Protecting Secret Key Generation Systems Against Jamming: Energy Harvesting and Channel Hopping Approaches

E. Veronica Belmega, *Member, IEEE,* and Arsenia Chorti, *Member, IEEE*

***Abstract*—Jamming attacks represent a critical vulnerability for wireless secret key generation (SKG) systems. In the present study, two counter-jamming approaches are investigated for SKG systems: first, the employment of energy harvesting (EH) at the legitimate nodes to turn part of the jamming power into useful communication power, and, second, the use of channel hopping or power spreading in block fading channels to reduce the impact of jamming. In both cases, the adversarial interaction between the pair of legitimate nodes and the jammer is formulated as a two-player zero-sum game and the Nash and Stackelberg equilibria (NE and SE) are characterized analytically and in closed form. In particular, in the case of EH receivers, the existence of a critical transmission power for the legitimate nodes allows the full characterization of the game's equilibria and also enables the complete neutralization of the jammer. In the case of channel hopping vs. power spreading techniques, it is shown that the jammer's optimal strategy is always power spreading while the legitimate nodes should only use power spreading in the high signal-to-interference ratio (SIR) regime. In the low SIR regime, when avoiding the jammer's interference becomes critical, channel hopping is optimal for the legitimate nodes. Numerical results demonstrate the efficiency of both counter-jamming measures.**

***Index Terms*—Secret key generation, jamming, energy harvesting, channel hopping, zero-sum game.**

I. Introduction

Secret key generation (SKG) from shared randomness at two remote locations has been extensively studied [3]–[12] and has recently been extended to unauthenticated channels [13], [14]. SKG techniques have also been be incorporated in protocols that are resilient to spoofing, tampering and man-in-the-middle active attacks [15], [16]. Still, such key generation techniques are not entirely robust against active adversaries, particularly during the advantage distillation phase. Denial of service attacks in the form of jamming are a known vulnerability of SKG systems; in [17], it was demonstrated that when increasing the jamming power, the reconciliation rate normalized to the rate of the SKG increases sharply and the SKG process can in essence be brought to a halt. As SKG techniques are currently being considered for applications such as the Internet of things (IoT) [18], the study of appropriate counter-jamming approaches is timely.

Typically, jamming in wireless communication systems has been investigated using game theoretic tools [19]–[27]. Contrary to our work, these earlier studies focus on performance metrics that are either based on the legitimate nodes' signal-to-interference-plus-noise ratio (SINR) [19]–[25] and do not incorporate physical-layer security constraints at all, or are based on the secrecy capacity [26], [27]. The secrecy capacity is inherently different than the SKG capacity considered in this work; the former measures the maximum rate at which both confidential and reliable communication is possible, while, the latter represents the maximum rate at which a common secret key that can be extracted from the observation of correlated sequences at two remote locations [28].

In the past, two main counter-jamming approaches have been commonly considered: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) [29], [30]. In either approach, the impact of power constrained jammers can be limited because their optimal strategy has been proved to be spreading of their available power over the entire bandwidth (and thus jam with potentially low power). However, DSSS and FHSS systems require a pre-shared secret to establish the spreading sequence or the hopping pattern at Alice and Bob; as such, they are not directly applicable to SKG systems that on the contrary *seek to establish* a secret key. Attempting to resolve this contradiction and reconcile DSSS and FHSS with SKG, uncoordinated frequency hopping and spreading techniques have recently been investigated in [31], [32]. The main idea behind the proposed approaches was the randomization of the selection of the hopping/spreading sequences, at the cost of reduction of the achievable rates for secret key establishment.

However, in uncoordinated hopping/spreading techniques there are minimum requirements regarding the length of the pseudorandom sequences employed. As a result, accounting for the strict bandwidth specifications of fourth and fifth generation networks, the use of long pseudorandom sequences can be a limiting factor. Thus, investigating alternative counter-jamming approaches based on the use of channel hopping or power spreading over multiple orthogonal subcarriers, e.g., orthogonal frequency division multiplexing (OFDM) systems) [19], [21], is timely and offer an interesting alternative to [31], [32] as in OFDM systems there is no need for coordination of the remote nodes. Furthermore, although in [31], [32] the numerical investigations focused on the throughput, a Media Access Control (MAC) layer quantity, when analyzing physical layer security SKG systems the standard approach is

Preliminary results have been accepted for publication in Proc. IEEE Int. Conf. Commun. (ICC) 2017 [1], [2]. This research has been supported in part by ENSEA, Cergy-Pontoise, France. E.V. Belmega is with ENSEA/ETIS - Université de Cergy-Pontoise - CNRS, Cergy-Pontoise, France and Inria (email: belmega@ensea.fr). A. Chorti is with the School of Computer Science and Electronic Engineering (CSEE), University of Essex, Colchester, United Kingdom (email: achorti@essex.ac.uk).

to utilize the SKG capacity (a physical layer quantity).

On a different note, next generation terminals are likely to be enhanced with many new features that could prove pivotal in protecting against jamming. For example, greater energy autonomy exploiting energy harvesting (EH) approaches [33], [34] is being researched for systems such as wireless sensor networks for IoT applications. Thus, it is interesting to investigate whether EH could be utilized as a counter-jamming technique by exploiting the harvested jamming power to enhance the quality of the legitimate communication.

Motivated by the above, in the present work we propose two novel approaches for alleviating the impact of jamming in SKG systems. In both approaches, we model the interaction between the legitimate nodes and the adversarial jammer as a two-player zero-sum game in which the SKG capacity plays the role of the utility function. We investigate two non-cooperative solutions: the Nash equilibria (NE), when both players make their decision simultaneously and the Stackelberg equilibria (SE), when the legitimate nodes hold an advantage and choose their strategy first while anticipating the jammer's response.

In the first part of this contribution, we study systems in which the legitimate nodes are equipped with EH capabilities and examine whether this added functionality is useful in preempting jamming attacks. We focus on time switching EH protocols [34]: for a fraction of time the legitimate nodes operate in EH mode and switch to the SKG procedure for the rest. To the best of our knowledge, this is among the first works to investigate EH as a counter-jamming approach with the exception of [25].[1]

Our analysis reveals the existence of a critical power threshold p_{th} for the legitimate nodes and of an associated threshold harvesting duration τ_{th}. When the legitimate nodes employ EH for longer than τ_{th}, the attacker's optimal strategy is not to jam at all, i.e., the jammer is effectively neutralized. However, neutralizing the jammer is not a stable solution to unilateral deviations (if the strategic decisions are taken simultaneously) and is therefore not a Nash equilibrium (NE) of the game. At the NE, it is found that both the legitimate nodes and the jammer transmit with full power and that the EH duration does not correspond always to the above threshold. At low signal to interference ratio (SIR) (e.g., relatively low transmit power or high jamming power), the EH optimal duration equals τ_{th}. Although the attacker jams with full power, the power collected from EH cancels out the impact of the attack and the SKG capacity is equivalent to the case of using EH for the same duration in absence of a jammer. At medium to high SIR, the EH optimal duration is lower than τ_{th} and the legitimate nodes may even not harvest energy at all.

On the other hand, when moving to a hierarchical game formulation, the SE analysis reveals that the legitimate nodes should play the NE strategy. Whenever the legitimate nodes' harvest energy for a duration τ_{th} (at the NE), the jammer neutralization strategy is also a SE solution. This means that, in a hierarchical game, the jammer can potentially be deterred from launching the attack.

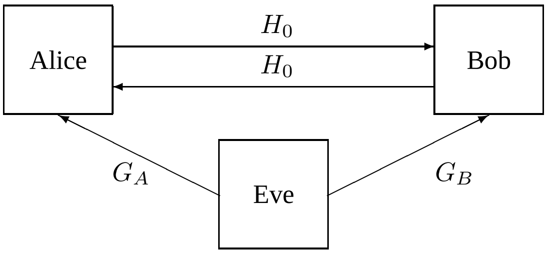

Fig. 1. SKG system model with two legitimate nodes and a single adversary.

In the second part of this investigation, extending the studies in [19], [21] to SKG systems, counter-jamming policies are investigated for N block (subcarriers) fading additive white Gaussian noise (BF AWGN) channels. At the NE, the jammer always spreads its power over all subcarriers, while for the legitimate nodes the optimality of channel hopping or power spreading depends on the channel parameters. In the high SIR regime, the legitimate nodes should use power spreading to exploit the entire available spectrum given the relatively low jamming interference. On the other hand, at low SIR, the legitimate nodes should use channel hopping and transmit over a single subcarrier to avoid most of the jammer's interference. Furthermore, in characterizing the game's SE we find that the optimal SE strategies reduce to the NE ones, demonstrating that there is no extra payoff to be earned from the advantage of playing first.

Preliminary results of this work have been presented in [1] and [2]. The major contributions and improvements of this journal paper as compared with [1] and [2] consist in: providing complete proofs of all the results regarding the NE analysis and the jammer neutralization state; relaxing the action set of the jammer, in the energy harvesting case, from the discrete choice between remaining silent and transmitting at full power into the continuous interval of all possible powers, which has brought to light the existence of additional NEs; providing the additional analysis of the Stackelberg equilibrium; providing a comparative discussion between the two counter-jamming methods in Sec. V-C.

The paper is organized as follows. In Sec. II, the SKG baseline system model is introduced. In Sec. III, the adversarial interaction between the EH legitimate nodes and the jammer is formulated and analyzed using a zero-sum non-cooperative game framework, while in Sec. IV this setting is used to study channel hopping vs. power spreading in BF AWGN systems. Numerical illustrations and a detailed discussion of these counter-jamming strategies are provided in Sec. V, while the conclusions are given in Sec. VI.

II. SKG System Model in the Presence of a Jammer

The baseline SKG system model with two legitimate nodes, denoted by Alice and Bob and a single adversary, denoted

[1] The recent work [25] proposes to harvest energy from the jamming interference in a multi-user interference channel in which the jammer is not a strategic decision maker. In terms of formulation, a global optimization problem is investigated (as opposed to an adversarial game). Furthermore, the global performance metric in [25] does not incorporate security constraints and the harvested energy is not directly exploited in the communication phase, appearing only as an additional term in the utility function.

by Eve, is depicted in Fig. 1. Typically, the SKG process consists of three phases [4], [6]. In the first phase, referred ro as *shared randomness distillation*, Alice and Bob observe dependent random variables denoted by Y_A, Y_B while an eavesdropper, referred to as Eve, observes Y_E. In wireless channels, a readily available source of shared randomness is the multipath fading due to the reciprocity of the wireless medium during the channel's coherence time [10]–[12]. Here, we focus exclusively on shared randomness extraction from Rayleigh fading coefficients.

In the next two phases, known as *information reconciliation* and *privacy amplification*, side information V is exchanged between Alice and Bob, generated by corresponding encoders f_A, f_B. At the end of the SKG process, a common key $K \in \mathcal{K}$ is extracted at Alice and Bob such that, for any $\epsilon > 0$, the following statements hold [8]:

$$\begin{aligned} Pr\left(K = f_A\left(Y_A, V\right) = f_B\left(Y_B, V\right)\right) &\geq 1 - \epsilon, &(1)\\ I(K; V) &\leq \epsilon, &(2)\\ H(K) &\geq \log|\mathcal{K}| - \epsilon, &(3) \end{aligned}$$

where $H(K)$ denotes the entropy of the key K and $I(K;V)$ denotes the mutual information between K and V.

The first inequality demonstrates that the SKG process can be made error free; (2) ensures that the exchange of side information through public discussion does not leak any information to eavesdroppers; while (3) establishes that the generated keys attain maximum entropy (i.e., are uniform). Under the three conditions, an upper bound on the rate for the generation of secret keys is given by $\min\{I(Y_A;Y_B), I(Y_A;Y_B|Y_E)\}$ [3], [4]. Assuming rich multipath environments, the decorrelation properties of the wireless channel over short distances can be exploited to ensure that Eve's observation Y_E is uncorrelated with Y_A and Y_B [7]–[11]; in this case, the SKG capacity is given by [3, Sec. II]

$$C = I(Y_A; Y_B). \tag{4}$$

We assume that this holds true in the rest of this study and consider the SKG capacity above to be the focal performance metric.

SKG in Rayleigh fading channels has been extensively analyzed, e.g., [7], [8]. In these works, it was assumed that Alice and Bob exchange unit probe signals to excite the fading channel and obtain respective observations Y_A and Y_B with

$$Y_A = H_0 + Z_A, \; Y_B = H_0 + Z_B,$$

where H_0 denotes the fading coefficient in the link between the legitimate nodes, modeled as a zero mean Gaussian random variable $H_0 \sim \mathcal{N}(0, \sigma_H^2)$, and, Z_A and Z_B model the effect of AWGN and denote independent and identically distributed (i.i.d.) Gaussian random variables $Z_A \sim \mathcal{N}(0, N_A)$, $Z_B \sim \mathcal{N}(0, N_B)$. Using this notation, the SKG capacity has been expressed as [8]:

$$C = I(Y_A; Y_B) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2}{N_A + N_B + \frac{N_A N_B}{\sigma_H^2}}\right). \tag{5}$$

In this work, we assume that Eve is no longer a passive eavesdropper but a malicious jammer. To include jamming attacks in the above model, we consider the following extension:

$$\begin{aligned} Y_A &= \sqrt{p}H_0 + \sqrt{\gamma}G_A + Z_A, &(6)\\ Y_B &= \sqrt{p}H_0 + \sqrt{\gamma}G_B + Z_B, &(7) \end{aligned}$$

assuming that Alice and Bob exchange constant probe signals [8] with power $p \leq P$ and that Eve transmits constant jamming signals [17] with power $\gamma \leq \Gamma$. The fading coefficient in the link between Eve and Alice is denoted by $G_A \sim \mathcal{N}\left(0, \sigma_A^2\right)$ and in the link between Eve and Bob by $G_B \sim \mathcal{N}\left(0, \sigma_B^2\right)$. For simplicity and without loss of generality, the noise variables Z_A and Z_B are assumed to have unit variance, i.e., are modeled as i.i.d. Gaussian random variables $Z_A, \; Z_B \sim \mathcal{N}(0,1)$.

Under these assumptions, a simple calculation reveals that the SKG capacity can be expressed as a function of p and γ:

$$C(p,\gamma) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2 p}{2 + (\sigma_A^2 + \sigma_B^2)\gamma + \frac{(1+\sigma_A^2\gamma)(1+\sigma_B^2\gamma)}{\sigma_H^2 p}}\right). \tag{8}$$

By inspecting the first-order derivatives of (8), we conclude that $C(p,\gamma)$ is a strictly increasing function of p for any fixed γ, and a strictly decreasing function of γ for any fixed p. This implies that the legitimate nodes will transmit at full power P to maximize the SKG capacity, whereas the jammer will also transmit with full power Γ to minimize the SKG capacity. Also, it is a strictly convex function with respect to (w.r.t.) γ for any fixed $p > 0$ as its second derivative w.r.t. γ is strictly positive.

III. Energy Harvesting Against Jamming

In order to study EH as a counter-jamming measure, we focus on a time-switching EH scheme [34], i.e., we assume that each transmission symbol of duration T is divided in two parts. In the first period of duration τT ($0 < \tau \leq 1$ being the fraction of T dedicated to EH), both Alice and Bob operate in EH mode with efficiency $0 < \zeta \leq 1$; in the second period of duration $(1-\tau)T$, the legitimate nodes operate in SKG mode using the overall available power (including harvested power). For simplicity, we assume that the energy harvested can be stored in a battery without any overflowing issues (unlimited storage) [35].

Furthermore, for simplicity of the mathematical derivation and to ensure symmetry in the energy harvested at Alice and Bob we assume that $\sigma_A^2 = \sigma_B^2 = \sigma^2$ (the Eve-Alice and Eve-Bob links have equal variance). Given the above considerations and assuming that the energy harvested by Alice and Bob is linear in the received RF power [34], [36]:

$$E = \zeta\tau T\gamma\sigma^2, \tag{9}$$

the harvested power for each legitimate node per communication cycle can be expressed as

$$p^{EH} = \frac{E}{(1-\tau)T} = \kappa\gamma, \tag{10}$$

where $\kappa = \frac{\zeta\tau\sigma^2}{1-\tau}$ is a convex increasing function of τ. Since the SKG procedure encompasses two cycles (from Alice to

Bob and from Bob to Alice), each legitimate node harvests $2\kappa\gamma$ overall power that can be used in the SKG mode. Thus, the SKG capacity is given by:

$$\tilde{u}(p,\tau,\gamma) = \frac{1-\tau}{2}\log_2\left(1+\frac{(p+2\kappa\gamma)\,\sigma_H^2}{2(1+\sigma^2\gamma)+\frac{(1+\sigma^2\gamma)^2}{(p+2\kappa\gamma)\sigma_H^2}}\right), \tag{11}$$

with power constraints $p \leq P$, $\gamma \leq \Gamma$.

A simple inspection of (11) reveals that this scenario is a generalization of the standard SKG setting. Indeed, if the legitimate nodes decide not to harvest energy, i.e., $\tau = 0$, (8) is obtained for $\sigma_A^2 = \sigma_B^2 = \sigma^2, N_A = N_B = 1$. In the model with EH, the legitimate nodes can maximize $\tilde{u}$ by tuning the additional variable τ. However, it is no longer straightforward that the jammer should transmit with the maximum available power as $\tilde{u}(p,\gamma,\tau)$ is no longer monotonically decreasing in γ.

Non-cooperative game theory provides the natural framework to study the adversarial interaction between the legitimate nodes and the jammer. Although game theory has already been exploited in physical layer security problems, e.g. [26], [27], to the best of our knowledge, this work is among the first to investigate EH as an effective means to counteract on jamming attacks.

A. Jammer Neutralization

Before introducing the game framework, we make two important observations regarding the SKG utility in (11) and discuss their implications.

Remark 1: For any fixed τ and γ, $\tilde{u}(p,\tau,\gamma)$ is monotonically increasing in p and

$$\arg\max_{p\in[0,P]} \tilde{u}(p,\tau,\gamma) = P. \tag{12}$$

Remark 2: For any fixed p and τ, $\tilde{u}(p,\tau,\gamma)$ is monotone in γ. In particular, it is monotonically decreasing in γ if $p > p_{th}(\tau) \triangleq \frac{2\zeta\tau}{1-\tau}$, a constant if $p = p_{th}(\tau)$, and monotonically increasing if $p < p_{th}(\tau)$. This implies that:

$$\arg\min_{\gamma\in[0,\Gamma]} \tilde{u}\,(p,\tau,\gamma) = 0, \text{ if } p < p_{th}(\tau) \tag{13}$$

$$\arg\min_{\gamma\in[0,\Gamma]} \tilde{u}\,(p,\tau,\gamma) \in [0,\Gamma], \text{ if } p = p_{th}(\tau) \tag{14}$$

$$\arg\min_{\gamma\in[0,\Gamma]} \tilde{u}\,(p,\tau,\gamma) = \Gamma, \text{ if } p > p_{th}(\tau). \tag{15}$$

Remark 1 shows that, to maximize the utility, the legitimate nodes should transmit at maximum power P. On the contrary, Remark 2 shows that the jammer should practically switch in between staying silent, i.e., $\gamma = 0$, and jamming at full power, i.e., $\gamma = \Gamma$, depending on the choice (p,τ) of the legitimate nodes.

Remark 2 reveals that the legitimate nodes can neutralize the jammer by transmitting at a relatively low power $p < p_{th}(\tau)$. Although this result may seem counter-intuitive at first, this condition is equivalent to $\tau > \tau_{th}(P) \triangleq \frac{P}{P+2\zeta}$, which means that the legitimate nodes spend a relatively large proportion of time harvesting the jamming interference before actually transmitting. In other words, the jammer is forced to stay silent since the harm it can cause by interfering in the SKG phase is overcome by the harvested energy in the EH phase. This novel result shows that the jamming interference, which is commonly thought as being harmful to the legitimate communication, can be exploited and transformed into useful power via EH. If Alice and Bob transmit with exactly $p_{th}(\tau)$, the jammer becomes indifferent between all its choices $\gamma \in [0,\Gamma]$ and has no interest in actively jamming the transmission.

The necessary conditions for the jammer neutralization are formalized below.

***Proposition** 1: The optimal strategy for the legitimate nodes that maximizes the SKG utility while ensuring that the jammer has no interest in actively jamming the transmission is given by:*

$$p^{NJ} = \min\{P, p_{th}(\tau^*)\} \text{ and } \tau^{NJ} = \min\{\tau_{th}(P), \tau^*\}, \tag{16}$$

where $\tau^* \in (0,1)$ is the unique maximizer of $\tilde{u}(p_{th}(\tau),\tau,0)$ w.r.t. τ.

For the detailed proof the reader is referred to Appendix A. Notice that, if the jammer stays silent $\gamma = 0$, there is no actual energy harvested during the EH phase of duration τ^{NJ}. Rather, the legitimate nodes' choice to use EH for a fraction of time τ^{NJ} acts as an effective threat to ensure the jammer has no interest in actively jamming the transmission. However, neutralizing the jammer may not be the overall optimal strategy for the legitimate nodes. A hint for this is that whenever $\tau^{NJ} = \tau^* < \tau_{th}(P)$, the transmit power is $p^{NJ} < P$, which we know is not optimal from Remark 1.

B. Game Formulation and Nash Equilibria

The interaction between the legitimate nodes and the jammer is formalized as a two-player zero-sum game, defined as the tuple $\tilde{\mathcal{G}} = \{\tilde{\mathcal{A}}_L, \tilde{\mathcal{A}}_J, \tilde{u}\,(p,\tau,\gamma)\}$ in which the players are: player L representing the legitimate nodes (Alice and Bob act as a single player) on one side, and player J, the jammer, on the other. The action (p,τ) of player L lies in the set $\tilde{\mathcal{A}}_L = [0,P] \times [0,1]$, and the action γ of player J lies in the set $\tilde{\mathcal{A}}_J = [0,\Gamma]$. The objective of player L is to maximize the SKG utility $\tilde{u}(p,\tau,\gamma)$ given in (11), whereas player J aims at minimizing it.

The two players are adversaries and the optimal strategy of one player depends on the choice of their opponent and cannot be determined unilaterally. In such interactive situations, the NE [37] is the natural solution concept. Intuitively, a profile $(p^{NE}, \tau^{NE}, \gamma^{NE}) \in \tilde{\mathcal{A}}_L \times \tilde{\mathcal{A}}_J$ is a NE if none of the players can benefit by deviating from this profile knowing that their opponent plays accordingly. Hence, NEs are system states that are stable to unilateral deviations.

We can easily check that the state $(p^{NJ}, \tau^{NJ}, 0)$ is not a NE since the legitimate nodes gain by deviating from it. Knowing that the jammer stays silent, player L can increase the SKG utility by deviating to $\tau = 0$. Using the whole symbol period in SKG mode increases the utility when no energy is harvested in the EH phase. This, in turn, will cause also the jammer to deviate from $\gamma = 0$ and actively jam the transmission.

Theorem 1 shows that the game $\tilde{\mathcal{G}}$ has at least one NE at which both players transmit with maximum power. This NE may be unique or not, depending on the system parameters.

***Theorem** 1: The game $\tilde{\mathcal{G}}$ has at least one NE. Moreover, the profile (P, τ^{NE}, Γ) is a NE solution such that the EH strategy is either $\tau^{NE} = 0$ or $\tau^{NE} = \min\{\tau_{th}(P), \tau_{max}\}$ with $\tau_{th}(P) = \frac{P}{P+2\zeta}$ and $\tau_{max} \in (0, 1)$ representing the critical maximum point of $\tilde{u}(P, \tau, \Gamma)$ w.r.t. τ, depending on the system parameters. If $\tau^{NE} < \tau_{th}(P)$, then the profile (P, τ^{NE}, Γ) is the unique NE of the game almost surely.*

The proof is detailed in Appendix B. We observe that, at the NE above (P, τ^{NE}, Γ) and depending on the system parameters, player L may harvest energy for a fraction of time $\tau^{NE} \leq \tau^{NJ}$ or not at all $\tau^{NE} = 0$. Intuitively, not using the SKG mode for the entire transmission symbol (for example to neutralize the jammer) becomes too costly at high SIR when the jamming interference is relatively low or negligible.

Concerning the uniqueness of the NE, the only cases in which the states $(P, 0, \Gamma)$ and $(P, \min\{\tau_{max}, \tau_{th}\}, \Gamma)$ can both be NEs is when the provided utilities are identical, i.e., $\tilde{u}(P, 0, \Gamma) = \tilde{u}(P, \min\{\tau_{max}, \tau_{th}(P)\}, \Gamma)$ in addition to the constraint on the system parameters $1 + \sigma^2\Gamma \geq \sqrt{2}\sigma_H^2 P$ (see Appendix B). However, we argue that such an equality condition on the system parameters can only happen in very special cases, otherwise stated, with zero probability (on a continuous sample space).

Furthermore, whenever player L chooses a strategy of the form $(P, \tau_{th}(P))$ at the NE, the jammer becomes indifferent between all their possible transmit powers in $[0, \Gamma]$ (as per Remark 2). Hence, in such cases, the strategy profile $(P, \tau_{th}(P), \Gamma)$ may not be the unique NE.

***Theorem** 2: If the legitimate nodes' NE strategy in Theorem 1 is such that $\tau^{NE} = \tau_{th}(P)$, the game $\tilde{\mathcal{G}}$ may have other solutions of the form $(P, \tau_{th}(P), \gamma^{NE})$ with $\gamma^{NE} \in (0, \Gamma)$. More precisely, any strategy of the form $(P, \tau_{th}(P), \gamma^{NE})$ with $\gamma^{NE} \in (0, \Gamma)$ meeting the additional condition $\arg\max_{\tau\in[0,1]} \tilde{u}(P, \tau, \gamma^{NE}) = \tau_{th}(P)$ is also a NE of the game. All such NEs provide identical utility to $\tilde{u}(P, \tau_{th}(P), \Gamma)$.*

The proof and the detailed system conditions under which the game may have other NEs of the type $(P, \tau_{th}(P), \gamma^{NE})$ with $\gamma^{NE} \in (0, \Gamma)$ aside from $(P, \tau_{th}(P), \Gamma)$ is provided in Appendix B. These NEs may exist with non-zero probability since the additional condition depends on the variable $\gamma^{NE} \in (0, \Gamma)$ and not only on the system parameters, as opposed to the condition entailing that $(P, 0, \Gamma)$ and $(P, \min\{\tau_{max}, \tau_{th}\}, \Gamma)$ are both NEs. It suffices that $\arg\max_{\tau\in[0,1]} \tilde{u}(P, \tau, \gamma^{NE}) = \tau_{th}(P)$ holds for a single value of $\gamma^{NE} \in (0, \Gamma)$ to entail the existence of such NEs.

Apart from providing a complete NE analysis, the existence of the NEs in Theorem 2 is not very relevant in practice. First, whenever they exist, the utility at such NEs is identical to the utility of the NE profile: $(P, \tau_{th}(P), \Gamma)$ in Theorem 1. Second, given Remark 2, the jammer can be assumed to restrict their strategy space from $[0, \Gamma]$ to the discrete choices $\{0, \Gamma\}$ with no loss of optimality. Assuming $\tilde{\mathcal{A}}_J = \{0, \Gamma\}$, the resulting game $\tilde{\mathcal{G}}$ has a unique pure-strategy NE (almost surely) which is given in Theorem 1.

As a last result, it turns out that neutralizing the jammer (NJ) in Proposition 1 incurs a non-trivial cost and the obtained utility is lower or equal to the NE utility.

***Proposition** 2: The SKG utility obtained when neutralizing the jammer (NJ) can never be greater that the utility at the NE. Both utilities are equal, if and only if $\tau^{NE} = \tau_{th}(P)$.*

Proof: Since $(P, \tau^{NE}) = \arg\max_{p,\tau} \tilde{u}(p, \tau, \Gamma)$, from the NE's best-response property, we have that $\tilde{u}(p^{NJ}, \tau^{NJ}, \Gamma) \leq \tilde{u}(P, \tau^{NE}, \Gamma)$. From Remark 2, we have that $\tilde{u}(p^{NJ}, \tau^{NJ}, \Gamma) = \tilde{u}(p^{NJ}, \tau^{NJ}, 0)$ (the jammer is indifferent between all its choices) and we obtain that $\tilde{u}(P, \tau^{NE}, \Gamma) \geq \tilde{u}(p^{NJ}, \tau^{NJ}, 0)$. Intuitively, when searching for the NJ state in Proposition 1 the additional condition that the jammer has to be neutralized (i.e., $p = p_{th}(\tau)$) restricts the feasible set of all pairs (p, τ) which results in an optimality loss compared to the NE. Notice that $\max_\tau \tilde{u}(p_{th}(\tau), \tau, 0) \equiv \max_\tau \tilde{u}(p_{th}(\tau), \tau, \Gamma)$. This further implies that, if $\tau^{NE} = \tau_{th}(P)$, the aforementioned restriction is optimal and $(p^{NJ}, \tau^{NJ}) = (P, \tau^{NE})$ which proves the direct implication of the second claim. The hypothesis of the reverse implication: $\tilde{u}(p^{NJ}, \tau^{NJ}, 0) = \tilde{u}(P, \tau^{NE}, \Gamma)$ is equivalent to $\tilde{u}(p^{NJ}, \tau^{NJ}, 0) = \tilde{u}(P, \tau^{NE}, 0)$. From Appendix A, the function $\tilde{u}(p_{th}(\tau), \tau, 0)$ has a unique maximizer w.r.t $\tau \in [0, \tau_{th}(P)]$ given by τ^{NJ} which results in that $(p^{NJ}, \tau^{NJ}) = (P, \tau^{NE})$. ■

C. Stackelberg Equilibrium

After investigating the NE solution of the strategic interaction in which the legitimate nodes and the jammer choose their optimal strategies simultaneously, a natural rising issue is whether the solution of the game changes assuming a hierarchy in the players' choices [24], [26], [37]. To tackle this issue, we study the SE and compare it to the NE and the jammer neutralization (NJ) states in Sec. III-B and III-A, respectively. We assume that the leader of the game L is playing first by choosing their best action (p^{SE}, τ^{SE}) while anticipating the response of player J. The follower, player J, observes the choice of the leader and reacts optimally (or best-responds) by choosing γ^{SE}.

To be specific, for an arbitrary choice of player L (p, τ), the best-response of the jammer is defined as:

$$\gamma^{BR}(p, \tau) = \arg\min_{\gamma\in[0,\Gamma]} \tilde{u}(p, \tau, \gamma). \tag{17}$$

The leader, anticipating the jammer's reaction described above, can choose their optimal strategy as follows

$$(p^{SE}, \tau^{SE}) = \arg\max_{p,\tau} \tilde{u}(p, \tau, \gamma^{BR}(p, \tau)). \tag{18}$$

The optimal strategy of the jammer is the best response $\gamma^{SE} = \gamma^{BR}(p^{SE}, \tau^{SE})$ given the optimal leader's strategy above. The solution is described in the next Theorem.

***Theorem** 3: Assuming the hierarchy described above, if $\tau^{NE} < \tau_{th}(P)$ where τ^{NE} is given in Theorem 1, the SE of the game $\tilde{\mathcal{G}}$ is unique (almost surely) and identical to the NE (P, τ^{NE}, Γ). Otherwise, if $\tau^{NE} = \tau_{th}(P)$, both the NJ state in Proposition 1 and the NE (P, τ^{NE}, Γ) are SE solutions providing identical SKG utility.*

The proof is included in Appendix C. Notice that in all possible cases $\tau^{NE} \leq \tau_{th}(P)$ (see Theorem 1). The above result shows that neutralizing the jammer is a rational solution when the strategic decisions are not taken simultaneously and the legitimate nodes play first. However, since the NJ state cannot provide a strictly better utility than the NE state (see Proposition 2), the hierarchical play does not bring an actual benefit to player L when compared with the NE.

Finally, we note that as opposed to the NE, the SE requires the leader to be able to anticipate precisely the response of the follower. For this reason, the leader cannot actually choose a strategy such that $p = p_{th}(\tau)$ which renders the follower indifferent between all its actions $\gamma \in [0, \Gamma]$ (and may choose any jamming power in an unpredictable way). A simple way to overcome this issue is for the leader to transmit at $p = p_{th}(\tau) - \varepsilon$ whenever it wants to silence the jammer (at the NJ), and to transmit at $p = p_{th}(\tau) + \varepsilon$ whenever it wants the jammer to transmit at full power (at the NE), with $\varepsilon > 0$ and $\varepsilon \ll 1$ chosen arbitrarily small, with little or no practical impact. Furthermore, this also the excludes other SE solutions (e.g., the NEs in Theorem 2 cannot be SEs).

IV. Channel Hopping vs. Power Spreading in BF AWGN Channels

If the legitimate nodes do not have EH capabilities, we investigate yet another way to defend against jamming by assuming that the legitimate nodes can employ channel hopping or power spreading strategies over multiple orthogonal subcarriers. For this, we generalize the system model (6) and (7) to an N-BF AWGN channel. Alice's and Bob's observations on the i-th subcarrier – denoted by $\hat{Y}_{A,i}$ and $\hat{Y}_{B,i}$ respectively – are expressed as:

$$\hat{Y}_{A,i} = \sqrt{p_i} H_i + \sqrt{\gamma_i} G_{A,i} + Z_{A,i}, \quad (19)$$

$$\hat{Y}_{B,i} = \sqrt{p_i} H_i + \sqrt{\gamma_i} G_{B,i} + Z_{B,i}, \quad (20)$$

where the fading coefficient in the link between Alice and Bob on the i-th subcarrier is denoted by H_i, in the link between Eve and Alice by $G_{A,i}$ and in the link between Eve and Bob by $G_{B,i}$. We assume that the fading coefficients are i.i.d. Gaussian random variables with $H_i \sim \mathcal{N}\left(0, \sigma_H^2\right)$, $G_{A,i} \sim \mathcal{N}\left(0, \sigma_A^2\right)$ and $G_{B,i} \sim \mathcal{N}\left(0, \sigma_B^2\right)$. Notice that the fading coefficients are assumed to have the same statistics. This assumption is justified, since, broadly speaking, narrowband fading depends on the bandwidth (which is the same for all subcarriers) and not on the central frequency (unlike wideband fading or large scale fading) [38]. Furthermore, the noise variables $Z_{A,i}$ and $Z_{B,i}$ are assumed to be i.i.d. Gaussian zero mean unit variance random variables. Finally, Alice and Bob exchange constant probe signals [8] with power p_i and that Eve transmits constant jamming signals [17] with power γ_i on the i-th subcarrier so that the following average power constraints are satisfied[2] [19], [21]:

$$\frac{1}{N}\sum_{i=1}^{N} p_i \leq P, \ \frac{1}{N}\sum_{i=1}^{N} \gamma_i \leq \Gamma. \quad (21)$$

Given the above model, an easy calculation reveals that the SKG capacity over the i-th subcarrier can be expressed as a function of p_i and γ_i as:

$$\begin{aligned} C(p_i, \gamma_i) &= I(\hat{Y}_{A,i}; \hat{Y}_{B,i}) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2 p_i}{N_{A,i} + N_{B,i} + \frac{N_{A,i}N_{B,i}}{\sigma_H^2 p_i}}\right), \quad (22) \\ &\text{with} \quad N_{A,i} = 1 + \sigma_A^2 \gamma_i, \quad N_{B,i} = 1 + \sigma_B^2 \gamma_i. \end{aligned}$$

In order to evaluate the overall SKG capacity, we formalize the channel hopping vs. power spreading techniques similarly to [19], [21]. When channel hopping is employed, all of the available power is used to transmit on a *single* randomly chosen subcarrier i. Therefore, when the legitimate nodes employ channel hopping on subcarrier i, then $p_i = NP$ and $p_k = 0$ for $k \neq i$, while when the jammer hops on subcarrier i then $\gamma_i = N\Gamma$ and $\gamma_k = 0, k \neq i$. On the other hand, when power spreading is used, the available power is equally distributed across all subcarriers so that $p_i = P$ and $\gamma_i = \Gamma$ $\forall i \leq N$.

When transmitting over the entire spectrum, the choice of the uniform power allocation is motivated by the fact that the nodes do not know their actual channel gains and that their statistics are identical across all frequency carriers. Moreover, assuming that player L transmits with uniform power allocation and from the convexity of the SKG function in (22) w.r.t. γ_i, it turns out that the uniform power allocation for the jammer is optimal and minimizes the overall SKG utility. More general power allocation policies can be considered in future investigations.

From an implementation point of view for the proposed channel hopping and power spreading strategies, we consider that an OFDM transmitter with a standard inverse fast Fourier transform (IFFT) block is employed. In channel hopping mode, all but a randomly chosen IFFT input are set to zero. No coordination regarding the chosen channel hopping or spreading options is required between transmitting and receiving terminals. This is possible if wideband reception is employed by all parties, allowing transmitting terminals to independently choose their strategies without coordination with the receiving terminals. Such a wideband reception of the N orthogonal subcarriers can be efficiently implemented using a standard FFT based OFDM receiver.

Using this framework in the following, for Alice and Bob the probability of channel hopping on subcarrier i is denoted by α_i $\forall i \leq N$, while α_{N+1} denotes the probability of spreading the available power uniformly over the whole spectrum. Similarly, we define β_i for the jammer. Since $\alpha = [\alpha_1, \ldots, \alpha_{N+1}]$ and $\beta = [\beta_1, \ldots, \beta_{N+1}]$ are discrete probability distributions, we have the constraints $\alpha_j \geq 0, \ \forall j$, $\sum_{i=1}^{N+1} \alpha_i = 1$, $\beta_j \geq 0, \ \forall j$, and $\sum_{i=1}^{N+1} \beta_i = 1$.

Given the above, the SKG capacity over the N orthogonal subcarriers is given by:

$$\begin{aligned} \hat{u}(\alpha, \beta) = \frac{1}{N}\Bigg\{ \sum_{i=1}^{N} \{ & \alpha_i(1 - \beta_i - \beta_{N+1}) C(NP, 0) \\ & + \alpha_i \beta_i C(NP, N\Gamma) + \alpha_i \beta_{N+1} C(NP, \Gamma) \end{aligned}$$

[2] Using constant probe signals preserves the Gaussianity of the inputs $\sqrt{p_i} H_i$, $\sqrt{\gamma_i} G_{A,i}$ and $\sqrt{\gamma_i} G_{B,i}$, which is optimal for the legitimate nodes and the jammer in our AWGN setting.

$$+\alpha_{N+1}\beta_i[(N-1)C(P,0)+C(P,N\Gamma)]\}$$
$$+\alpha_{N+1}\beta_{N+1}NC(P,\Gamma)\Big\}, \qquad (23)$$

where the normalization $\frac{1}{N}$ accounts for measuring the SKG capacity in bits/s/Hz. In (23), the first term corresponds to the case in which Alice (resp. Bob) hops on subcarrier i and the jammer hops on a different subcarrier; the second term to the case in which Alice (resp. Bob) and the jammer both hop on subcarrier i; the third term to the case in which Alice (resp. Bob) hops on subcarrier i and the jammer spreads; the fourth term to the case in which the Alice (resp. Bob) spreads and the jammer hops on subcarrier i. Finally, the last term corresponds to the case in which they both spread their power.

A. Game Formulation and Nash Equilibria

We model the competitive interaction between player L and J as the following zero-sum game $\hat{\mathcal{G}} = \{\hat{\mathcal{A}}_L, \hat{\mathcal{A}}_J, \hat{u}(\alpha,\beta)\}$, where the payoff $\hat{u}(\alpha,\beta)$ is given in (23). The action sets of the players are the probabilities of channel hopping and power spreading:

$$\hat{\mathcal{A}}_L = \left\{\alpha \in [0,1]^{N+1} \middle| \sum_{i=1}^{N+1} \alpha_i = 1\right\},$$
$$\hat{\mathcal{A}}_J = \left\{\beta \in [0,1]^{N+1} \middle| \sum_{i=1}^{N+1} \beta_i = 1\right\}.$$

As we have argued in the previous section, the natural solution in such a strategic interaction without cooperation among the opponents is the NE.

To derive the game's NE, let us introduce a finite discrete game $\hat{\mathcal{G}}^D = \{\hat{\mathcal{E}}_L, \hat{\mathcal{E}}_J, \hat{u}(\alpha,\beta)\}$ with action sets defined as $\hat{\mathcal{E}}_L \equiv \hat{\mathcal{E}}_J = \{e_1,\ldots,e_N,e_{(N+1)}\}$, where $e_i \in \{0,1\}^{N+1}$ is the canonical vector containing 1 on the i-th position and 0 otherwise. The i-th action e_i represents channel hopping on subcarrier i for all $i \leq N$ and e_{N+1} represents spreading the power across the spectrum. Such finite discrete games always have at least one NE in mixed strategy (α^*,β^*) [37, Sec. 1.3.1]. We observe that our game $\hat{\mathcal{G}}$ represents the mixed strategy extension of $\hat{\mathcal{G}}^D$ and thus $\hat{\mathcal{G}}$ has at least one NE.

***Corollary** 1:* [37, Thm. 1.1] *Game $\hat{\mathcal{G}}$ has at least one NE.*

To compute the NE, one possibility is to use the Minimax Theorem of von Neumann and Morgenstern [39] which allows us to compute mixed NE of any two-player zero-sum game via linear programming (i.e., by solving two dual linear optimization problems). In our case, we show that the NE can be characterized in an analytical closed-form manner without the need of solving any optimization problem. To this aim, an alternative characterization of the NE (see Definition 1.2 in [37, Sec.1.2.1]) is used:

***Definition** 1: A strategy profile $(\alpha^*,\beta^*) \in \hat{\mathcal{A}}_L \times \hat{\mathcal{A}}_J$ is a NE of the game $\hat{\mathcal{G}}$ if the following hold:*

i) *both players are indifferent among the pure actions that are played with positive probability at the NE*

$$\hat{u}(\alpha^*,e_i) = \hat{u}(\alpha^*,e_k), \ \forall i,k, \in \mathcal{I}_J,$$
$$\hat{u}(e_i,\beta^*) = \hat{u}(e_k,\beta^*), \ \forall i,k, \in \mathcal{I}_L,$$

ii) *the pure actions that result in strictly smaller payoffs are played with zero probability at the NE*

$$\text{if } \hat{u}(\alpha^*,e_i) < \hat{u}(\alpha^*,e_k), \ i \in \mathcal{I}_J, \text{then } k \in \mathcal{N}_J,$$
$$\text{if } \hat{u}(e_i,\beta^*) > \hat{u}(e_k,\beta^*), \ i \in \mathcal{I}_L, \text{then } k \in \mathcal{N}_L,$$

where the sets $\mathcal{N}_L, \mathcal{I}_L \subseteq \{1,\ldots,N+1\}$ denote, respectively, the indices of the pure actions that are not played at the NE and those that are played at the NE by player L: $\mathcal{N}_L = \{i|\alpha_i^* = 0\}$, $\mathcal{I}_L = \{1,\ldots,N+1\} \setminus \mathcal{N}_L$; similarly, the sets $\mathcal{N}_J, \mathcal{I}_J \subseteq \{1,\ldots,N+1\}$ denote, respectively, the set of indices of the pure actions that are not used or are used by player J at the NE: $\mathcal{N}_J = \{i|\beta_i^* = 0\}$, and $\mathcal{I}_J = \{1,\ldots,N+1\} \setminus \mathcal{N}_J$.

At a first glance, Definition 1 provides a simple way to compute the NE of the game $\hat{\mathcal{G}}$ by solving a system of linear equations and checking some conditions. Still, in order to use Definition 1, one would have to know in advance the faces of the simplex $\hat{\mathcal{A}}_L \times \hat{\mathcal{A}}_J$ on which the NEs lie, i.e., one would have to know $\mathcal{I}_L$, $\mathcal{I}_J$ for all NEs. An exhaustive search has an exponential complexity (the $N+1$-simplex has $2^{N+1}-1$ faces). Nevertheless, the NE of our game $\hat{\mathcal{G}}$ have a special structure which allows us to exploit Definition 1 and fully characterize the set of NE in a simple manner.

To characterize the set of NEs as function of the system's parameters we begin by examining the matrix structure of the discrete game $\hat{\mathcal{G}}^D$ given in Table I. We notice that there is a symmetry between the channel hopping strategies. In particular, the payoff does not depend on the particular index of the chosen subcarrier but only on whether both players hop on the same subcarrier or not. This symmetry allows us to show that the NE of the game $\hat{\mathcal{G}}$ have a particular structure specified in the following propositions.

***Proposition** 3: At the NE (α^*,β^*), a player uses either all channel hopping actions with non-zero probability or none of them: either $\alpha_i^* = 0, \ \forall i \leq N$ or $\alpha_i^* \neq 0, \ \forall i \leq N$, and similarly, either $\beta_i^* = 0, \ \forall i \leq N$ or $\beta_i^* \neq 0, \ \forall i \leq N$.*

***Proposition** 4: If both players employ channel hopping with non-zero probability at the NE, i.e., $\alpha_i^* > 0$ and $\beta_i^* > 0 \ \forall i \leq N$, then the players will hop uniformly across all channels and the NE will have the following structure: $\alpha^* = (a,\ldots,a,(1-Na))$, $\beta^* = (b,\ldots,b,(1-Nb))$ for some $0 \leq a \leq 1/N$, $0 \leq b \leq 1/N$.*

Propositions 3 and 4 are proven in Appendices D and E. These results shape the special structure of the NE of $\hat{\mathcal{G}}$, which, alongside Definition 1 and the strict convexity of $C(p,\gamma)$ w.r.t. γ, allows us to fully characterize the set of NEs in a very simple and explicit manner as function of the system parameters.

***Theorem** 4: The set of NE of the game $\hat{\mathcal{G}}$ is characterized as follows:*

1. If $C(NP,\Gamma) < NC(P,\Gamma)$, then the game has a unique pure-strategy NE: both players spread their powers, $\alpha^* = \beta^* = e_{N+1}$.

2. If $C(NP,\Gamma) > NC(P,\Gamma)$, then player L hops and player J spreads at the NE: $\alpha^* = (\alpha_1,\ldots,\alpha_N,0)$ and $\beta^* = e_{N+1}$.

TABLE I
TWO PLAYER ZERO-SUM DESCRIPTION OF $\hat{\mathcal{G}}_d$

	e_i, $i \le N$	e_k, $k \le N, k \neq i$	e_{N+1}
e_i, $i \le N$	$\frac{1}{N}C(NP, N\Gamma)$	$\frac{1}{N}C(NP, 0)$	$\frac{1}{N}C(NP, \Gamma)$
e_k, $k \le N, k \neq i$	$\frac{1}{N}C(NP, 0)$	$\frac{1}{N}C(NP, N\Gamma)$	$\frac{1}{N}C(NP, \Gamma)$
e_{N+1}	$\frac{N-1}{N}C(P, 0) + \frac{1}{N}C(P, N\Gamma)$	$\frac{N-1}{N}C(P, 0) + \frac{1}{N}C(P, N\Gamma)$	$C(P, \Gamma)$

The NE strategies of player L are given by the (infinite number of) solutions to the following system of linear inequalities:

$$\begin{cases} 0 \le \alpha_i \le 1, \ \forall i \le N, \\ \sum_{j=1}^{N} \alpha_j = 1, \\ \alpha_i < \frac{C(NP,0) - C(NP,\Gamma)}{C(NP,0) - C(NP,N\Gamma)}, \ \forall i \le N. \end{cases}$$

In particular, the uniform probability over the channels is one of the NE solutions: $\alpha^* = (1/N, \ldots, 1/N, 0)$. All NEs are equivalent in terms of achieved utility.

3. *If $C(NP, \Gamma) = NC(P, \Gamma)$, player L employs all their actions and player J spreads at the NE: $\alpha^* = (\alpha_1, \ldots, \alpha_N, \alpha_{N+1})$ and $\beta^* = e_{N+1}$. The NE strategies of player L are the (infinite number of) solutions to the following linear system of inequalities:*

$$\begin{cases} \alpha_i \ge 0, \ \forall i \le N, \\ \sum_{j=1}^{N} \alpha_j = 1, \\ \alpha_i [C(NP, N\Gamma) - C(NP, 0)] + \alpha_{N+1} [(N-1)C(P, 0) \\ +C(P, N\Gamma) - C(NP, 0) + C(NP, \Gamma) - NC(P, \Gamma)] \\ > C(NP, \Gamma) - C(NP, 0), \ \forall i \le N. \end{cases}$$

In this case, both players spreading (case 1) is an NE. Also, player J spreading and player L hopping strategies (case 2) are all NEs. All NEs are equivalent in terms of achieved utility.

The proof is provided in Appendix F. We remark that the NE can be unique and in pure strategies if $C(NP, \Gamma) < NC(P, \Gamma)$ and the outcome of the game provides a utility equal to $\hat{u}(\alpha^*, \beta^*) = C(P, \Gamma)$. On the contrary, if $C(NP, \Gamma) \ge NC(P, \Gamma)$, there are an infinite number of NEs which are generally in mixed strategies. All these NEs are equivalent in terms of achieved utility, which equals $\hat{u}(\alpha^*, \beta^*) = \frac{1}{N}C(NP, \Gamma)$. Hence, the outcome of the game can be predicted without the need for implementing iterative or learning procedures.

Theorem 4 also shows that the optimal strategy for the jammer is always spreading their power across the entire spectrum. Intuitively, if the jammer were to use channel hopping, player L would exploit this fact and would also hop; this scenario is unfavorable for the jammer as the probability that both players hop on the same subcarrier equals $\frac{1}{N^2}$ (due to Proposition 3, when both players hop at the NE, they use uniform probabilities). Thus, the jammer's payoff from hopping cannot exceed that gained from spreading, assuming that the legitimate nodes play their optimal strategy. On the contrary, for player L the best strategy can be either channel hopping or power spreading depending on which provides higher utility against a spreading jammer.

B. Stackelberg Equilibrium

In Sec. III-C, we have shown that the hierarchy of play among the adversaries does not bring an advantage to the legitimate nodes assuming they have EH capabilities. Here, we investigate whether this remains true in OFDM systems in which the players choose between channel hopping and power spreading strategies. The leader, player L, is assumed to play first and to choose α^{SE} anticipating the jammer's response. The follower, player J, observes α^{SE} and best-responds by choosing β^{SE}.

More precisely, the best-response of the jammer for an arbitrary choice of α is defined as: $\beta^{BR}(\alpha) = \arg\min_\beta \hat{u}(\alpha, \beta)$. Thus, the leader chooses their optimal strategy as follows

$$\alpha^{SE} = \arg\max_{\alpha} \hat{u}(\alpha, \beta^{BR}(\alpha)) \tag{24}$$

and the resulting best-response or SE strategy of the jammer is $\beta^{SE} = \beta^{BR}(\alpha^{SE})$.

To characterize the SE in closed-form, we use a similar approach as for the NE: we show first that the leader's strategy at the SE has a special form described below. Then, we exploit this structure to provide the SE solution.

***Proposition** 5: At the SE, the legitimate player uses either all hopping strategies with uniform probability or none of them, i.e., $\alpha^{SE} = (a, \ldots, a, 1 - Na)$ for some $a \in [0, 1/N]$.*

The proof is provided in Appendix G. The above structure of α^{SE} allows us to analyze the optimal response of the jammer β^{SE} and to prove that, in all cases, the jammer's best strategy is to spread: $\beta^{SE} = (0, \ldots, 0, 1)$. On the other hand, depending on the channel parameters, the leader will either channel hop or spread their powers, identically to the NE.

***Theorem** 5: The set of SEs of the game $\hat{\mathcal{G}}$ is identical to the set of NEs.*

The proof is provided in Appendix H. Therefore, the legitimate nodes do not gain in utility by choosing first their strategy as opposed to the NE where both players choose their strategies simultaneously.

V. NUMERICAL ILLUSTRATIONS AND DISCUSSION

In this Section, several representative illustrations are chosen allowing the deduction of generic conclusions that carry over most setups. The benchmark setting is chosen as follows: unit jamming power $\Gamma = 1$, unit variance Rayleigh channel coefficients $\sigma_A^2 = \sigma_B^2 = \sigma^2 = \sigma_H^2 = 1$.

A. EH at the Legitimate nodes

We start by evaluating the SKG capacity at the NJ in Proposition 1 and NE in Theorem 1 as functions of the system parameters for a harvesting efficiency $\zeta = 0.7$. In Fig. 2, the relative gain in utility obtained at the NE compared with the NJ, defined by $E \triangleq \frac{C^{NE} - C^{NJ}}{C^{NE}}$, is depicted as a function of the signal to interference ratio (SIR) P/Γ for different

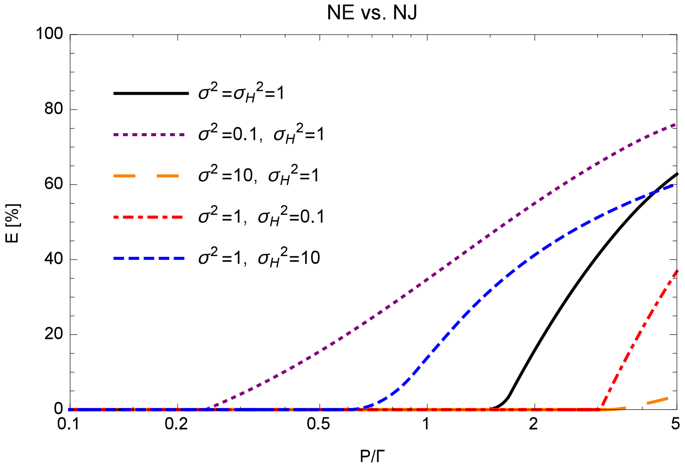

Fig. 2. Relative utility gain at the NE vs. NJ $E = (C^{NE} - C^{NJ})/C^{NE}$ as a function of $P/\Gamma \geq 0$ for $\zeta = 0.7$.

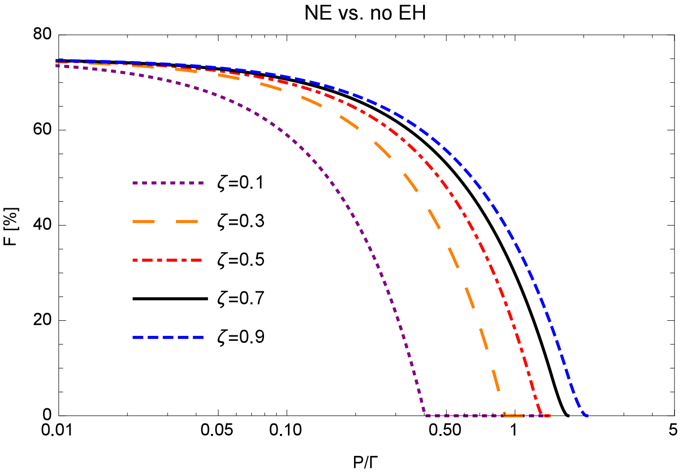

Fig. 3. Relative utility gain at the NE vs. no EH: $F = (C^{NE} - C^{noEH})/C^{NE}$ as a function of $P/\Gamma \geq 0$.

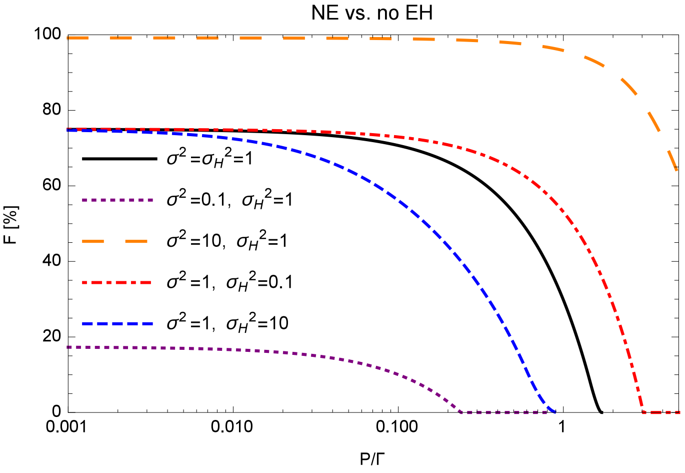

Fig. 4. Relative utility gain at the NE vs. no EH: $F = (C^{NE} - C^{noEH})/C^{NE}$ as a function of $P/\Gamma \geq 0$ for $\zeta = 0.7$ and different channel parameters.

values of σ^2 and σ_H^2. In the investigated settings, the NJ strategy never outperforms the NE in terms of utility, which is consistent with Proposition 2. When the SIR P/Γ is relatively low, both the NE and the NJ provide identical utilities. In this case, $p^{NJ} = P$ and $\tau^{NJ} = \tau^{NE} = \tau_{th}(P)$, the jammer is indifferent between $\{0, \Gamma\}$ and both states are SE solutions. With increasing SIR P/Γ, it is no longer optimal for the legitimate nodes to harvest energy for a fraction of time $\tau_{th}(P)$ in order to neutralize the jammer. Instead, by limiting the duration of EH to $\tau^{NE} < \tau_{th}(P)$ the SKG capacity increases in spite of the full power jamming $\gamma = \Gamma$ and only the NE is also a SE solution. Moreover, as the SIR increases, e.g., for $P/\Gamma \gg 1$, the legitimate nodes should not harvest energy at all as the jammer's interference is relatively negligible.

Notice that Fig. 2 also illustrates the SE solution described in Theorem 3. Indeed, at low SIR, when both NE and NJ provide equal SKG capacity, they are both SE solutions. At high SIR, the SE is unique and identical to the NE.

Subsequently, we evaluate the impact of the EH capability on the SKG capacity at the NE. The relative gain in utility obtained at the NE compared with the case in which there is no EH capability $C^{NoEH} = C(P, 0, \Gamma)$, defined as $F \triangleq \frac{C^{NE} - C^{NoEH}}{C^{NE}}$, is depicted as a function of P/Γ in Fig. 3. The benchmark setup is considered and the different curves correspond to harvesting efficiencies $\zeta \in \{0.1, 0.3, 0.5, 0.7, 0.9\}$. As expected, F increases with the harvesting efficiency ζ. For $P/\Gamma = 1$ and $\zeta = 0.5$ the gain in using EH is around 20 % while it increases to 30 % for $\zeta = 0.7$. At low SIR P/Γ the gain observed can reach 60 %, while at the high SIR it is negligible as expected.

Finally, the relative utility F defined above is depicted in Fig. 4 for $\zeta = 0.7$ and various channel parameters. For low SIR P/Γ, there is a significant gain in utility when employing EH. This gain becomes significantly large at very low SIR, exceeding 97.5 % when the legitimate nodes experience poor channel conditions as opposed to the jammer. When both parties experience similar channel conditions the gain is in the range of 60 % in the medium SIR. Overall, the numerical results demonstrate that using EH as a counter-jamming technique is of particular interest in the low and medium SIR regimes but, as expected, does not increase the utility in the high SIR.

B. Channel Hopping vs. Power Spreading

First, we analyze the NE as function of N and the ratio P/Γ for the benchmark scenario in Fig. 5. There exist two regions delimited by the curve $C(NP, \Gamma) = NC(P, \Gamma)$: a region in which the NE is unique and both players spread their power, and a region in which the jammer spreads their power and the legitimate nodes employ channel hopping.

Player L hops at the NE below the curve, when the SIR P/Γ is relatively small. This is intuitive since, in the low transmit power regime, the legitimate nodes should avoid as much jamming interference as possible by transmitting on a single subcarrier, which also means that their available power is concentrated on a single channel. In Fig. 6, the NE regions are illustrated for different channel parameters. When σ_H^2 increases, the region in which player L should employ channel

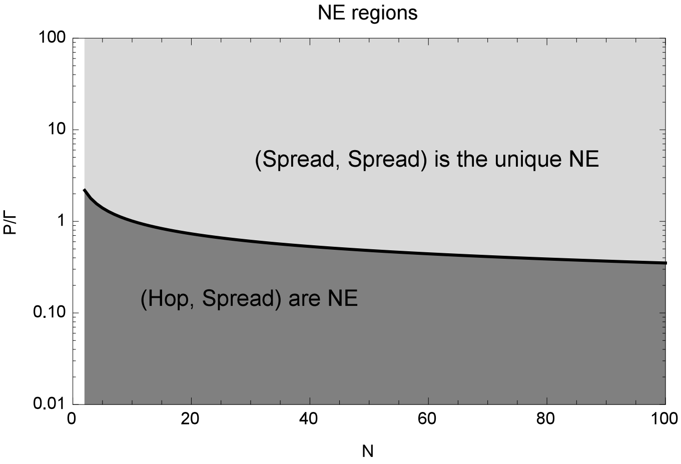

Fig. 5. NE regions as a function of $P/\Gamma \geq 0$ and $N \geq 2$ for $\Gamma = \sigma_A^2 = \sigma_B^2 = \sigma_H^2 = 1$.

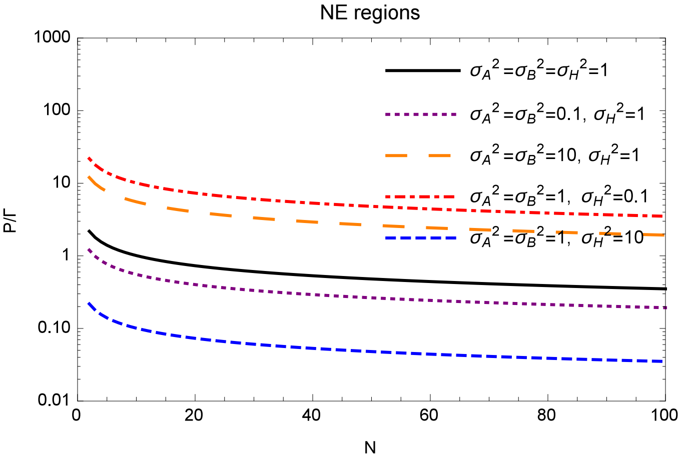

Fig. 6. NE regions as a function of $P/\Gamma \geq 0$ and $N \geq 2$ for $\Gamma = 1$ and different channel parameters.

hopping at the NE shrinks down while when σ_A^2, σ_B^2 increase, this region expands.

In Fig. 7, the relative gain obtained by player L when employing the NE strategy as opposed to a naive hopping strategy is depicted. The relative utility gain $D_H = (u^{NE} - u^{Hop,Spread})/u^{NE}$, where $u^{Hop,Spread} = 1/NC(NP, \Gamma)$ is relatively large (up to 80%) in the high SIR regime, in which case the optimal strategy for player L is to use the entire spectrum in spite of the jammer's interference.

Finally, in Fig. 8, the relative utility gain when using the NE strategy over N subcarriers as opposed to a single subcarrier ($u^{single} = C(P, \Gamma)$) is investigated for $\Gamma = \sigma_H^2 = \sigma_A^2 = \sigma_B^2 = 1$ as a function of P/Γ for $N \in \{2, 4, 8, 16, 32, 64\}$. At low SIR, when the channel hopping strategy is optimal for the legitimate nodes, the higher the number of subcarriers N, the lower the jammer's interference in each subcarrier, and hence, the higher the SKG capacity. At last, in the high SIR regime, when spreading is optimal the SKG utility becomes $C(P, \Gamma)$, which is identical to transmitting over a single channel with powers P and Γ.

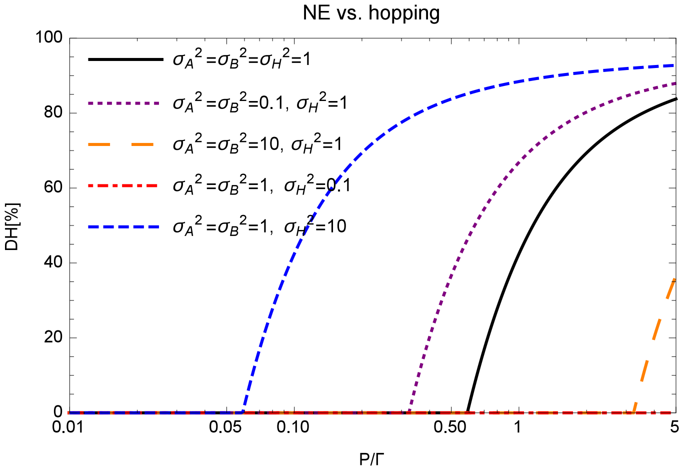

Fig. 7. Relative utility gain between the NE vs. always hopping: $D_H = (u^{NE} - u^{Hop,Spread})/u^{NE}$ as a function of P/Γ for $N = 32$, $\Gamma = 1$ and different channel parameters.

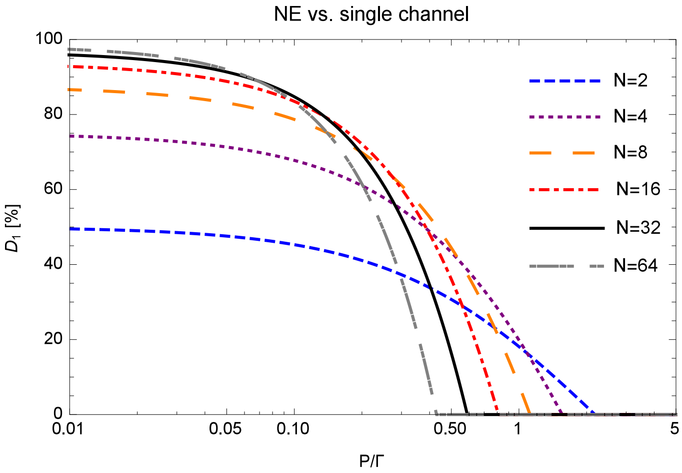

Fig. 8. Relative utility gain between the NE vs. single channel SKG: $D_1 = (u^{NE} - u^{single})/u^{NE}$ as a function of P/Γ for $\Gamma = \sigma_H^2 = \sigma_A^2 = \sigma_B^2 = 1$ and $N \in \{2, 4, 8, 16, 32, 64\}$.

Remark that all figures illustrating the NE, in this subsection, also illustrate the SE solution, since the SE is identical to the NE as per Theorem 5.

C. Discussion and Perspectives

We discuss here the differences and similarities between the two approaches: a) EH at the legitimate nodes, and b) employing channel hopping or power spreading techniques.

EH at the legitimate nodes enables them to completely neutralize the jammer. By harvesting the jamming power in a first phase and exploiting it for SKG in a second phase, the jammer's attacks may increase the SKG capacity; in this case, the jammer should not launch the attack, i.e., is neutralized. However, it is not always optimal for the legitimate nodes to neutralize the jammer. Indeed, using EH can reduce the SKG capacity since, for a non-trivial fraction of time, there is no useful communication; when the jammer is neutralized the penalty in terms of utility might become too high, depending on the system parameters (e.g., high SIR regime). In such cases, the obtained utility at the NE is strictly higher than the one at the NJ state.

On the other hand, in the case of BF AWGN channels (i.e., in systems with multiple orthogonal subcarriers), the idea is to use channel hopping in a random fashion and avoid most of the jammer's interference as opposed to completely neutralizing it. Since potential jammers cannot predict the subcarrier used by the legitimate nodes, they will always spread their powers over the entire spectrum: the larger the number of subcarriers, the smaller the jammer's interference on each subcarrier. However, channel hopping is not always optimal since only a fraction of the entire spectrum is used for SKG transmission. Depending on the system parameters (high SIR), it can be preferable for the legitimate nodes to spread the available power across the entire spectrum rather than concentrate it on a single subcarrier. In this case, the SKG capacity (measured in bits/s/Hz) is identical to that of single channel with the same average power constraints.

In the critical cases of low and medium SIR regimes ($P/\Gamma < 1$), both approaches turn out to be advantageous in terms of SKG capacity compared to a single channel SKG system without EH capabilities; the gains in SKG capacity depend on the harvesting duration or the number of subcarriers N. On the contrary, in the high SIR regime ($P/\Gamma \gg 1$), the jammer's impact and interference become relatively low or even negligible and the cost of counter-jamming measures might not be justified compared to simply tolerating it. However, the interesting cases are indeed the former ones in which the jamming power is higher or of the same order as the legitimate nodes' transmit powers, in which settings overcoming the attack becomes critical.

For both approaches it turns out that a hierarchical decision model that in principle could favor the legitimate nodes compared to a simultaneous decision model does not bring an actual benefit. Indeed, the SKG utility obtained at the SE is identical to the SKG utility at the NE (even though the set of SEs is not necessarily identical to the set of NEs as in the EH approach).

Several questions arise for future work. First, an interesting issue would be to study reactive vs. proactive jamming [40] as well as the joint use of EH and multi-carrier transmission against jamming attacks. Second, in the EH case, the study of more realistic models accounting for finite storage capabilities, asymmetries in the legitimate nodes' parameters and EH at the jammer's side, are interesting future extensions. Moreover, the study of multi-user and multi-jammer interactions as well as games of incomplete information are challenging open issues.

VI. Conclusions

In this work, the adversarial interaction between a pair of legitimate nodes and a malicious jammer in a wireless key generation framework was investigated. Two different counter-jamming approaches were proposed and studied. First, EH at the legitimate nodes, and, second, channel hopping vs. power spreading in BF AWGN channels. In either approach, a zero-sum game was introduced as the objectives of the two parties involved were opposed. Complete characterizations of the NEs and the SEs in closed-form were provided in both cases. It was demonstrated that either approach may offer significant gains in utility, particularly in the low SIR regime, in which counteracting the jamming interference becomes crucial. As a result, viable and low complexity alternatives for defending SKG systems may be developed by exploiting either novel transceiver features or available spectral resources.

Appendix

A. Proof of Proposition 1

Let us assume that the legitimate nodes neutralize the jammer by transmitting at power $p \in [0, \min\{p_{th}(\tau), P\}]$. The jammer observes player L's choice and from Remark 2, decides to stay silent. Notice that player L can force the jammer to remain silent by transmitting at $p \in [0, \min\{p_{th}(\tau) - \varepsilon, P\}]$ for an arbitrarily small $\varepsilon > 0$. For simplicity, $\varepsilon \simeq 0$ is assumed in the following.

The remaining question is: how will player L choose $\tau \in [0, 1)$ and $p \in [0, \min\{p_{th}(\tau), P\}]$ to maximize the resulting SKG utility

$$\tilde{u}(p, \tau, 0) = \frac{1-\tau}{2} \log_2 \left(1 + \frac{p\sigma_H^2}{2 + \frac{1}{p\sigma_H^2}} \right), \tag{25}$$

while ensuring that the jammer stays silent and cannot decrease the utility by transmitting with non-zero power. Since the feasible set of p depends on τ, we first have to find the maximum of $\tilde{u}(p, \tau, 0)$ w.r.t. p for any fixed τ. The function $\tilde{u}(p, \tau, 0)$ is strictly increasing in p and, hence, the optimal power is given by $\tilde{p}(\tau) = \min\{P, p_{th}(\tau)\}$. Now, we need to maximize $\tilde{u}(\tilde{p}(\tau), \tau, 0)$ w.r.t. $\tau \in [0, 1]$:

$$\tilde{u}(p_{th}(\tau), \tau, 0) = \frac{1-\tau}{2} \log_2 \left(1 + \frac{2\zeta\sigma_H^2\tau}{(2 + \frac{1-\tau}{2\zeta\sigma_H^2\tau})(1-\tau)} \right).$$

At the extremes $\tau = 0$ and $\tau \to 1$ the utility goes to zero. By investigating its second order derivatives w.r.t. τ, which amounts to the following quadratic equation:

$$(1-\tau)^2 - 8\sigma_H^4\zeta^2\tau^2 = 0, \tag{26}$$

it can be shown that $\tilde{u}(p_{th}(\tau), \tau, 0)$ always has an inflexion point in between $(0, 1)$ and starts as convex and then becomes concave. Knowing that the the utility is always positive, we can conclude that $\tilde{u}(p_{th}(\tau), \tau, 0)$ has a unique critical point that is the global maximizer $\tau^* \in (0, 1)$ and which is the solution to $\frac{d\tilde{u}(p_{th}(\tau), \tau, 0)}{d\tau} = 0$. This implies that, if $p_{th}(\tau^*) \leq P$, then the optimal solution that neutralizes the jammer is $\tau^{NJ} = \tau^*$ and $p^{NJ} = p_{th}(\tau^*)$. If $p_{th}(\tau^*) > P$, then the optimal solution that neutralizes the jammer is $p^{NJ} = P$ and $\tau^{NJ} = \tau_{th}(P) = \frac{P}{P+2\zeta}$.

B. Proof of Theorem 1 and Theorem 2

From Remark 1, we know that transmitting at maximum power is a strictly dominant strategy for player L and, hence, $p^{NE} = P$. We first prove that at the NE, player L will not operate in EH mode for longer than the threshold $\tau_{th}(P)$. Let's suppose by absurdum that $\tau^{NE} > \tau_{th}(P)$, then the jammer's best response would be to remain silent $\gamma^{NE} = 0$ (as the energy harvested from the jammer in the EH phase is enough to overcome the interference inflicted by the jammer in the SKG phase). Then, the optimal τ^{NE} maximizing the utility $\tilde{u}(P, \tau, 0)$ (which is decreasing in τ) would be $\tau^{NE} \to \tau_{th}(P)$ obtaining the utility $\tilde{u}^{NE} \to \tilde{u}(P, \tau_{th}(P), 0)$. However, this state cannot be an NE. Indeed, if the jammer stays silent $\gamma^{NE} = 0$, no energy is harvested during τ^{NE} and player L gains in utility by deviating to $\tau = 0$. This will also cause the jammer to deviate to $\gamma = \Gamma$.

The above implies that, player L can only choose an EH strategy such that $\tau^{NE} \leq \tau_{th}(P)$ at the NE. This condition is equivalent to $P \geq p_{th}(\tau^{NE})$, which means that the utility is either decreasing or simply a constant in γ (see Remark 2). This further implies that if the jammer uses maximum power $\gamma^{NE} = \Gamma$, then it cannot benefit by deviating unilaterally. Hence, to find the NE of the form (P, τ^{NE}, Γ), we only need to find the optimal value or values of $\tau \in [0, \tau_{th}(P)]$ that maximizes the function $\tilde{u}(P, \tau, \Gamma)$ given by:

$$\tilde{u}(P, \tau, \Gamma) = \frac{1-\tau}{2} \log_2 \left(1 + \frac{(P + 2\kappa(\tau)\Gamma)\, \sigma_H^2}{2(1+\sigma^2\Gamma) + \frac{(1+\sigma^2\Gamma)^2}{(P+2\kappa(\tau)\Gamma)\sigma_H^2}} \right),$$

where $\kappa(\tau) = \frac{\zeta\tau\sigma^2}{1-\tau}$. At $\tau = 0$, this function is strictly positive $\tilde{u}(P, 0, \Gamma) > 0$ equal to the SKG capacity without EH and, when $\tau \to 1$ the function goes to 0. By investigating the second order derivative of $\tilde{u}(P, \tau, \Gamma)$ w.r.t. τ, which amounts to the analysis of the following quadratic equation

$$(1-\tau)^2(1+\sigma^2\Gamma)^2 - 2\sigma_H^4(P(1-\tau) + 2\sigma^2\zeta\Gamma\tau)^2 = 0, \quad (27)$$

two different cases arise:

- *Case A:* If $1 + \sigma^2\Gamma \geq \sqrt{2}\sigma_H^2 P$, this function has a unique inflexion point that lies in $(0, 1)$ and the function starts as convex and then becomes concave. Thus, $\tilde{u}(P, \tau, \Gamma)$ has a critical point that is a local maximum $\tau_{max} \in (0, 1)$, which is a solution of the equation $\frac{d\tilde{u}(P,\tau,\Gamma)}{d\tau} = 0$. Hence, the optimal strategy is given by either the maximal point τ_{max} or by one (or both) of the borders of the interval $[0, \tau_{th}(P)]$ depending on the system parameters:

$$\tau^{NE} = \arg \max_{\tau \in \{0, \min\{\tau_{th}(P), \tau_{max}\}\}} \tilde{u}(P, \tau, \Gamma). \quad (28)$$

- *Case B:* If $1 + \sigma^2\Gamma < \sqrt{2}\sigma_H^2 P$, then the function is always concave (and it does not have an inflexion point) in $(0, 1)$. If the function has a critical point in $(0, 1)$, then this critical point is a maximum point denoted by τ_{max} and $\tau^{NE} = \min\{\tau_{th}(P), \tau_{max}\}$. Otherwise, the function is concave decreasing and $\tau^{NE} = 0$.

Remark that, at least in theory, Case A can lead to the existence of two NEs whenever the additional equality condition is met: $\tilde{u}(P, 0, \Gamma) = \tilde{u}(P, \min\{\tau_{th}(P), \tau_{max}\}, \Gamma)$, i.e., when both borders of the interval $[0, \min\{\tau_{max}, \tau_{th}(P)\}]$ provide equal maximum utility. However, this can happen only in very special cases of the system parameters or with zero probability.

Since the state $(P, \tau_{th}(P), 0)$ is not a NE, the game has (almost surely) a unique NE of the form (P, τ^{NE}, Γ) where τ^{NE} depends on the system parameters. Aside from the zero probability case described above, this profile may not be the unique NE of the game $\tilde{\mathcal{G}}$ as there may exist other NEs such that $\gamma^{NE} \in (0, \Gamma)$. Such cases can only happen if the strategy of player L at the NE equals $(P, \tau_{th}(P))$ or equivalently if $(P, \tau_{th}(P), \Gamma)$ is a NE of the game. Otherwise, whenever $\tau^{NE} < \tau_{th}(P)$, the utility is strictly decreasing in γ and the only strategy of the jammer at the NE is Γ (case discussed previously).

Now, whenever the legitimate user chooses their strategy $(P, \tau_{th}(P))$, the jammer becomes totally indifferent between all their strategies and, in particular, all jamming powers in $(0, \Gamma)$ provide the same utility (see Remark 2). Hence, in this case, there may be other NEs aside from $(P, \tau_{th}(P), \Gamma)$ that provide identical utilities to $\tilde{u}(P, \tau_{th}(P), \Gamma)$.

In order to find all NE of the form $(P, \tau_{th}(P), \gamma^{NE})$, we need to find all $\gamma^{NE} \in (0, \Gamma)$ such that the legitimate user cannot deviate from $(P, \tau_{th}(P))$ or it will lose in terms of utility. Stated otherwise, all $\gamma^{NE} \in (0, \Gamma)$ such that $\tau_{th}(P) = \arg\max_\tau \tilde{u}(P, \tau, \gamma^{NE})$ provide additional NE profiles of the form $(P, \tau_{th}(P), \gamma^{NE})$.

The analysis of the utility $\tilde{u}(P, \tau, \gamma^{NE})$ as a function of τ is very similar to $\tilde{u}(P, \tau, \Gamma)$ above. There are two cases in function of the system parameters.

- *Case A:* If $1 + \sigma^2\Gamma \geq \sqrt{2}\sigma_H^2 P$, for all $\gamma^{NE} \in \left[\frac{\sqrt{2}\sigma_H^2 P - 1}{\sigma^2}, \Gamma\right)$, the function $\tilde{u}(P, \tau, \gamma^{NE})$ has a unique inflexion point that lies in $(0, 1)$ and starts as convex and then becomes concave. Thus, $\tilde{u}(P, \tau, \gamma^{NE})$ has a critical point that is a local maximum $\tau_{max}(\gamma^{NE}) \in (0, 1)$, which is a solution of the equation $\frac{d\tilde{u}(P,\tau,\gamma^{NE})}{d\tau} = 0$. The additional conditions for the strategy $(P, \tau_{th}(P))$ to be optimal for player L are:

$$\begin{array}{lcl} \tau_{th}(P) & \leq & \tau_{max}(\gamma^{NE}) \\ \tilde{u}(P, 0, \gamma^{NE}) & \leq & \tilde{u}(P, \tau_{th}(P), \gamma^{NE}) \end{array} \quad (29)$$

- *Case B:* If $1 + \sigma^2\Gamma < \sqrt{2}\sigma_H^2 P$, for all $\gamma^{NE} \in \left(0, \frac{\sqrt{2}\sigma_H^2 P - 1}{\sigma^2}\right)$, the function $\tilde{u}(P, \tau, \gamma^{NE})$ is always concave in $\tau \in (0, 1)$. If the function has a critical point in $(0, 1)$, then this critical point is a maximum point denoted by $\tau_{max}(\gamma^{NE})$. The additional condition for the strategy $(P, \tau_{th}(P))$ to be optimal is $\tau_{th}(P) = \tau_{max}(\gamma^{NE})$. Otherwise, the function is concave decreasing in τ and $(P, \tau_{th}(P))$ cannot be optimal for player L.

C. Proof of Theorem 3

Let us first find the best-response of the jammer defined in (17). Given the second remark, it is easy to see that:

$$\gamma^{BR}(p, \tau) = \begin{cases} 0, \text{ if } p < p_{th}(\tau) \\ \in [0, \Gamma], \text{ if } p = p_{th}(\tau) \\ \Gamma, \text{ if } p > p_{th}(\tau) \end{cases}, \quad (30)$$

where $p_{th}(\tau) = \frac{2\zeta\tau}{1-\tau}$. Notice that whenever $p = p_{th}(\tau)$ the best response of the jammer can be anything and cannot in fact be predicted by player L. However, the obtained payoff is anticipated by player L as it does not depend on the actual choice of the jammer: $\tilde{u}(p_{th}(\tau), \tau, \gamma) = \tilde{u}(p_{th}(\tau), \tau, 0)$, for all γ.

The SE action of the leader, anticipating that the jammer will best respond to their own choice is given by:

$$(p^{SE}, \tau^{SE}) = \arg\max_{p,\tau} \tilde{u}(p, \tau, \gamma^{BR}(p, \tau)) \quad (31)$$

From (30), we see that player L can either neutralize the jammer or allow it to transmit, knowing that the jammer will transmit with full power Γ. The situation that proves to be mostly advantageous to the legitimate player will be chosen.

- *Case A:* Assume the legitimate player neutralizes the jammer by choosing a strategy such that $p \leq p_{th}(\tau)$. Player L has to find the best pair (p, τ) that maximizes $\tilde{u}(p, \tau, 0)$ knowing that $p \in [0, \min\{P, p_{th}(\tau)\}]$ and that $\tau \in [0, 1]$; the solution equals (p^{NJ}, γ^{NJ}) in Proposition 1.

- *Case B:* Assume now that the legitimate player does not neutralize the jammer and $p \geq p_{th}(\tau)$. Player L has to find the best pair (p, τ) that maximizes $\tilde{u}(p, \tau, \Gamma)$ knowing that $p \in [0, P] \cap [p_{th}(\tau), \infty)$ and $\tau \in (0, 1)$. By fixing τ first and optimizing with respect to p, we have that $u(p, \tau, \Gamma)$ is increasing in p and hence, the optimal power equals P and the value of τ will be constrained by $P \geq p_{th}(\tau)$ or equivalently $\tau \leq \tau_{th}(P)$. This analysis is identical to the analysis of the NE and one possible SE solution is the NE in Theorem 1.

At the SE, the legitimate user will choose one of the two possibilities which provides a higher SKG utility. From Proposition 2, we know that the NJ state cannot provide a strictly higher utility than the NE state. Hence, whenever $\tau^{NE} < \tau_{th}(P)$, the utility of the unique NE is strictly higher than that of the NJ state. This implies a unique SE that is identical to the NE. If $\tau^{NE} = \tau_{th}(P)$, this means that $(p^{NJ}, \tau^{NJ}) = (P, \tau^{NE})$ which implies that the utilities at both states NJ and NE are identical. Both the NE (in Theorem 1) and NJ (in Proposition 1) states are SE solutions: $(P, \tau_{th}(P), \Gamma)$ and $(P, \tau_{th}(P), 0)$.

The remaining question is whether there exist other solutions when player L chooses the strategy $(p^{SE}, \tau^{SE}) = (P, \tau_{th}(P))$. In this case, the jammer is rendered indifferent between all of its actions $\gamma \in [0, \Gamma]$, which means that it is also rendered unpredictable. As opposed to the NE, the SE requires the legitimate user to be able to anticipate precisely the jammer's response. To avoid this problem, the leader can silence the jammer by transmitting with power $p = P - \varepsilon$ or ensures that the jammer transmits with full power by transmitting at power $p = P + \varepsilon$, where ε could be made arbitrarily small and, hence, has no practical impact. None of the other NE in Theorem 2 can be SEs, since the jammer's response cannot be predictable.

In conclusion, if $\tau^{NE} < \tau_{th}(P)$, then the SE is unique and identical to the NE in Theorem 2. Otherwise, both the NE and the NJ states are SE solutions.

D. Proof of Proposition 3

Assume by absurdum and WLOG that player J has an NE strategy such that the first channel is left unused $\beta^* = (0, \beta_2, \ldots, \beta_{N+1})$ while other channels are used $\beta_i > 0$ for some $2 \leq i \leq N$. Exploiting this knowledge, player L will only employ channel hopping on channel 1 and maybe spreading with non zero probability at the NE. To see this, we write the expected payoff of player L assuming $\beta_1 = 0$

$$\begin{aligned} 2N\hat{u}(\alpha^*, \beta^*) = &\sum_{i=2}^{N} \{\alpha_i(1 - \beta_i - \beta_{N+1})C(NP, 0) \\ &+\alpha_i\beta_i C(NP, N\Gamma) + \alpha_i\beta_{N+1}C(NP, \Gamma)\} \\ &+\alpha_{N+1}(1 - \beta_{N+1})[(N-1)C(P, 0) + C(P, N\Gamma)] \\ &+\alpha_{N+1}\beta_{N+1}NC(P, \Gamma)\alpha_1(1 - \beta_{N+1})(N-1)C(NP, 0). \end{aligned}$$

Since $C(NP, 0) > C(NP, N\Gamma)$ and there exists some $\beta_i > 0$, we have that:

$$\begin{aligned} &(1 - \beta_{N+1})(N-1)C(NP, 0) > \textstyle\sum_{i\neq 1}[\beta_i C(NP, N\Gamma) \\ &+(1 - \beta_i - \beta_{N+1})C(NP, 0)]. \end{aligned}$$

This means that, if the jammer does not use channel 1, the legitimate ndes will only employ this channel and none of the other channel hopping strategies and the NE will be of the form $\alpha^* = (1 - \alpha_{N+1}, 0, \ldots, 0, \alpha_{N+1})$. The utility becomes:

$$\begin{aligned} &2N\hat{u}(\alpha^*, \beta^*) = (1 - \alpha_{N+1})(1 - \beta_{N+1})(N-1)C(NP, 0) \\ &+\alpha_{N+1}(1 - \beta_{N+1})[(N-1)C(P, 0) + C(P, N\Gamma)] \\ &+\alpha_{N+1}\beta_{N+1}NC(P, \Gamma). \end{aligned}$$

But now, if the jammer uses all channel hopping probabilities back in channel 1, he can strictly decrease the utility. Assume that the jammer switches from the initial β^* to $\delta = (1 - \beta_{N+1}, 0, \ldots, 0, \beta_{N+1})$. The payoff becomes:

$$\begin{aligned} &2N\hat{u}(\alpha^*, \delta) = (1 - \alpha_{N+1})(1 - \beta_{N+1})(N-1)C(NP, N\Gamma) \\ &+\alpha_{N+1}(1 - \beta_{N+1})[(N-1)C(P, 0) + C(P, N\Gamma)] \\ &+\alpha_{N+1}\beta_{N+1}NC(P, \Gamma). \end{aligned}$$

Since $\hat{u}(\alpha^*, \beta^*) > \hat{u}(\alpha^*, \delta)$, the jammer has an incentive to deviate from the NE which is a contradiction. Thus, the jammer uses either all or none of the channel hopping actions. For player L, the proof follows similarly.

E. Proof of Proposition 4

Let us write the linear equations obtained when the players are indifferent among their channel hopping actions. There are four very similar cases depending on whether the players use spread with zero probability at the NE or not. We only detail one case here below. If both players use spread at the NE, the following conditions must be met:

$$\begin{aligned} &\alpha_i C(NP, N\Gamma) + (1 - \alpha_i - \alpha_{N+1})C(NP, 0) \\ &+\alpha_{N+1}[(N-1)C(P, 0) + C(P, N\Gamma)] = c_\alpha, \\ &\beta_i C(NP, N\Gamma) + (1 - \beta_i - \beta_{N+1})C(NP, 0) \\ &+\beta_{N+1}C(NP, \Gamma) = c_\beta. \end{aligned}$$

The equations in α illustrate that player J becomes indifferent among their pure channel hopping actions at the NE. Similarly, the equations in β make player L indifferent among their pure channel hopping actions at the NE. We remark that all these equations are identical in the sense that their coefficients do not depend on the index i of the α and β variables. This means that their solutions are of the form: $\alpha_i = a$ and $\beta_i = b$ for any $i \leq N$. Therefore – irrespective of whether the players employ or not spreading at the NE – if both players employ the channel hopping strategy, then the NE takes on the special form $\alpha^* = (a, \ldots, a, (1 - Na))$, $\beta^* = (b, \ldots, b, (1 - Nb))$ for some $0 \leq a \leq 1/N$, $0 \leq b \leq 1/N$.

F. Proof of Theorem 4

If $N = 1$, the NE analysis is trivial and both players transmit at full powers $(NP, N\Gamma)$. If $N > 1$ and given the strict convexity of $C(p,\gamma)$ in γ, we have the following inequality for all p, $\gamma_1 \neq \gamma_2$ and $\lambda \in (0,1)$:

$$C(p, \lambda\gamma_1 + (1-\lambda)\gamma_2) \quad < \quad \lambda C(p,\gamma_1) + (1-\lambda)C(p,\gamma_2).$$

By taking $p = P$, $\gamma_1 = 0, \gamma_2 = N\Gamma, \lambda = \frac{N-1}{N}$, we obtain:

$$NC(P,\Gamma) \quad < \quad (N-1)C(P,0) + C(P,N\Gamma) \qquad (32)$$

Similarly, by taking $p = NP$, $\gamma_1 = 0, \gamma_2 = N\Gamma, \lambda = \frac{N-1}{N}$, we obtain:

$$NC(NP,\Gamma) < (N-1)C(NP,0) + C(NP,N\Gamma). \qquad (33)$$

From Proposition 3 and Proposition 4, the NE can only take nine forms which are not mutually exclusive. Each case is studied using Definition 1 and for which necessary and sufficient conditions are provided. Then, using (32) and (33), we show that only three of the nine cases can occur. The proof is rather long and tedious and only a sketch containing the main ideas is provided below. 1) *Both players spread at the NE* (i.e., $\alpha^* = \beta^* = e_{N+1}$), iff $C(NP,\Gamma) < NC(P,\Gamma)$ and $(N-1)C(P,0) + C(P,N\Gamma) > NC(P,\Gamma)$. The second condition is always true due to (32).

2) *Both players use only channel hopping at the NE* (i.e., $\alpha^* = \beta^* = (1/N,\dots,1/N,0)$), iff $C(NP,N\Gamma) + (N-1)C(NP,0) > N(N-1)C(P,0) + NC(P,N\Gamma)$ and $C(NP,N\Gamma) + (N-1)C(NP,0) < NC(NP,\Gamma)$. This case is impossible because of (33).

3) *The game has a strictly mixed NE,* i.e., all actions are used with non-zero probability, of the form $\alpha^* = (a,\dots,a,(1-Na))$, $\beta^* = (b,\dots,b,(1-Nb))$ iff there exist $0 < a < 1/N$ and $0 < b < 1/N$ such that both players are indifferent among all their pure strategies. Let us write the condition for $(a,\dots,a,1-Na)$ to be a NE and for which the jammer is indifferent among their pure strategies by Definition 1. This yields the following linear equation:

$$\begin{aligned} &a[NC(NP,\Gamma) - C(NP,N\Gamma) - (N-1)C(NP,0)] = \\ &(1-Na)[(N-1)C(P,0) + C(P,N\Gamma) - NC(P,\Gamma)], \end{aligned}$$

where the term on the LHS is a strictly negative value from $a > 0$ and (33) and the RHS is a strictly positive value from $a < 1/N$ and (32). Thus, this case can never occur.

4) *Player L only channel hops and player J uses both channel hopping and spreading at the NE*: $\alpha^* = (1/N,\dots,1/N,0)$ and $\beta^* = (b,\dots,b,(1-Nb))$, iff $C(NP,N\Gamma) + (N-1)C(NP,0) = NC(NP,\Gamma)$, $0 < b < 1/N$, and $Nb[(N-1)C(P,0) + C(P,N\Gamma)] + (1-Nb)NC(P,\Gamma) < bC(NP,N\Gamma) + (N-1)bC(NP,0) + (1-Nb)C(NP,\Gamma)$, where b is chosen such that player L is indifferent among their pure strategies. Given (33), the above equality never holds.

5) *Player J only channel hops and player L uses both channel hopping and spreading at the NE* (i.e., $\alpha^* = (a,\dots,a,(1-Na))$ and $\beta^* = (1/N,\dots,1/N,0)$), iff $C(NP,N\Gamma) + (N-1)C(NP,0) = N(N-1)C(P,0) + C(P,N\Gamma)$, $0 < a < 1/N$, and $MaC(NP,\Gamma) + (1-Na)NC(P,\Gamma) > aC(NP,N\Gamma) + (N-1)aC(NP,0) + (1-Na)[(N-1)C(P,0) + C(P,N\Gamma)]$ where a is chosen such that player J is indifferent among their pure strategies. The last inequality condition becomes:

$$\begin{aligned} &a[NC(NP,\Gamma) - C(NP,N\Gamma) - (N-1)C(NP,0)] > \\ &(1-Na)[(N-1)C(P,0) + C(P,N\Gamma) - NC(P,\Gamma)] \end{aligned}$$

where the term on the LHS is a strictly negative value from $a > 0$ and (33) and the RHS is a strictly positive value from $a < 1/N$ and (32). Thus, this case can never occur.

6) *Player L spreads and player J channel hops at the NE* (i.e., $\alpha^* = e_{N+1}$ and $\beta^* = (\beta_1,\dots,\beta_N,0)$), iff $NC(P,\Gamma) > (N-1)C(P,0) + C(P,N\Gamma)$, $NC(NP,0) - N(N-1)C(P,0) - NC(P,N\Gamma) < C(NP,0) - C(NP,N\Gamma)$ and β_i meet some additional constraints. Because of (32) this case never occurs as the first condition is never satisfied.

7) *Player J spreads and player L channel hops at the NE* (i.e., $\beta^* = e_{N+1}$ and $\alpha^* = (\alpha_1,\dots,\alpha_N,0)$), iff $C(NP,\Gamma) > NC(P,\Gamma)$ and $NC(NP,0) - NC(NP,\Gamma) > C(NP,0) - C(NP,N\Gamma)$. The NE strategies of player L are given by the (infinite number) of solutions to the following system of linear inequalities:

$$\begin{cases} 0 \le \alpha_i \le 0, \ \forall i, \\ \displaystyle\sum_{j=1}^{N} \alpha_j = 1 \\ \alpha_i < \frac{C(NP,0) - C(NP,\Gamma)}{C(NP,0) - C(NP,N\Gamma)}, \ \forall i \le N. \end{cases}$$

The second condition is always true (33). From (33), the above system of inequality always has the uniform probability over the channels solution $\alpha^* = (1/N,\dots,1/N,0)$.

8) *Player L spreads and player J employs all their actions at the NE* (i.e., $\alpha^* = e_{N+1}$, $\beta^* = (\beta_1,\dots,\beta_{N+1})$), iff $(N-1)C(P,0) + C(P,N\Gamma) = NC(P,\Gamma)$ and $\beta_i, \forall i$ meet some additional constraints that are not detailed here. The reason is that, given (32), the equality condition never holds and, hence, this case is impossible.

9) *Player J spreads and player L employs all their actions at the NE* (i.e., $\beta^* = e_{N+1}$ and $\alpha^* = (\alpha_1,\dots,\alpha_N,\alpha_{N+1})$), iff $C(NP,\Gamma) = NC(P,\Gamma)$ and the solutions to the following linear system of inequalities are NE strategies for player L:

$$\begin{cases} 0 \le \alpha_i \le 1, \ \forall i, \\ \displaystyle\sum_{j=1}^{N} \alpha_j = 1 \\ \alpha_i[C(NP,N\Gamma) - C(NP,0)] + \alpha_{N+1}[(N-1)C(P,0) \\ +C(P,N\Gamma) - C(NP,0) + C(NP,\Gamma) - NC(P,\Gamma)] \\ > C(NP,\Gamma) - C(NP,0), \ \forall i \le N. \end{cases}$$

Notice that, by taking $\alpha_{N+1} = 0$, the above system of linear equations is precisely the one in case 7 which has an infinite number of solutions, and in particular $\alpha_i = 1/N, \ \forall i \le N$. Similarly, $\alpha_i = 0$ for all $i \le N$ and $\alpha_{N+1} = 1$ (player L spreads) is also a solution, which follows directly from (32).

G. Proof of Proposition 5

The best-response for the jammer is defined as $\beta^{BR}(\alpha) = \arg\min_{\beta} \hat{u}(\alpha,\beta)$, where $\beta^{BR}(\alpha)$ represents the best action the jammer can take knowing that the legitimate player choses

α. The payoff is affine in β and can be rewritten it as $\hat{u}(\alpha,\beta)=\sum_{i=1}^{N+1}\beta_i c_i(\alpha)+c_0(\alpha)$, with the coefficients:

$$\begin{aligned} c_i(\alpha) &= \alpha_i[C(NP,N\Gamma)-C(NP,0)] \\ &+ \alpha_{N+1}[C(P,N\Gamma)-C(P,0)], i\leq N, \\ c_{N+1}(\alpha) &= \sum_{j=1}^{N}\alpha_i[C(NP,\Gamma)-C(NP,0)] \\ &+ N\alpha_{N+1}[C(P,\Gamma)-C(P,0)], \\ c_0(\alpha) &= \sum_{j=1}^{N}\alpha_i C(NP,0)+N\alpha_{N+1}C(P,0). \end{aligned} \tag{34}$$

Thus, we observe that to find the best-response function $\beta^{BR}(\alpha)$, the jammer has to solve a linear program under the constraints: $\beta_i\geq 0,\ \forall\ i$ and $\sum_{j=1}^{N+1}\beta_j=1$. The SE action of the leader, anticipating that the jammer will best respond to their own choice is given by:

$$\alpha^{SE}=\arg\max_{\alpha}\hat{u}(\alpha,\beta^{BR}(\alpha))=\arg\max_{\alpha}\left\{\min_{j>0}c_j(\alpha)+c_0(\alpha)\right\}.$$

Player L can anticipate the response of the jammer, who seeks to minimize the coefficients $c_j(\alpha)$. We remark that: $c_{N+1}(\alpha)=(1-\alpha_{N+1})[C(NP,\Gamma)-C(NP,0)]+N\alpha_{N+1}[C(P,\Gamma)-C(P,0)]$ and $c_0(\alpha)=(1-\alpha_{N+1})C(NP,0)+N\alpha_{N+1}$ do not depend on the way in which the load $1-\alpha_{N+1}$ is spread over the channel hopping actions. Therefore we can only focus on $c_i(\alpha),\ 1\leq i\leq N$.

If player L uses channel hopping strategies with uniform probability $\alpha^{(1)}=(a,\dots,a,1-Na)$, all coefficients will be equal $c_i(\alpha^{(1)})=a[C(NP,N\Gamma)-C(NP,0)]+(1-Na)[C(P,N\Gamma)-C(P,0)]$. This means that the jammer is indifferent between the different channels $\min_{1\leq j\leq N}c_j(\alpha)=a[C(NP,N\Gamma)-C(NP,0)]+(1-Na)[C(P,N\Gamma)-C(P,0)]$.

Now, if player L has a preference for a certain channel, say for channel 1: $\alpha^{(2)}=(a+\delta_1,a-\delta_2,\dots,a-\delta_N,1-Na)$, with $\sum_{j=2}^{N}\delta_j=\delta_1>0$, the coefficients will be: $c_1(\alpha^{(2)})=(a+\delta)[C(NP,N\Gamma)-C(NP,0)]+(1-Na)[C(P,N\Gamma)-C(P,0)]$, $c_i(\alpha^{(2)})=(a-\delta_i)[C(NP,N\Gamma)-C(NP,0)]+(1-Na)[C(P,N\Gamma)-C(P,0)]$. In this case, the jammer will profit from this information and will put all their channel hopping load on channel 1 alone: $\beta_1^{BR}(\alpha^{(2)})=1-\beta_{N+1}^{BR}(\alpha^{(2)})$, $\beta_i(\alpha^{(2)})=0,\forall 2\leq N$ and $\min_{1\leq j\leq N}c_j(\alpha^{(2)})=(a+\delta)[C(NP,N\Gamma)-C(NP,0)]+(1-Na)[C(P,N\Gamma)-C(P,0)]$. But this means that $\min_{1\leq j\leq N}c_j(\alpha^{(2)})<\min_{1\leq j\leq N}c_j(\alpha^{(1)})$, which further implies that $\hat{u}(\alpha^{(1)},\beta^{BR}(\alpha^{(1)}))<\hat{u}(\alpha^{(2)},\beta^{BR}(\alpha^{(2)}))$. This means that player L will lose in utility by not assigning uniform probability to the channel hopping strategies.

H. Proof of Theorem 5

Proposition 1 tells us that the SE strategy of player L is of the form: $\alpha^{SE}=(a,\dots,a,(1-Na))$ for some $a\in[0,1/N]$, which is to be determined. The coefficients in (34) become:

$$\begin{aligned} c_i(\alpha^{SE}) &= a[C(NP,N\Gamma)-C(NP,0)] \\ &+ (1-Na)[C(P,N\Gamma)-C(P,0)], i\leq N \\ c_{N+1}(\alpha^{SE}) &= Na[C(NP,\Gamma)-C(NP,0)] \\ &+ N(1-Na)[C(P,\Gamma)-C(P,0)]. \end{aligned}$$

Using the fact that $C(p,\gamma)$ is convex w.r.t. γ for a fixed p, we have the following inequalities: $NC(P,\Gamma)<(N-1)C(P,0)+C(P,N\Gamma)$ and $NC(NP,\Gamma)<(N-1)C(NP,0)+C(NP,N\Gamma)$ which imply that $c_i(\alpha^{SE})<c_{N+1}(\alpha^{SE})$. This means that the jammer's strategy is to spread always: $\beta^{SE}=(0,\dots,0,1)$. The SE utility becomes:

$$\hat{u}(\alpha^{SE},\beta^{SE})=aC(NP,\Gamma)+(1-Na)C(P,\Gamma). \tag{35}$$

This implies that, if $C(NP,\Gamma)>NC(P,\Gamma)$ player L will only channel hop with uniform probability $a=1/N$. If $C(NP,\Gamma)<NC(P,\Gamma)$ player L will only spread $a=0$. If $C(NP,\Gamma)=NC(P,\Gamma)$ then the legitimate user is indifferent between spreading and channel hopping and all $a\in[0,1/N]$ are solutions.

References

[1] E. Belmega and A. Chorti, "Energy harvesting in secret key generation systems under jamming attacks," in *Proc. IEEE Int. Conf. Commun. (ICC), to appear*, May 2017.

[2] A. Chorti and E. Belmega, "Secret key generation in Rayleigh block fading AWGN channels under jamming attacks," in *Proc. IEEE Int. Conf. Commun. (ICC), to appear*, May 2017.

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography – part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 7, pp. 1121–1132, Jul. 1993.

[4] U. Maurer, "Secret key agreement by public discussion based on common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 733–742, May 1993.

[5] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography – part II: CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[6] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 1995.

[7] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. Int. Symp. Inform. Theory (ISIT)*, Seatle, US, Jul. 2006, pp. 2593–2597.

[8] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–154, Jun. 2010.

[9] T.-H. Chou, S. Draper, and A. M. Sayeed, "Key generation using external source excitation: Capacity, reliability and secrecy exponent," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2455–2474, Apr. 2012.

[10] W. Yunchuan, Z. Kai, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, Sep. 2013.

[11] A. Mukherjee, S.A.A., Fakoorian, H. Jing, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys and Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[12] O. Gungor, F. Chen, and C. Koksal, "Secret key generation via localization and mobility," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2214–2230, Jun. 2015.

[13] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part III: privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[14] V. Yakovlev, V. Korzhik, and G. Morales-Luna, "Key distribution protocols based on noisy channels in presence of an acive adversary: conventional and new versions with parameter optimization," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2535–2549, Jun. 2008.

[15] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a cryptographic key from an un-authenticated wireless channel," in *Proc. 14th ACM Annual Int. Conf. Mobile Comput. Netw.*, 2008.

[16] C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness," in *IEEE Conf. Commun. Netw. Security (CNS)*, 2015, pp. 113 – 118.

[17] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, Oct. 2012.

[18] R. Molière, F. Delaveau, C. L. K. Ngassa, C. Lemenager, T. Mazloum, and A. Sibille, “Tag signals for early authentication and secret key generation in wireless public networks,” in *Eur. Conf. Netw. Commun. (EuCNC)*, 2015, pp. 108–112.

[19] G. Amariucai, S. Wei, and R. Kannan, “Gaussian jamming in block-fading channels under long term power constraints,” in *Proc. Int. Symp. Inf. Theory (ISIT)*. Nice, France: IEEE, 24-29 Jun. 2007, pp. 1001–1005.

[20] X. Song, P. Willett, S. Zhou, and P. Luh, “The MIMO radar and jammer games,” *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 687–699, Feb. 2012.

[21] S. Wei, R. Kannan, V. Chakravarthy, and M. Rangaswamy, “CSI usage over parallel fading channels under jamming attacks: a game theory study,” *IEEE Trans. Wireless Commun.*, vol. 60, no. 4, pp. 1167–1175, Apr. 2012.

[22] R. El-Bardan, S. Brahma, and P. Varshney, “Strategic power allocation with incomplete information in the presence of a jammer,” *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3467–3479, 2016.

[23] ——, “Learning-based power allocation in cognitive radio networks with a jammer,” in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Montreal, Canada, Dec. 2016.

[24] L. Xiao, T. Chen, L. Jinliang, and D. Huaiyu, “Anti-jamming transmission Stackelberg game with observation errors,” *IEEE Commun. Lett.*, vol. 19, no. 6, pp. 949–952, 2015.

[25] J. Guo, N. Zhao, R. Yu, X. Liu, and V. Leung, “Exploiting adversarial jamming signals for energy harvesting in interference networks,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1267 – 1280, Feb. 2017.

[26] H. Fang, L. Xu, and K. Choo, “Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks,” *Applied Mathematics and Computation*, vol. 296, pp. 153–167, 2017.

[27] A. Mukherjee and A. Swindlehurst, “Jamming games in the MIMO wiretap channel with an active eavesdropper,” *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[28] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[29] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. Electronic Ed.: McGraw Hill, Inc., 2002.

[30] R. Poisel, *Modern Communications Jamming Priniples and Techniques*. Artech House Publishers, 2003.

[31] M. Strasser, C. Pöpper, S. Căpkun, and M. Čagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” in *Proc. 2008 IEEE Symp. Security Privacy*, 2008.

[32] C. Pöpper, M. Strasser, and S. Căpkun, “Anti-jamming broadcast communication using uncoordinated spread spectrum techniques,” *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 703–715, Jun. 2010.

[33] R. Ramachandran, V. Sharma, and P. Viswanath, “Capacity of Gaussian channels with energy harvesting and processing cost,” *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2563–2575, May 2014.

[34] Y. Gu and S. Aïssa, “RF-based energy harvesting in decode-and-forward relaying systems: Ergodic and outage capacities,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6425–5434, Nov. 2015.

[35] S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, and K. Huang, “Energy harvesting wireless communications: A review of recent advances,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 3, pp. 360–381, Mar. 2015.

[36] R. Zhang and C. K. Ho, “MIMO broadcasting for silmutaneous wireless information and power transfer,” vol. 12, no. 5, pp. 1989–2001, May 2013.

[37] D. Fudenberg and J. Tirole, *Game theory*. MIT press, 1991.

[38] A. Goldsmith, *Wireless Communications*. Cambridge University Press, NY, 2005.

[39] J. V. Neumann and O. Morgenstern, *Theory of games and economic behavior*. Princeton University Press, 2007.

[40] J. Xu, L. Duan, and R. Zhang, “Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels,” *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 80–83, 2016.