Energy Harvesting in Secret Key Generation Systems under Jamming Attacks

Elena Veronica Belmega, Arsenia Chorti

Energy Harvesting in Secret Key Generation Systems under Jamming Attacks

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

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

***Abstract*—Secret key generation (SKG) from shared randomness at two remote locations has been shown to be vulnerable to denial of service attacks in the form of jamming. Typically, such attacks are alleviated with frequency hopping/spreading techniques that rely on expansion of the system bandwidth. In the present study, energy harvesting (EH) is exploited as a novel counter-jamming approach that alleviates the need for extra bandwidth resources. Assuming the legitimate users have EH capabilities, the idea is that part of the jamming signal can potentially be harvested and converted into useful communication power. In this framework, the competitive interaction between a pair of legitimate users and a jammer is formulated as a zero-sum game. A critical transmission power for the legitimate users is identified which allows to completely characterize the unique NE of the game in closed form. Remarkably, this threshold also provides the option to effectively neutralize the jammer, i.e., prevent the jammer from carrying out the attack altogether. Through numerical evaluations, EH is shown to be a counter-jamming approach that can offer substantial gains in terms of relative SKG rates.**

***Index Terms*—Energy harvesting, secret key generation, jamming attacks, zero-sum games, Nash equilibrium**

I. Introduction

Secret key generation (SKG) from shared randomness at two remote locations has been extensively studied for more than three decades [1]–[4] and is currently being considered for applications such as the internet of things (IoT) [5]. In this direction, practical designs combining SKG with standard message authentication codes for integrity have been shown to be resilient to spoofing, tampering and man-in-the-middle (MiM) active attacks [6]. Nevertheless, SKG techniques are not fully robust against active adversaries. Denial of service attacks in the form of jamming are a known vulnerability of SKG systems; in [7] it was demonstrated that with increasing jamming power, the rate of the generated keys decreases sharply and the SKG process can in essence be brought to a halt.

Typically, counter-jamming measures rely on the availability of spectral resources and employ frequency hopping/spreading strategies [8], [9]. However, 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 [10], [11] is being researched for systems such as wireless sensors and RFID devices for IoT applications. Given the interest in employing SKG in IoT, it is sensible to investigate whether EH could be utilized in such systems as a counter-jamming approach by using the jamming power to enhance the quality of the legitimate transmissions.

Motivated by the above, in the present work we investigate SKG systems under jamming attacks in which the legitimate nodes are equipped wih EH capabilities. We focus on time switching EH protocols [11] in which for a portion of time the legitimate nodes operate in EH mode and switch to the SKG procedure for the rest. A zero-sum game theoretic framework is employed to study the adversarial interaction between the legitimate nodes and the jammer and the game's unique Nash equilibrium (NE) is characterized in closed form. Our analysis reveals the existence of a critical power threshold p_{th} and of an associated optimal harvesting duration for the legitimate users; when the legitimate nodes employ EH for longer than this duration, the attacker's optimal strategy is not to jam at all, hence, it is effectively neutralized. However, this proves a suboptimal strategy; interestingly, at the NE it is found that both parties transmit at full power. Our numerical results demonstrate that the gains in employing EH as a counter-jamming technique are substantial in terms of relative SKG rates. To the best of our knowledge, this work is the first to consider EH as a counter-jamming technique.

The paper is organized as follows. In Section II the SKG model is introduced while in Section III the adversarial interaction between the EH legitimate nodes and the jammer is formulated as a zero-sum game. In III-A, the necessary conditions for neutralizing the jammer are investigated while the complete characterization of the unique NE is presented in III-B. Numerical illustrations and a detailed discussion of the possible counter-jamming strategies are presented in Section IV. Finally, we conclude in Section V.

II. System Model

In the present work we propose a novel approach for alleviating the impact of jamming in SKG systems assuming that the legitimate nodes are equipped with EH capabilities and examine whether this added functionality is useful in preempting jamming attacks. The main motivation behind this study is two-fold. First, the scarcity of the spectral resources renders the investigation of counter-jamming approaches that do not

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

require an increase of the necessary bandwidth very attractive. Secondly, it is interesting to investigate under what conditions harvesting the jamming power could act as a counter-incentive to jamming itself, i.e., characterize the operating region in which the adversary does not benefit from the attack anymore. In this Section, we build the system model in a progressive and intuitive manner. First, we briefly review SKG related basics in II-A. Subsequently, in II-B the baseline system model is extended to incorporate jamming attacks and finally in II-C the complete system model is presented assuming that the legitimate users exploit EH to counteract the jammer's attacks.

A. Background on SKG Processes

Typically, the SKG process consists of three phases. In the first phase, known as *shared randomness distillation*, the legitimate nodes – referred to as Alice and Bob – observe dependent random variables denoted by Y_A, Y_B while an eavesdropper, referred to as Eve observes Y_E. In multi-path wireless channels, a readily available source of shared randomness is provided by the fading channel coefficients [3], [4], [12]. In this work, we focus precisely 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. V is generated with the aid of corresponding encoders f_A, f_B implemented as Slepian-Wolf decoders with side information. At the end of the SKG process, a common key $K \in \mathcal{K}$ is extracted by Alice and Bob so that for any $\epsilon > 0$ the following statements are satisfied [4]:

$$Pr\left(K = f_A\left(Y_A, V\right) = f_B\left(Y_B, V\right)\right) \geq 1-\epsilon, \quad (1)$$

$$I(K;V) \leq \epsilon, \quad (2)$$

$$H(K) \geq \log|\mathcal{K}| - \epsilon. \quad (3)$$

The first statement shows that the SKG process can be made error free, in the asymptotic regime (for long length encoders f_A, f_B). Inequality (2) ensures that the exchange of side information through public discussion does not leak any information regarding K to eavesdroppers, while (3) establishes maximum entropy (uniform distribution) of the generated keys.

Under these conditions, an upper bound on the SKG rate is given by $\min\left[I(Y_A;Y_B), I(Y_A;Y_B|Y_E)\right]$ [1], [2]. In rich multi-path environments, the decorrelation properties of the wireless channel 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]. In such cases, the previous bound becomes tight and the maximum achievable SKG rate, referred to as the SKG capacity, is simply given by

$$C = I(Y_A;Y_B) \quad (4)$$

(see Section II in [1]). Here, we assume that the decorrelation property of the observations holds.

SKG in Rayleigh fading channels has been analyzed extensively; in [4] in particular Alice and Bob were assumed to exchange unit probe signals to excite a Rayleigh fading channel and obtain observations Y_A and Y_B, respectively, as follows

$$Y_A = H + Z_A, \quad (5)$$

$$Y_B = H + Z_B, \quad (6)$$

where H denoted the fading coefficient, modeled as a Gaussian random variable $H \sim \mathcal{N}(0, \sigma_H^2)$, and Z_A and Z_B denoted independent Gaussian noise variables with $(Z_A, Z_B) \sim \mathcal{N}(\mathbf{0}, \mathrm{diag}\,(N_A, N_B))$. Using this notation, the SKG capacity was expressed as [4]

$$C = I(Y_A;Y_B) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2}{N_A + N_B + \frac{N_A N_B}{\sigma_H^2}}\right). \quad (7)$$

B. Jamming Attacks

In the following, we assume that Eve is an active adversary that launches jamming attacks by transmitting constant jamming signals to excite the Rayleigh fading medium in order to impair the SKG process. The extended system model captures the impact of jamming as follows:

$$Y_A = \sqrt{p}H + \sqrt{\gamma}G_A + W_A, \quad (8)$$

$$Y_B = \sqrt{p}H + \sqrt{\gamma}G_B + W_B, \quad (9)$$

where as previously Y_A and Y_B denote Alice's and Bob's observations, respectively. The fading coefficient in the link between Eve and Alice is denoted by $G_A \sim \mathcal{N}\left(0, \sigma^2\right)$ and in the link between Eve and Bob by $G_B \sim \mathcal{N}\left(0, \sigma^2\right)$. For simplicity, the noise terms W_A and W_B are modeled as independent and identically distributed Gaussian random variables with zero mean and unit variance. Finally, in order to incorporate the dimension of power control at the legitimate users and the adversary, the legitimate transmit power is denoted by $p \leq P$ and the jamming power by $\gamma \leq \Gamma$.

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

$$C(p,\gamma) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_H^2 p}{2(1+\sigma^2\gamma) + \frac{(1+\sigma^2\gamma)^2}{\sigma_H^2 p}}\right). \quad (10)$$

We note that $C(p,\gamma)$ is increasing in p for fixed γ and convex decreasing in γ for fixed p. Thus, in absence of EH, the optimal strategy (p^*, γ^*) for the legitimate nodes and the jammer is to transmit at maximum power, i.e., $p^* = P$ and $\gamma^* = \Gamma$.

C. Energy Harvesting to Counteract Jamming

Our aim is to investigate whether EH at the legitimate users can improve the SKG capacity in the presence of jamming. For this, we focus on a simple time-switching scheme [11]: we assume that each transmission symbol of duration T is divided in two parts. In the first part of duration τT ($\tau \in [0,1]$ being the proportion of the time dedicated to EH) both Alice and Bob operate in EH mode with efficiency $\zeta \in (0,1]$. In the second part of duration $(1-\tau)T$, the legitimate users operate in SKG mode using the overall available power (including previously harvested power). Also, we assume that

the harvested energy can be stored in an energy storage unit without any overflowing issues (unlimited storage) [13].

Under the above considerations, the energy harvested by Alice and Bob can be expressed as

$$E = \zeta \sigma^2 \gamma \tau T, \tag{11}$$

so that the harvested power for each legitimate user per communication cycle (to be used in the SKG mode) can be expressed as

$$\frac{E}{(1-\tau)T} = \kappa\gamma, \tag{12}$$

where $\kappa(\tau) \triangleq \frac{\zeta\tau\sigma^2}{1-\tau}$ is a convex increasing function of τ. Since the SKG process encompasses two cycles (from Alice to Bob and from Bob to Alice), each legitimate user harvests $2\kappa\gamma$ overall power before it actually transmits. Thus, the SKG capacity can be expressed as

$$C(p,\tau,\gamma) = \frac{1-\tau}{2}\log_2\left(1 + \frac{(p+2\kappa\gamma)\,\sigma_H^2}{2(1+\sigma^2\gamma) + \frac{(1+\sigma^2\gamma)^2}{(p+2\kappa\gamma)\sigma_H^2}}\right). \tag{13}$$

Inspecting (13), we notice that our model generalizes the SKG setting in II-B. To be specific, if the legitimate users decide not to harvest energy ($\tau = 0$), we obtain (10). In the proposed system model, the legitimate users are able to exploit an additional degree of freedom (i.e., τ) to maximize the SKG capacity. Moreover, by harvesting energy from the wireless environment, the legitimate users can transform part of the jamming power to useful transmission power. As a result, the jammer may not wish to transmit always at its maximum power.

III. Two Players Zero-Sum Game

Non-cooperative game theory captures naturally the competitive interaction between the legitimate users and the jammer. Although the game theoretic framework has already been exploited in physical layer security problems e.g., [14], to the best of our knowledge, this work is the first to investigate EH as an effective means to counteract jamming attacks.

We begin our analysis by discussing two important remarks and their implications regarding the SKG capacity in (13).

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

$$\arg\max_{p\in[0,P]} C(p,\tau,\gamma) = P. \tag{14}$$

Remark 2: For any fixed p and τ, $C(p,\tau,\gamma)$ 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:

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

$$\arg\min_{\gamma\in[0,\Gamma]} C(p,\tau,\gamma) \in [0,\Gamma], \text{ if } p = p_{th}(\tau) \tag{16}$$

$$\arg\min_{\gamma\in[0,\Gamma]} C(p,\tau,\gamma) = \Gamma, \text{ if } p > p_{th}(\tau). \tag{17}$$

Remark 1 shows that the legitimate users should transmit at maximum power P to maximize the SKG utility. On the contrary, Remark 2 shows that the jammer should practically switch in between staying silent and jamming at full power Γ depending on the choice (p,τ) of the legitimate users. This implies that the legitimate users can neutralize the jammer by choosing first (p,τ) such that $p < p_{th}(\tau)$. Intuitively, equation (15) illustrates that, if the legitimate users transmit at a power level below the threshold $p_{th}(\tau)$, the jammer's optimal strategy is to remain silent. Otherwise stated, the harm that the jammer can cause in the SKG mode is overcome by the harvested energy in the EH mode. If the legitimate users transmit at 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.

A. Jammer Neutralization

Given the above discussion and for the sake of simplicity of the analysis, we assume that the choices of the jammer are limited to its extremes $\gamma \in \{0,\Gamma\}$ instead of $[0,\Gamma]$ in the remainder of this work. Denoting by $p_{th}^{-1}(P) \triangleq \frac{P}{P+2\zeta}$ the inverse function of $p_{th}(\tau)$ defined in Remark 2, the necessary conditions for the jammer neutralization are formalized in Proposition 1.

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

$$p^{NJ} = \min\{P, p_{th}(\hat{\tau})\} \text{ and } \tau^{NJ} = \min\{p_{th}^{-1}(P), \hat{\tau}\}, \tag{18}$$

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

For the detailed proof the reader is referred to Appendix A.

Whenever the legitimate user chooses (p^{NJ},τ^{NJ}), the legitimate user transmits at the threshold identified in Remark 2. We can argue that the jammer is neutralized as it has no interest in actively jamming the transmission. To formally guarantee that the jammer stays silent the legitimate users should harvest energy a fraction of time equal to τ^{NJ} and transmit at power $p = p^{NJ} - \varepsilon_p < p^{NJ}$ (strictly below the threshold in Remark 2) for some $\varepsilon_p > 0$ which can be chosen arbitrarily small (so that it has negligible impact on the SKG capacity). Notice that if the jammer stays silent, i.e., $\gamma = 0$, there is no actual energy that is harvested during the EH mode of duration τ^{NJ}. Rather, the legitimate users' choice to harvest energy for a duration of τ^{NJ} acts as a threat to ensure that the jammer has no interest in jamming the transmission. This means that neutralizing the jammer may not be necessarily the overall optimal strategy for the legitimate users. Another hint for this is that whenever $\tau^{NJ} = \hat{\tau} < p_{th}^{-1}(P)$, the transmit power is $p^{NJ} = p_{th}(\hat{\tau}) < P$, which we know from Remark 1 is not optimal.

B. Game Formulation and Nash Equilibrium

To formalize the interaction between the legitimate users and the jammer, we define the following two-player zero-sum

game $\mathcal{G} = \{\mathcal{A}_L, \mathcal{A}_J, C(p,\tau,\gamma)\}$. The players of the game are: player L representing the legitimate users (that collaborate and act as a single player) on one hand, and player J, the jammer, on the other hand. Any of player's L actions (p,τ) belong to the set $\mathcal{A}_L = [0,P]\times[0,1]$ and player's J actions γ belong to the set $\mathcal{A}_J = \{0,\Gamma\}$. The objective of player L is to maximize the SKG capacity $C(p,\tau,\gamma)$ given in (13), whereas player J aims at minimizing it.

The optimal strategy of one player depends on the choice of its opponent and cannot be determined unilaterally. In such interactive situations, the Nash equilibrium (NE) [15] is the natural solution. Intuitively, a profile $(p^{NE},\tau^{NE},\gamma^{NE})$ is a NE if none of the players can benefit by deviating from their NE actions knowing that their opponents play according to the NE. Hence, NEs are system states that are stable to unilateral deviations. We can easily check that neutralizing the jammer $(p^{NJ},\tau^{NJ},0)$ in Proposition 1 is not an NE. Knowing that the jammer stays silent, player L can increase the game's utility by deviating to $\tau = 0$ (reducing τ increases the utility if no energy is harvested in the EH mode). This, in turn, will also cause the jammer to deviate from $\gamma = 0$ to $\gamma = \Gamma$.

The NE of the game $\mathcal{G}$ turns out to be unique; at the NE both players transmit with maximum power (similarly to the case in which there is no EH capability). Also, depending on the system parameters, the legitimate users may or may not use their EH capability. The above are captured in the following theorem.

***Theorem** 1: The game $\mathcal{G}$ has a unique NE given by (P,τ^{NE},Γ). Depending on the system parameters, the EH strategy is either $\tau^{NE} = 0$ or $\tau^{NE} = \min\{p_{th}^{-1}(P),\tau_{max}\}$ with $p_{th}^{-1}(P) = \frac{P}{P+2\zeta}$ and $\tau_{max} \in (0,1)$ representing the critical maximum point of $C(P,\tau,\Gamma)$ w.r.t. τ.*

The proof is detailed in Appendix B.

We observe that, at the NE and depending on the system parameters, player L may either harvest energy at a rate $\tau^{NE} < \tau^{NJ}$ or not at all $\tau^{NE} = 0$. Intuitively, at relatively high transmit power P, the dominant term in the utility (13) is the multiplicative term $1-\tau$ outside of the logarithmic term. Thus, when in NJ mode we may expect that the fraction of time spent neutralizing the jammer is too costly given that no energy is harvested and the NE provides a better utility to the legitimate users in spite of full power jamming.

IV. 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 $\Gamma = 1$, harvesting efficiency $\zeta = 0.7$, unit variance Rayleigh channel coefficients $\sigma^2 = \sigma_H^2 = 1$. The legitimate users transmit with power $P = \rho G$ with $\rho \in [0,5]$.

We start by evaluating the SKG capacity at both the NJ and NE states as a function of the system parameters. In Fig. 1, the relative gain in utility obtained at the NE $(C^{NE} = C(P,\tau^{NE},\Gamma))$ compared with the NJ $(C^{NJ} = C(p^{NJ},\tau^{NJ},0))$, 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

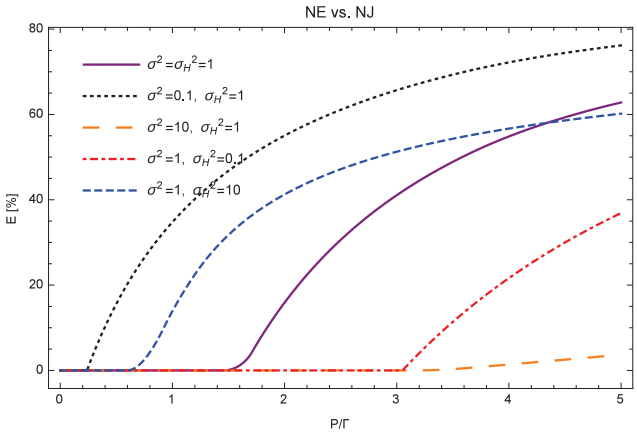

Fig. 1. Relative utility gain at the NE vs. NJ $E = (C^{NE}-C^{NJ})/C^{NE}$ as a function of $P/\Gamma \geq 0$ for $\zeta = 0.7$.

different values of σ^2 and σ_H^2. As expected the NJ strategy never outperforms the NE in terms of utility. However, when the SIR P/Γ is relatively small, both the NE and the NJ provide identical utilities. In this case, the strategies of player L are identical at both NE and NJ: $p^{NJ} = P$ and $\tau^{NJ} = \tau^{NE}$ and the jammer is indifferent between $\{0,\Gamma\}$. With increasing SIR P/Γ, it is no longer optimal for the legitimate player to harvest energy for a fraction of time τ^{NJ} in order to neutralize the jammer. Instead, by limiting the duration of EH to a fraction $\tau^{NE} < \tau^{NJ}$ the SKG capacity increases in spite of full power jamming $\gamma = \Gamma$. Finally, in the very high SIR regime, i.e., for $P/\Gamma \gg 1$, the legitimate users should not harvest energy at all.

In Fig. 2, for the benchmark setting, two operating regions are depicted w.r.t. P/Γ and the harvesting efficiency ζ. The darker region represents the operating modes in which $C^{NE} = C^{NJ}$, and the lighter region the operating modes for which $C^{NE} > C^{NJ}$. For small ζ, the harvesting return is limited and, as a result, a longer fraction of the symbol duration has to be used to neutralize the jammer. This implies that, at the NE, the legitimate users gain by decreasing the EH duration $\tau^{NE} < \tau^{NJ}$ for relatively lower values of the SIR P/Γ.

Subsequently, we evaluate the impact of the EH capability on the SKG capacity. In Fig. 3, the relative gain in utility obtained at the NE $C^{NE} = C(P,\tau^{NE},\Gamma)$ 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. The benchmark setup is considered and the different curves correspond to different harvesting efficiencies $\zeta \in [0.1,0.9]$. As expected, F increases with ζ. For $P/\Gamma = 1$, $\zeta = 0.5$ the gain is around 20 % while it increases to 30 % for $\zeta = 0.7$. At high SIR P/Γ, harvesting energy renders only negligible relative gains, irrespective of the harvesting efficiency.

Finally the relative utility F 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

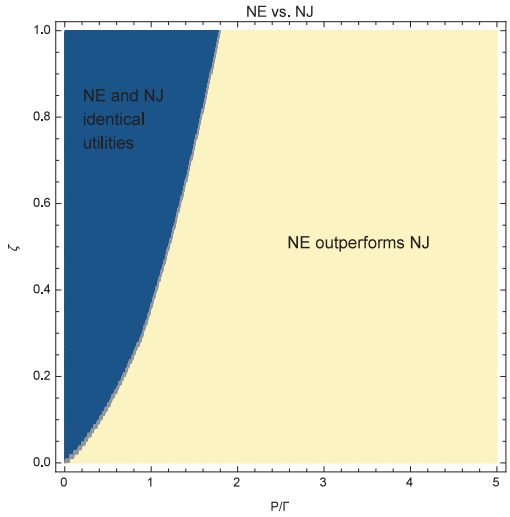

Fig. 2. NE vs. NJ regions as functions of $P/\Gamma \geq 0$ and $0 \leq \zeta \leq 1$ for $\sigma^2 = \sigma_H^2 = 1$.

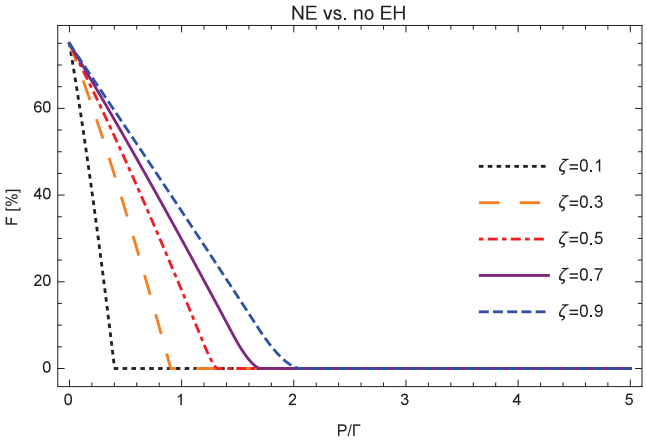

Fig. 3. Relative utility gain at the NE vs. no EH $F = (C^{NE} - C^{noEH})/C^{NE}$ as a function of $P/\Gamma \geq 0$.

97.5 % in certain cases, while for similar settings it is in the range of 60 % in the medium SIR range.

In conclusion, EH enables the legitimate users to combat the jammer's attacks more efficiently especially at relatively low SIR. This capability allows either to completely neutralize the jammer when $\tau^{NE} = \tau^{NJ}$ or to simply turn part of the jamming power to useful communication power.

V. Conclusions

In this work, energy harvesting at the legitimate users was investigated as a possible way to counteract malicious jamming in wireless SKG systems. A zero-sum game framework was introduced to analyze the adversarial interaction between a jammer and a pair of legitimate nodes; the game's unique NE was characterized in closed-form. The EH capability was shown to offer to the legitimate users the opportunity to effectively neutralize the jammer. However, this option does

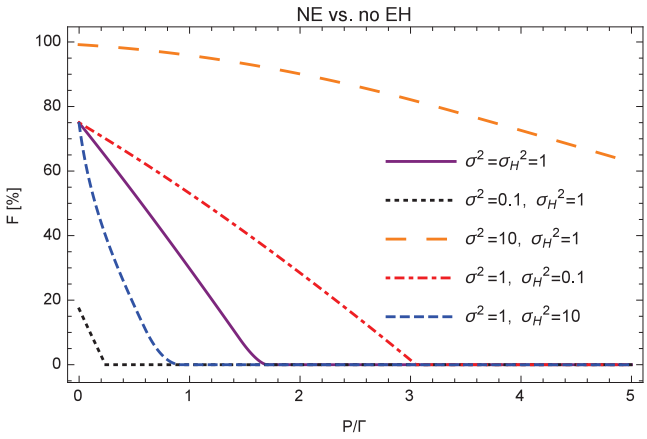

Fig. 4. Relative utility gain at the NE vs. no EH $F = (C^{NE} - C^{noEH})/C^{NE}$ as a function of $P/\Gamma \geq 0$ for $\zeta = 0.7$.

not necessarily correspond to the optimal strategy because when the jammer remains silent no actual energy can be harvested and the EH capability simply acts as a threat against jamming. Hence, at the NE, the legitimate users do not necessarily neutralize the jammer; in many cases the jamming power should instead be harvested in order to be used in the actual transmission. Numerical simulations show that the EH capability can greatly improve the relative utility compared to a system without EH, especially in the low SIR regime in which the relative gain can be particularly high.

Appendix A
Proof of Proposition 1

Proof: Assume that the legitimate users neutralize the jammer by transmitting at power $p \in [0, \min p_{th}(\tau), P]$. The jammer observes the legitimate user's choice and decides to stay silent. Notice that the legitimate user can force the jammer to remain silent by transmitting at $p \in [0, \min\{p_{th}(\tau) - \varepsilon_p, P\}]$ for an arbitrarily small $\varepsilon_p > 0$ (with little impact on the SKG utility). However, for simplicity, we will ignore this detail here.

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

$$C(p, \tau, 0) = \frac{1-\tau}{2} \log_2 \left(1 + \frac{p\sigma_H^2}{2 + \frac{1}{p\sigma_H^2}} \right), \qquad (19)$$

(while ensuring that the jammer stays silent). Since the feasible set of p depends on τ, we first have to find the maximum of $C(p, \tau, 0)$ w.r.t. p for any fixed τ. The function $C(p, \tau, 0)$ is strictly increasing in p and, hence, the optimal power is given by $\hat{p}(\tau) = \min\{P, p_{th}(\tau)\}$. Now, we need to maximize $C(\hat{p}(\tau), \tau, 0)$ w.r.t. $\tau \in [0, 1]$:

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

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:

$$(1-\tau)^2 - 8\sigma_H^4\zeta^2\tau^2 = 0, \tag{20}$$

it can be shown that $C(p_{th}(\tau),\tau,0)$ 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 $C(p_{th}(\tau),\tau,0)$ has a unique critical point that is the global maximizer $\hat{\tau} \in (0,1)$ and which is the solution to $\frac{dC(p_{th}(\tau),\tau,0)}{d\tau} = 0$. This implies that, if $p_{th}(\hat{\tau}) \leq P$, then the optimal solution that neutralizes the jammer is $\tau^{NJ} = \hat{\tau}$ and $p^{NJ} = p_{th}(\hat{\tau})$. If $p_{th}(\hat{\tau}) > P$, then the optimal solution that neutralizes the jammer is $p^{NJ} = P$ and $\tau^{NJ} = p_{th}^{-1}(P)$. ■

APPENDIX B
PROOF OF THEOREM 1

Proof: From Remark 1, we know that transmitting at maximum power is a strictly dominant strategy for player L and, hence, $p^{NE} = P$.

We start by proving that, at the NE, player L will not spend time harvesting energy longer than the threshold $p_{th}^{-1}(P)$. Let's suppose by absurdum that $\tau^{NE} > p_{th}^{-1}(P)$, then the jammer's best response would be to remain silent $\gamma^{NE} = 0$. Then, the optimal τ^{NE} maximizing the utility $C(P,\tau,0)$ (which is decreasing in τ) would be $\tau^{NE} \to p_{th}^{-1}(P)$ obtaining the utility $C^{NE} \to C(P,p_{th}^{-1}(P),0)$. 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 will choose an EH strategy such that $\tau^{NE} \leq p_{th}^{-1}(P)$ 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).

If the jammer uses maximum power $\gamma^{NE} = \Gamma$, then it does not gain by deviating. Thus, we only need to find the optimal value of $\tau \in [0, p_{th}^{-1}(P)]$ that maximizes the function $C(P,\tau,\Gamma)$ given by:

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

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

$$(1-\tau)^2(1+\sigma^2\Gamma)^2 - 2\sigma_H^4(P(1-\tau)+2\sigma^2\zeta\Gamma\tau)^2 = 0, \tag{21}$$

two different cases arise:

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

$$\tau^{NE} = \arg \max_{\tau \in \{0, \min\{p_{th}^{-1}(P), \tau_{max}\}\}} C(P,\tau,\Gamma). \tag{22}$$

- *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 $\tau^{NE} = \min\{p_{th}^{-1}(P), \tau_{max}\}$. Otherwise, the function is concave decreasing and $\tau^{NE} = 0$.

Since the state $(P, p_{th}^{-1}(P), 0)$ is not a NE, the game's unique NE is given by (P,τ^{NE},Γ) where τ^{NE} depends on the system parameters and equals zero or $\min\{p_{th}^{-1}(P), \tau_{max}\}$. ■

REFERENCES

[1] 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.

[2] 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.

[3] M. Bloch, J. Barros, M. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[4] 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.

[5] G. Wunder, R. Fritschek, and K. Reaz, "RECiP: Wireless channel reciprocity restoration method for varying transmission power," in *IEEE Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC)*, Valencia Congress Centre, Valencia, Spain, Sep. 2016.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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