Secret Key Generation in Rayleigh Block Fading AWGN Channels under Jamming Attacks

Arsenia Chorti, Elena Veronica Belmega

Secret Key Generation in Rayleigh Block Fading AWGN Channels under Jamming Attacks

Arsenia Chorti
School of Computer Science and Electronic Engineering
University of Essex, Wivenhoe Park, UK
Email: achorti@essex.ac.uk

E. Veronica Belmega
ETIS / ENSEA Université de Cergy-Pontoise - CNRS
Cergy-Pontoise and Inria, Grenoble, France
Email: belmega@ensea.fr

***Abstract*—Jamming attacks have been shown to disrupt secret key generation (SKG) in systems that exploit the reciprocity of the wireless medium to generate symmetric keys at two remote locations through public discussion. In this study, the use of frequency hopping/spreading in Rayleigh block fading additive white Gaussian noise (BF-AWGN) channels is investigated as a means to counteract such attacks. The competitive interaction between a pair of legitimate users and a jammer is formulated as a zero-sum game and the corresponding Nash equilibria (NE) are characterized analytically and in closed form. It is found that the jammer's optimal strategy is to spread its power across the entire spectrum. On the contrary, the pair of legitimate users should use frequency spreading only in favorable transmission conditions, and frequency hopping otherwise (e.g., low signal to jamming power ratio). Numerical results show that frequency hopping/spreading in BF-AWGN channels is an effective technique for combating jamming attacks in SKG systems; a modest increase of the system bandwidth can substantially increase the SKG rates.**

***Index Terms*—Secret key generation, jamming, zero-sum games, Nash equilibrium, frequency hopping/spreading**

I. Introduction

Direct sequence spread spectrum (DSSS) and spread spectrum frequency hopping (SSFH) are the principal counter-jamming approaches typically used in wireless systems [1]. In essence, these systems require a pre-shared secret to establish the spreading sequence or the hopping pattern between two legitimate nodes; as such, they are not directly applicable to secret key generation (SKG) systems that on the contrary *seek to establish* a secret key [2]–[5]. Attempting to resolve this contradiction and reconcile DSSS and SSFH with SKG, uncoordinated frequency hopping/spreading techniques have recently been investigated in [6], [7]. The main idea behind the proposed approaches was the randomization of the selection of the hopping/spreading sequences.

Such techniques typically employ long pseudo-random sequences and consequently often require a considerable expansion of the system bandwidth. On the other hand, fourth (4G) and fifth generation (5G) systems have strict bandwidth specifications; it is therefore timely to investigate alternative counter-jamming approaches for systems with limited spectral resources. Furthermore, their compatibility with orthogonal frequency division multiplexing (OFDM) modulation systems used in 4G would also be desirable. Motivated by the above, in the present work we extend the studies in [8], [9] to SKG systems and investigate frequency hopping/spreading counter-jamming policies in Rayleigh block fading additive white Gaussian noise (BF-AWGN) channels.

This research was supported in part by ENSEA, Cergy-Pontoise, France.

The strategic interaction between a pair of SKG nodes and a malicious jammer is modeled as a zero-sum non-cooperative game in which the SKG capacity serves as the utility function. By construction, this game has at least one Nash equilibrium (NE); the set of all pure and mixed NE are characterized in closed form. We show that optimally the jammer spreads its power. On the other hand, if the transmission conditions are poor (e.g., low transmit power or high jamming power), then the legitimate users should use frequency hopping, while when the transmission conditions are favorable they should use frequency spreading. Employing the NE as opposed to a fixed strategy can result in high gains in terms of SKG rates for the legitimate nodes. As an example, our numerical results demonstrate that more than 80% in relative utility can be gained at the NE compared to a fixed frequency hopping strategy. Importantly, it is shown that a mere doubling of the spectral resources allows for a substantial increase in SKG rates (relative gain $> 40\%$), while this gain rises considerably when quadrupling the system bandwidth (relative utility gain $> 60\%$). Thus, efficient counter-jamming approaches for SKG systems can be built even when spectral resources are limited.

The paper is organized as follows. In Section II the SKG system model is introduced. In Section III the zero-sum game is formulated and the NE are completely characterized in closed form. Numerical illustrations and a detailed discussion of the possible counter-jamming strategies are presented in Section IV, while the conclusions of this work are included in Section V.

II. System Model

SKG processes have been extensively studied and are considered a mature topic of physical layer security. They typically consists of three phases: a *shared randomness distillation* phase, in which the legitimate nodes – commonly referred to as Alice and Bob – observe dependent random variables denoted in the following by Y_A, Y_B while an eavesdropper, referred to as Eve observes Y_E. In the next two phases, known as *information reconciliation* and *privacy amplification*,

side information is exchanged between Alice and Bob and a common secret key is established with the aid of Slepian Wolf decoders. An upper bound on the SKG rate is given by $\min\left[I(Y_A;Y_B), I(Y_A;Y_B|Y_E)\right]$ [2], [3].

A commonly used source of shared randomness is provided by the fading coefficients in slowly varying rich multipath environments [4], [5], exploiting channel reciprocity during the channel coherence time. Particularly in Rayleigh and Rician fading channels, the decorrelation properties of the fading coefficients over short distances (of the order of a wavelength) can be exploited to ensure that Eve's observation Y_E is uncorrelated from Y_A and Y_B [4], [5]; in this case, the above upper bound becomes tight and the maximum SKG rate, referred to as the SKG capacity, is simply given by $C = I(Y_A;Y_B)$ (Sec. II [2]). In the following, we assume that the decorrelation property of the observations holds.

In this context in [5], Alice and Bob were assumed to exchange unit probe signals over a slow fading Rayleigh channel during its coherence time and obtain respective observations Y_A and Y_B expressed as:

$$Y_A = H + Z_A, \tag{1}$$

$$Y_B = H + Z_B, \tag{2}$$

where H denoted the fading coefficient, modeled as a zero mean Gaussian random variable with variance σ_H^2, $H \sim \mathcal{N}(0,\sigma_H^2)$, and, Z_A and Z_B modeled the effect of AWGN and denoted independent zero mean Gaussian random variables with variances N_A and N_B respectively, $(Z_A, Z_B) \sim \mathcal{N}(\mathbf{0}, \mathrm{diag}\,(N_A, N_B))$. Using this notation, the SKG capacity has been expressed as [5]:

$$C = I(Y_A;Y_B) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2}{N_A + N_B + \frac{N_A N_B}{\sigma_H^2}}\right). \tag{3}$$

However, SKG systems have been shown to be vulnerable to jamming attacks [10]. In this work, we study a generalization of the system model in [5] when N parallel subchannels are available for transmission in the presence of a malicious jammer. Alice's and Bob's observations on the i-th subchannel – denoted by $Y_{A,i}$ and $Y_{B,i}$ respectively – are expressed as

$$Y_{A,i} = \sqrt{p_i}H_i + \sqrt{\gamma_i}G_{A,i} + Z_{A,i}, \tag{4}$$

$$Y_{B,i} = \sqrt{p_i}H_i + \sqrt{\gamma_i}G_{B,i} + Z_{B,i}, \tag{5}$$

where the following notation is employed: on the i-th subchannel, the fading coefficient in the link between Alice and Bob 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 $G_{B,i}$ and the links are reciprocal. The fading coefficients are modeled as independent Gaussian random variables with $H_i \sim \mathcal{N}\left(0,\sigma_H^2\right)$, $G_{A,i} \sim \mathcal{N}\left(0,\sigma_A^2\right)$, $G_{B,i} \sim \mathcal{N}\left(0,\sigma_B^2\right)$, for all i. The noise terms $Z_{A,i}$ and $Z_{B,i}$ are modeled as Gaussian random variables with zero mean and unit variances. Alice and Bob exchange constant probe signals with power p_i and Eve transmits constant jamming signals with power γ_i on the i-th subchannel such that the following average power constraints are satisfied:

$$\frac{1}{N}\sum_{i=1}^{N} p_i \le P, \;\; \frac{1}{N}\sum_{i=1}^{N}\gamma_i \le \Gamma. \tag{6}$$

Under these assumptions, an easy calculation reveals that the SKG capacity over the i-th subchannel can be expressed as a function of p_i and γ_i as:

$$C(p_i,\gamma_i) = I(Y_{A,i};Y_{B,i})$$

$$= \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2 p_i}{N_{A,i} + N_{B,i} + \frac{N_{A,i}N_{B,i}}{\sigma_H^2 p_i}}\right), \tag{7}$$

$$\text{with} \quad N_{A,i} = 1 + \sigma_A^2\gamma_i, \quad N_{B,i} = 1 + \sigma_B^2\gamma_i. \tag{8}$$

By inspecting it's first-order derivatives, we conclude that $C(p_i,\gamma_i)$ is a strictly increasing function of p_i for any fixed γ_i, and a strictly decreasing function of γ_i for any fixed p_i. Furthermore, it is a strictly convex function with respect to (w.r.t.) γ_i for any fixed $p_i > 0$ as its second derivative w.r.t. γ_i is strictly positive.

In order to evaluate the N-subchannel BF-AWGN SKG capacity, we formalize the frequency hopping and spreading model for the legitimate users and the adversary similarly to [8], [9]. Frequency spreading can be simply implemented as a wideband transmission across N parallel subchannels employing a uniform power allocation policy, i.e., $p_i = P, \forall i \le N$ for the legitimate users and $\gamma_i = \Gamma \; \forall i \le N$ for the jammer. From an implementation point of view, this is equivalent to a standard OFDM transmission. On the other hand, frequency hopping corresponds to transmitting on a single, randomly chosen subchannel with full power so that when the legitimate users employ frequency hopping on subchannel i, then $p_i = NP$ and $p_k = 0$ for $k \ne i$, while when the jammer frequency hops on subchannel i then $\gamma_i = N\Gamma$ and $\gamma_k = 0, k \ne i$. In OFDM systems, this could be efficiently implemented by setting all the inputs of the inverse fast Fourier transform (IFFT) block to zero, except for one (randomly chosen). Importantly, for both frequency spreading or frequency hopping modes, *no coordination* is assumed between transmitting and receiving terminals; all receiving terminals blindly employ wideband detection using standard OFDM receivers, so that the need for a pre-shared frequency hopping or frequency spreading sequence is alleviated.

The hopping versus spreading strategies are randomly chosen as follows: $\alpha_i, \;\forall i \le N$ represents the probability of frequency hopping on subchannel i and α_{N+1} the probability of spreading the available power uniformly over the whole spectrum for the legitimate users. Similarly, we define $\beta_i, \; 1 \le i \le N+1$ 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: $\alpha_j \;\ge\; 0, \;\forall j, \quad \sum_{i=1}^{N+1}\alpha_i = 1, \;\beta_j \;\ge\; 0, \;\forall j,$ and $\sum_{i=1}^{N+1}\beta_i = 1$. These probabilities are assumed publicly known. Given all the above, the SKG capacity over the N parallel subchannels (measured in bits/sec/Hz) is given by:

$$u(\alpha,\beta) = \sum_{i=1}^{N}\{\alpha_i(1-\beta_i-\beta_{N+1})C(NP,0) + \alpha_i\beta_i C(NP,N\Gamma) + \alpha_i\beta_{N+1}C(NP,\Gamma)$$

$$+\alpha_{N+1}\beta_i[(N-1)C(P,0)+C(P,N\Gamma)]\}$$
$$+\alpha_{N+1}\beta_{N+1}NC(P,\Gamma). \quad (9)$$

In (9), the first term corresponds to the case in which the legitimate users hop on subchannel i and the jammer hops on a different subchannel; the second term to the case in which the legitimate users and the jammer both hop on subchannel i; the third term to the case in which the legitimate users hop on subchannel i and the jammer spreads; the fourth term to the case in which the legitimate users spread and the jammer hops on subchannel i. Finally, the last term corresponds to the case in which they both spread their power.

III. Analysis of Nash Equilibria

Here, we investigate the optimality of frequency hopping versus frequency spreading. For simplicity, in the following Alice and Bob will be collectively referred to as player L and Eve as player J. We model the competitive interaction between L and J as the following zero-sum game:

$$\mathcal{G}(P,\Gamma)=\{\mathcal{A}_L,\mathcal{A}_J,u\}, \quad (10)$$

where the payoff u is given in (9). The players' objective is to identify the optimal probability vectors α and β to maximize/minimize, respectively, the payoff u. Their corresponding action sets, denoted by $\mathcal{A}_L$ and $\mathcal{A}_J$ are defined as

$$\mathcal{A}_L = \{\alpha\in[0,1]^{N+1}|\sum_{i=1}^{N+1}\alpha_i=1\}, \quad (11)$$
$$\mathcal{A}_J = \{\beta\in[0,1]^{N+1}|\sum_{i=1}^{N+1}\beta_i=1\}.$$

From the utility expression (9), none of the players can choose their best strategies unilaterally since they depend on the opponent's choice. In such interactive situations, the Nash equilibrium (NE) is a natural solution [11]. Intuitively, a NE is a system state (α,β) that is stable to unilateral deviations. At the NE, none of the players can benefit by deviating knowing that their opponent plays the NE strategy.

To derive the game's NE we begin by studying a finite discrete game, denoted by $\mathcal{G}_d$ with action sets $\mathcal{E}_L\equiv\mathcal{E}_J\triangleq\{e_1,\ldots,e_N,e_{N+1}\}$ where $e_i\in\{0,1\}^{N+1}$ are the canonical vectors containing 1 on the i-th position and 0 otherwise. The i-th action e_i represents frequency hopping on subchannel 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^*) [11, Sec. 1.3.1]. We observe that our game $\mathcal{G}$ represents the mixed strategy extension of $\mathcal{G}_d$, which directly implies that $\mathcal{G}$ has at least one NE.

***Corollary** 1:* [11, Thm. 1.1] *The strategic form game $\mathcal{G}$ has at least one NE.*

To compute the NE, one possibility is to use the Minimax Theorem which allows us to numerically evaluate mixed NE of any two-player zero-sum game via linear programming; albeit, in our game, we show that the NE can be characterized analytically and in closed-form instead. We begin with a definition of the NE that follows directly from Definition 1.2 in [11, Sec.1.2.1]:

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

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

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

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

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

where the sets $\mathcal{N}_L,\mathcal{I}_L\subseteq\{1,\ldots,N+1\}$ denote, respectively, the indices of the pure actions that are never used at the NE and those that are used 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 never used or are used by player J at the NE: $\mathcal{N}_J=\{i|\beta_i^*=0\}$, and $\mathcal{I}_J=\{1,\ldots,N+1\}\setminus\mathcal{N}_J$.

Definition 1 provides a method to compute the NE of the game $\mathcal{G}$ by solving a system of linear equations as long as the faces of the simplex $\mathcal{A}_L\times\mathcal{A}_J$ on which the NE lie are known, i.e., $\mathcal{I}_L$, $\mathcal{I}_J$ need to be known in advance for all NE. An exhaustive search has a prohibitive complexity (the number of faces in the simplex of dimension $2(N+1)$ is of the order of $2^{2(N+1)}$). For general discrete non-cooperative games, the problem of finding its mixed strategy NE remains a difficult problem [12]. Nevertheless, as we will see in the following section, the NE of our game $\mathcal{G}$ have a special structure which allows us to exploit Definition 1 and fully characterize the set of NE in a simple manner.

In the particular case of a single subchannel, $N=1$, the NE is trivial and consists in both players transmitting with maximum power (P,Γ) or equivalently $\alpha^*=\beta^*=1$. Indeed, since the utility function is increasing as a function of the power of player L and decreasing as a function of player's J power, P and Γ are strictly dominant strategies.

Now, let us focus on the more challenging case $N\geq 2$. From Corollary 1, we know that the game $\mathcal{G}$ has at least one NE. Examining the matrix structure of the discrete game $\mathcal{G}_d$ given in Table I, we notice that there is a symmetry between the frequency hopping strategies. In particular, the utility does not depend on the particular index of the chosen subchannel but only on whether both players hop on the same subchannel or not. This symmetry allows us to show that the NE of the game $\mathcal{G}$ have a particular structure specified in the following propositions. The proofs of the propositions are omitted due to space limitations.

***Proposition** 1: 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** 2: If both players employ frequency 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*

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

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

channels and the NE will have the following structure: $\alpha^* = (a, \ldots, a, (1 - Na))$, $\beta^* = (b, \ldots, b, (1 - Nb))$ *for some* $0 \leq a \leq 1/N$, $0 \leq b \leq 1/N$.

Notice that Propositions 1 and 2 shape the special structure of the NE of $\mathcal{G}$. This structure alongside with Definition 1 and the strict convexity of $C(p, \gamma)$ w.r.t. γ, allows us to fully characterize the set of NE in a very simple and explicit manner as a function of the system parameters.

***Theorem** 1: The set of NE of the game $\mathcal{G}$ 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 , i.e., $\alpha^* = \beta^* = e_{N+1}$.*
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 $\beta^* = e_{N+1}$. The NE strategies of player L are given by the (infinite number of) solutions to the following system of linear inequalities:*

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

   In particular, the uniform probability distribution is one of the NE solutions: $\alpha^* = (1/N, \ldots, 1/N, 0)$. All NEs are equivalent in the sense that the utility is identical.
3. *If $C(NP, \Gamma) = NC(P, \Gamma)$, player L employs all its 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:*

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

   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 the sense that the utility is identical.

   Proof: The proof is detailed in Appendix A. ∎

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 $u(\alpha^*, \beta^*) = NC(P, \Gamma)$. On the contrary, if $C(NP, \Gamma) \geq NC(P, \Gamma)$, there are an infinite number of NE which are generally in mixed strategies for player L. All these NEs are equivalent in terms of achieved utility, which equals $u(\alpha^*, \beta^*) = C(NP, \Gamma)$. Since the jammer's NE strategy is always spreading, even though there may be an infinite number of NEs, the outcome of the game can always be predicted exactly based solely on the knowledge of the game's payoffs in Table I. Both players can choose their NE strategies without the need for implementing iterative or learning procedures, which would require some kind of information exchange or signaling among the players.

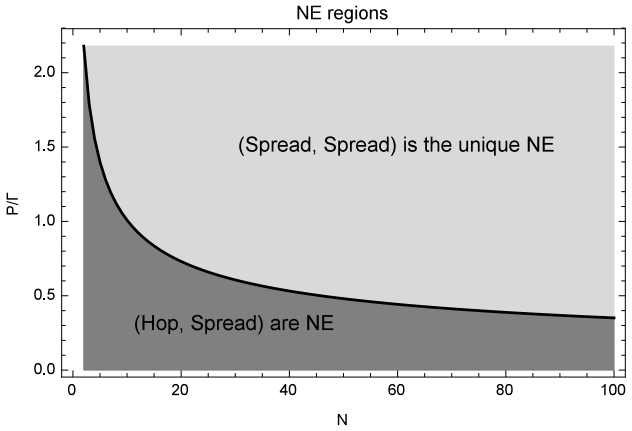

Fig. 1. NE regions as a function of $P/\Gamma \geq 0$ and $N \geq 2$ for $\Gamma = \sigma_A^2 = \sigma_B^2 = \sigma_H^2 = 1$.

Theorem 1 also shows that the optimal strategy of the jammer is always spreading. Intuitively, if the jammer were to use frequency 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 subchannel becomes small with increasing N. On the contrary, for player L the best strategy can be either frequency hopping of frequency spreading depending on the channel conditions, which we will further investigate in the next section.

IV. NUMERICAL ILLUSTRATIONS AND DISCUSSION

The best strategy for the legitimate users at the NE is illustrated in numerical examples of the NE regions as functions of the system parameters. 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 powers, and a region in which the jammer spreads and the legitimate users employ frequency hopping. In our benchmark setting we assume that $\Gamma = \sigma_A^2 = \sigma_B^2 = \sigma_H^2 = 1$. The NE regions as functions of $P/\Gamma \geq 0$ and $N \in \{2, \ldots, 100\}$ are depicted in Fig. 1. Player L hops at the NE below the curve, when the signal to interference ratio (SIR) P/Γ is relatively small. This is intuitive since, in the low transmit power regime, the legitimate users should not split their scarce power across different subchannels but should concentrate it

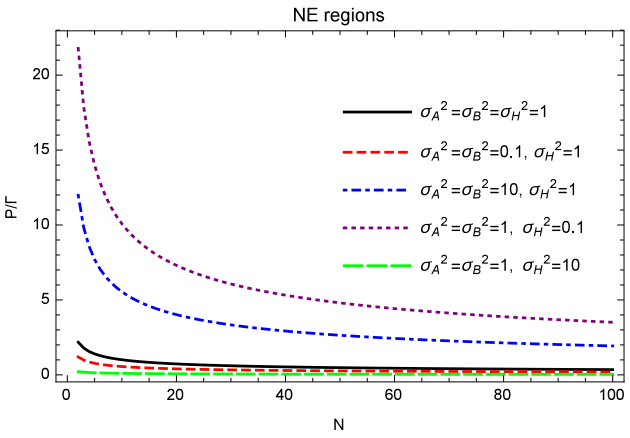

Fig. 2. NE regions as a function of $P/\Gamma \geq 0$ and $N \geq 2$ for different values of σ_A^2, σ_B^2, σ_H^2 and $\Gamma = 1$.

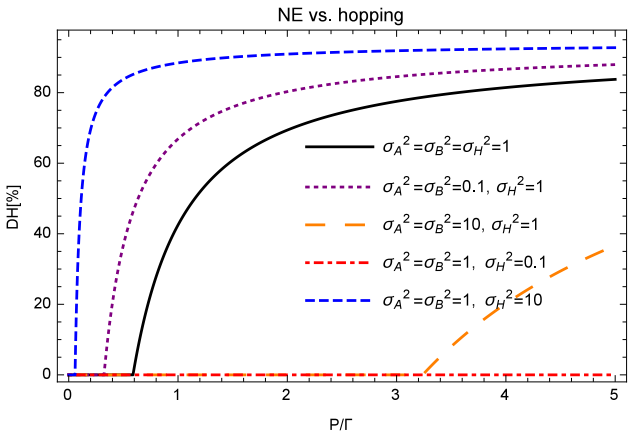

Fig. 3. Relative utility gain between the NE vs. always hopping: $D_H = (u^{NE} - u^{Hop,Spread})/u^{NE}$ as a function of P/Γ for $N = 32$ for different values of $\sigma_H^2, \sigma_A^2, \sigma_B^2$ and $\Gamma = 1$.

all on a single subchannel. Furthermore, in Fig. 2 the curve $C(NP, \Gamma) = NC(P, \Gamma)$ is illustrated for different channel parameters and $N \geq 2$. When σ_H^2 increases, the region in which player L should employ frequency hopping at the NE shrinks down while when σ_A^2, σ_B^2 increase, the region expands.

Fig. 3 illustrates the relative gain obtained by player L when employing the NE strategy as opposed to a fixed hopping strategy for $N = 32$ and different channel parameters. The relative utility gain $D_H = (u^{NE} - u^{Hop,Spread})/u^{NE}$ (where $u^{Hop,Spread} = C(NP, \Gamma)$) is relatively large (up to 85%) in the high SIR regime or in good transmission conditions.

Finally, in Fig. 4, the relative utility gain when using the NE strategy over N subchannels as opposed to a single channel (with $u^{single} = C(NP, N\Gamma)$ for a fair comparison) is investigated as a function of P/Γ for $N \in \{2, 4, 8, 16, 32, 64\}$. We observe that even a modest increase in the spectral resources of the SKG system can lead to a substantial increase in the relative utility. E.g., for $N = 2$ this gain is in the range of 40% while for $N = 4$ it is in the range of 60%. Importantly, the relative gain is even higher at low SIR $P/\Gamma < 1$. This shows that in SKG systems, the impact of malicious jamming can be decisively limited by even a modest increase of the bandwidth resources.

V. Conclusions

In this work, the interaction between a pair of legitimate users and a malicious jammer in SKG systems was investigated. Frequency hopping vs. frequency spreading in Rayleigh BF-AWGN channels was formulated as a zero-sum game for which a complete characterization (in closed-form) of the NE was provided. It was found that the jammer's optimal strategy is always to spread its available power over the entire spectrum while the legitimate users should either spread or hop depending on the transmission conditions. At poor SIR, the legitimate users should concentrate all of their power on a single subchannel, while when the transmission conditions are favorable, they should spread. Importantly, numerical simulations showed that even a modest increase in spectral resources

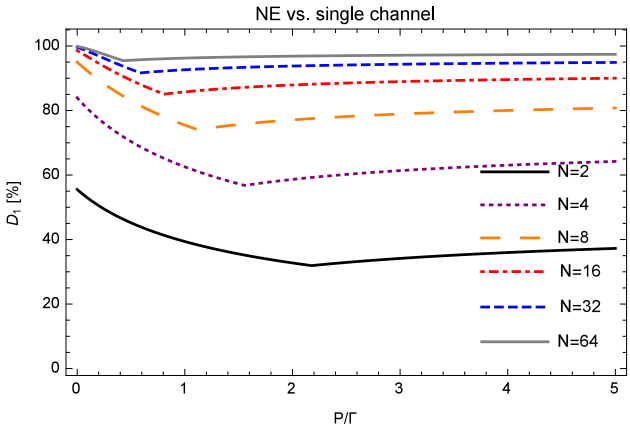

Fig. 4. Relative utility gain between the NE vs. single channel SKG: $D_1 = (u^{NE} - u^{single})/u^{NE}$ as a function of P/Γ for $\Gamma = \sigma_H^2 = \sigma_A^2 = \sigma_B^2 = 1$ and $N \in \{2, 4, 8, 16, 32, 64\}$.

compared to single channel SKG can substantially limit the jammer's impact, particularly at low SIR.

Appendix A
Proof of Theorem 1

Proof: 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:

$$NC(P, \Gamma) \quad < \quad (N-1)C(P, 0) + C(P, N\Gamma). \qquad (12)$$

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

$$NC(NP, \Gamma) < (N-1)C(NP, 0) + C(NP, N\Gamma). \qquad (13)$$

Now, given Proposition 1 and Proposition 2, the NE can only take nine forms which are not all mutually exclusive and which will be detailed below. Each case is studied by using Definition 1 and developing the necessary and sufficient conditions for

each of the nine cases to occur. Then, by using (12) and (13), we show that only three of the nine cases are possible.

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 (12).

2) *Both players use only channel hopping at the NE* (i.e., $\alpha^* = \beta^* = (1/N,\ldots,1/N,0)$), 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 (13).

3) *The game has a strictly mixed NE*, i.e., all actions are used with non-zero probability, of the form $\alpha^* = (a,\ldots,a,(1-Na))$, $\beta^* = (b,\ldots,b,(1-Nb))$ 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 $(a,\ldots,a,1-Na)$ to be a NE and for which the jammer is indifferent among its pure strategies by Definition 1. This yields the following linear equation:

$$a[NC(NP,\Gamma) - C(NP,N\Gamma) - (N-1)C(NP,0)] = (1-Na)[(N-1)C(P,0) + C(P,N\Gamma) - NC(P,\Gamma)],$$

where the term on the LHS is a strictly negative value from $a > 0$ and (13) and the RHS is a strictly positive value from $a < 1/N$ and (12). Thus, this case can never occur.

4) *Player L only channel hops and player J uses both channel hopping and spreading at the NE*: $\alpha^* = (1/N,\ldots,1/N,0)$ and $\beta^* = (b,\ldots,b,(1-Nb))$, 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 its pure strategies. Given (13), 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., $\alpha^* = (a,\ldots,a,(1-Na))$ and $\beta^* = (1/N,\ldots,1/N,0)$), 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 its pure strategies. The last inequality condition can be rewritten as follows:

$$a[NC(NP,\Gamma) - C(NP,N\Gamma) - (N-1)C(NP,0)] > (1-Na)[(N-1)C(P,0) + C(P,N\Gamma) - NC(P,\Gamma)]$$

where the term on the LHS is a strictly negative value from $a > 0$ and (13) and the RHS is a strictly positive value from $a < 1/N$ and (12). 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 $\beta^* = (\beta_1,\ldots,\beta_N,0)$), 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 (12) 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 $\alpha^* = (\alpha_1,\ldots,\alpha_N,0)$), 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:

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

The second condition is always true (13). From (13), the above system of inequality always has the uniform probability over the channels solution $\alpha^* = (1/N,\ldots,1/N,0)$.

8) *Player L spreads and player J employs all its actions at the NE* (i.e., $\alpha^* = e_{N+1}$, $\beta^* = (\beta_1,\ldots,\beta_{N+1})$), 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 (12), the equality condition never holds and, hence, this case is impossible.

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

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

By taking $\alpha_{N+1} = 0$, the above system of linear equations is precisely the one in case 7. ■

REFERENCES

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

[2] 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.

[3] 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.

[4] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] C. Daskalakis, P. Goldberg, and C. Papadimitriou, "The complexity of computing a Nash equilibrium," *SIAM Journal on Computing*, vol. 39, no. 1, pp. 195–259, 2009.