. Chorti. A novel physical layer authenticated encryption protocol exploiting shared randomness. Proceedings of the IEEE Conference on Communications and Network Security; , 2015.
11. S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, S. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. Proceedings of the 15th annual international conference on Mobile computing and networking. ACM, 2009, pp. 321–332.
12. T. Rappaport. *Wireless communications: principles and practice*, 2nd ed.; Prentice Hall PTR: USA, 2001.
13. J. Wan, A. Lopez, M. Faruque. Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security. Proceedings of the IEEE 7th International Conference on Cyber-Physical Systems, 2016, pp. 1–10.
14. M. Zoli, A. Barreto, S. Köpsell, P. Sen, G. Fettweis. Physical-layer-security box: a concept for time-frequency channel-reciprocity key generation. *EURASIP Journal on Wireless Communications and Networking* **2020**.
15. L. Xiao, L. Greenstein, N. Mandayam, W. Trappe. Using the physical layer for wireless authentication in time-variant channels. *IEEE Transactions on Wireless Communications* **2008**, *7*, 2571–2579.
16. A. Chorti, C. Hollanti, J. Belfiore, V. Poor. *Physical layer security: a paradigm shift in data confidentiality*; 2015.
17. M. Shakiba, A. Chorti, V. Poor. Physical layer security: authentication, integrity, and confidentiality. In *Physical Layer Security*; LE, K., Ed.; Springer, 2021.
18. M. Mitev, A. Chorti and V. Belmega, M. Reed. Man-in-the-middle and denial of service attacks in wireless secret key generation. Proceedings of the IEEE Global Communications Conference, 2019, pp. 1–6.
19. U. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory* **1993**, *39*, 733–742.
20. Q. Wang, H. Su, K. Ren, K. Kim. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. Proceedings of the IEEE International Conference on Computer Communications, 2011.
21. C. Ye, A. Reznik, Y. Shah. Extracting secrecy from jointly Gaussian random variables. Proceedings of the IEEE International Symposium on Information Theory, 2006.
22. S. Eberz, M. Strohmeier, M. Wilhelm, I. Martinovic. A practical man-in-the-middle attack on signal-based key generation protocols. Springer, Lecture Notes in Computer Science, 2012, pp. 235–252.
23. J. Rong, Z. Kai. Physical layer key agreement under signal injection attacks. Proceedings of the IEEE Conference on Communications and Network Security, 2015, pp. 254–262.
24. A. Chorti. A study of injection and jamming attacks in wireless secret sharing systems. *Springer, Lecture Notes in Electrical Engineering* **2018**, pp. 1–14.

- 
25. S. Fang, Y. Liu, P. Ning . Wireless communications under broadband reactive jamming attacks. *IEEE Transactions on Dependable and Secure Computing* **2016**, *13*, 394 – 408.
  26. M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, J. Schmitt. Detection of reactive jamming in DSSS-based wireless communications. *IEEE Transactions on Wireless Communications* **2014**, *13*, 1593 – 1603.
  27. E. Jorswieck, A. Wolf, S. Engelmann. Secret key generation from reciprocal spatially correlated MIMO channels. Proceedings of the IEEE Global Communications Workshop, 2013, pp. 1245–1250.